

INFORMATION ASSURANCE

Legal, Regulatory, Policy and Organizational Considerations

4th Edition

August 1999



"It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. The President intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."

[White Paper on the Clinton Administration's Policy on Critical Infrastructure Protection:
Presidential Decision Directive 63, May 1998]

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
	EXECUTIVE SUMMARY.....	ES-1
1	INTRODUCTION.....	1-1
	1.1 Purpose and Scope	1-1
	1.2 Significant Events	1-1
	1.3 Critical Infrastructure Protection and Information Assurance.....	1-2
	1.4 Related Items.....	1-3
	1.5 Organization of the Document.....	1-5
2	LEGAL AND REGULATORY.....	2-1
	2.1 Introduction.....	2-1
	2.2 Legal	2-1
	2.3 Significant Legislation and Federal Guidelines	2-2
	2.3.1 A Review of the Compute Fraud and Abuse Act..... (Title 18 U.S.C. §1030)	2-2
	2.3.2 No Electronic Theft Act.....	2-5
	2.3.3 1997 Supplement to Federal Guidelines for Searching..... and Seizing Computers	2-6
	2.4 Significant Arrests and Opinions of 1997 and 1998.....	2-7
	2.4.1 Prosecuting Juveniles	2-7
	2.4.2 Extradition.....	2-9
	2.4.3 First Amendment Issues	2-9
	2.4.4 Privacy Issues	2-10
	2.4.5 Particularly Damaging or Dangerous Cases.....	2-11
	2.5 New Regulations	2-11
	2.6 Executive Order 13103	2-14
	2.7 Conclusions	2-16
3	POLICY AND DOCTRINE.....	3-1
	3.1 Introduction.....	3-1
	3.2 Report of the PCCIP	3-2
	3.3 “A National Security Strategy for a New Century”	3-4

TABLE OF CONTENTS (Continued)

<u>Section</u>		<u>Page</u>
3.4	Presidential Decision Directives.....	3-5
3.4.1	PDD 62.....	3-5
3.4.2	PDD 63.....	3-6
3.5	Office of the Secretary of Defense (OSD) Initiatives.....	3-7
3.6	Joint Publication 3-13.....	3-8
3.7	Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01B, Change 1	3-10
3.8	Licensing and Certification of Computer Personnel.....	3-12
3.9	Certification and Accreditation of Systems and Networks.....	3-12
3.10	Critical Assets Assurance Program (CAAP) and the DOD Critical..... Infrastructure Program	3-12
3.11	DOD Policy on Web Security.....	3-13
3.12	The Chief Information Officer (CIO).....	3-14
3.13	Encryption Policy.....	3-15
3.14	Conclusions.....	3-17
4	STANDARDS AND TECHNOLOGY.....	4-1
4.1	Introduction.....	4-1
4.2	Defense-In-Depth.....	4-1
4.3	Public Key Infrastructure.....	4-5
4.4	PKI Roadmap.....	4-7
4.5	Joint Standards Architectures.....	4-8
4.6	Electronic Commerce.....	4-10
4.7	Global Networked Information Exchange (GNIE).....	4-11
4.8	Conclusions.....	4-12
5	ORGANIZATIONAL CONSIDERATIONS.....	5-1
5.1	General.....	5-1
5.2	Reorganization.....	5-1
5.2.1	Assistant Secretary of Defense for Command, Control,..... Communications and Intelligence	5-1

TABLE OF CONTENTS (Continued)

<u>Section</u>		<u>Page</u>
	5.2.2 Joint Staff	5-2
	5.2.3 Transnational Warfare Office for Information Warfare Support (TWI)	5-2
5.3	New Organizations	5-2
	5.3.1 Joint Task Force (JTF) Computer Network Defense (CND)	5-2
	5.3.2 Defense-wide Information Assurance Program (DIAP)	5-4
	5.3.3 Defense Intelligence Officer (DIO) for Information..... Operations (IO)	5-5
	5.3.4 National Information Assurance Partnership (NIAP).....	5-5
	5.3.5 The Critical Infrastructures Assurance Office (CIAO)	5-6
	5.3.6 The National Infrastructure Protection Center (NIPC)	5-6
	5.3.7 Joint Web Risk Assessment Cell (JWRAC).....	5-7
5.4	Combatant Commands.....	5-7
5.5	Considerations	5-8
	5.5.1 Education and Training	5-9
	5.5.2 Requirements.....	5-9
	5.5.3 Working Relationships.....	5-9
5.6	Conclusions	5-10
 <u>Appendices</u>		
A	Organizations.....	A-1
B	Coordinating Activities	B-1
C	Legal Reference Guide	C-1
D	A Summary Guide to Information Assurance: Public Law, Executive Orders, and Policy Document	D-1
E	List of Acronyms	E-1
F	Glossary	F-1
G	Index.....	G-1

LIST OF EXHIBITS

<u>Exhibit</u>		<u>Page</u>
2-1	Computer Fraud and Abuse Act Elements of the Crime	2-4
2-2	Computer Fraud and Abuse Act Punishments	2-5
3-1	National IA Structure	3-6
3-2	Incident Reporting Structure.....	3-11
4-1	Analogies Between the Medieval Castle and the Defended C4ISR.....	4-2
4-2	The C4ISR Defense in Depth Protections	4-5
4-3	The Unity of the Three C4ISR Architectures.....	4-9
4-4	The Functions of the Three C4ISR Architectures	4-10
5-1	JTF Organization	5-3
5-2	How JTF Fits Into the Overall Organization.....	5-4

EXECUTIVE SUMMARY

PURPOSE AND SCOPE

Information Assurance (IA) is defined as "... operations that protect and defend information and information systems by ensuring their availability ... (to include) providing for (the) restoration of information systems by incorporating protection, detection, and reaction capabilities."¹ The first edition of this report was published in 1995 to highlight the legal, regulatory, policy, organizational, technical and threat issues associated with IA and to serve as a reference document for numerous IA developments. Subsequent editions added depth, provided details on specific organizations and activities, and detailed areas of IA community consensus. They also introduced new material on IA operational considerations, international aspects of IA, and concepts of Information Operations (IO). This fourth edition provides updated information on specific organizations and also provides some of the emerging Critical Infrastructure Protection (CIP) policies, concepts, and organizations. Like previous editions, this edition addresses high-level DOD and Federal government organizations. This edition is provided to the engaged IA 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.

CRITICAL INFRASTRUCTURE PROTECTION (CIP)

In recent years, growing concern about terrorism has led to increased attention on information assurance and critical infrastructure protection at the highest levels of the Federal government. The importance of CIP is emphasized in the recently published National Security Strategy:

"Our military power and national economy are increasingly reliant upon interdependent critical infrastructures – the physical and information systems essential to the operations of the economy and government.... It has long been the policy of the United States to assure the continuity and viability of these critical infrastructures. But advances in information technology and competitive pressure to improve efficiency and productivity have created new vulnerabilities to both physical and information attacks as these infrastructures become increasingly automated and interlinked.... Any interruption or manipulation of these critical functions must be brief, infrequency, manageable, isolated, and minimally detrimental to the welfare of the United States."²

In response to this growing threat and subsequent infrastructure vulnerability, the President signed Executive Order 13010 in July 1996. The Executive Order created the President's Commission on Critical Infrastructure Protection, which was charged with

¹ Department of Defense Directive S-3600.1, *Information Warfare (U)*, December 1996.

² The White House, *A National Security Strategy for a New Century*, October 1998, page 20.

developing a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats. The Commission's report was released in October 1997. It provided over 70 specific recommendations regarding the need for increased training and awareness, government-industry cooperation and information sharing, modernization of laws related to infrastructure protection, focused research and development, and a national structure to manage implementation of the recommendations.

In May 1998, the White House released Presidential Decision Directive 63. The Directive: 1) Established a national goal for infrastructure protection; 2) Created a national structure much like that recommended by the President's Commission; 3) Provided guidelines on infrastructure protection; 4) Required each Federal department and agency to assign IA responsibilities to the Chief Information Officer and appoint a Chief Infrastructure Assurance Officer; and, 5) Called for a National Infrastructure Assurance Plan to address specific tasks such as vulnerability analyses, warning, response, reconstitution, etc.

The national structure outlined in PDD 63 is shown in Exhibit ES-1.

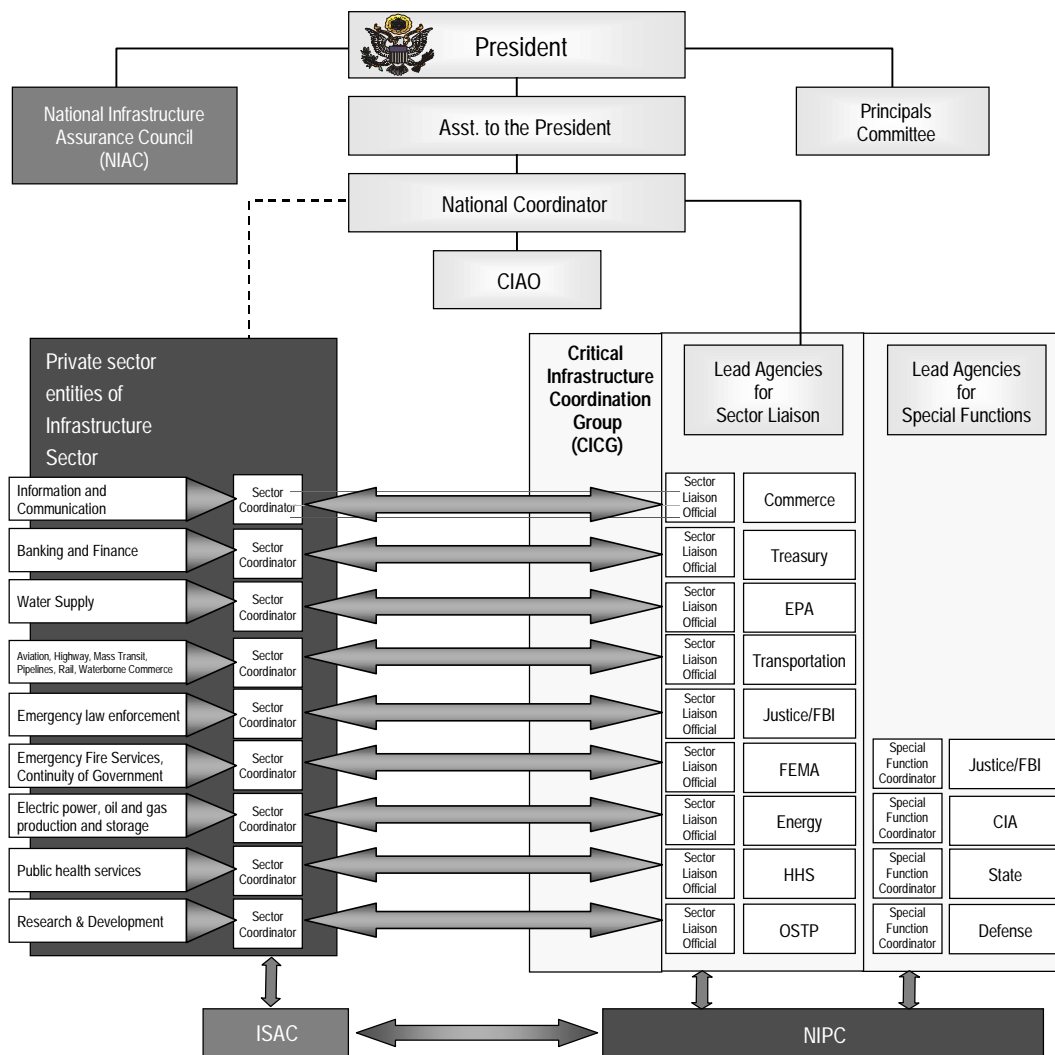


Exhibit ES-1. PDD 63 National Structure

The National Coordinator is a member of the staff of the Assistant to the President for National Security Affairs. The Principals Committee on the government side and the National Infrastructure Assurance Council on the private sector side provide high-level advice and assistance to the President and meet periodically to enhance the partnership of the public and private sectors in protecting critical infrastructures. PDD 63 charges the Critical Infrastructure Assurance Office with integrating the various sector plans into a National Infrastructure Assurance Plan. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official and to cooperate with the private-sector Sector Coordinators. The Critical Infrastructure Coordination Group, chaired by the National Coordinator, consists of Sector Liaison Officials and Functional Coordinators and chaired by the National Coordinator coordinates the implementation of PDD 63. On the public side, a National Infrastructure Protection Center (NIPC) has been established to serve as a national entity to collect, analyze and disseminate information on critical infrastructure threat assessments, warning, vulnerability, and law enforcement investigation and response capabilities. The National Coordinator working with various Federal officials and private sector representatives establishes one or more Information Sharing and Analysis Centers to serve as a mechanism to gather, analyze, and appropriately sanitize and disseminate private sector information (such as that developed by the NIPC) to both industry and the NIPC.

CRITICAL INFRASTRUCTURE PROTECTION AND INFORMATION ASSURANCE

Recent DOD exercises and actual attacks against DOD information systems reinforced the need to focus more attention on IA. Exercise ELIGIBLE RECEIVER 97, a no-notice Joint Chiefs of Staff exercise conducted in June 1997, demonstrated that hostile forces could penetrate national infrastructures and DOD networks and could affect DOD's ability to perform certain missions. An expert Red Team using only open source intelligence and commonly available hacker tools was able to demonstrate DOD and national-level system and network vulnerabilities and emphasized the need for effective vulnerability assessments, indications and warning, command and control, consequence management, and interagency planning, procedures, and processes.

In early February 1998, a series of intrusions code-named by the FBI as SOLAR SUNRISE, gave all the appearances of a well-orchestrated and concerted cyber attack against DOD systems and networks coincident with an escalating Middle East crisis. While the attackers were eventually shown to be US teenagers with an Israeli mentor, the simplistic, yet highly coordinated attack against DOD logistics, finance, and personnel systems reinforced the findings of ELIGIBLE RECEIVER 97 and clearly demonstrated the need for defined Federal and DOD organizations to manage the defensive information battle.

Such experiences suggest a need to identify the relationship of critical infrastructure protection and information assurance. While definitions and terms of reference have not yet been fully agreed to across both the public and private sectors, some basic concepts are emerging. CIP in the traditional sense is protecting the critical infrastructures against physical and electronic attack. Historically, most of the nation's critical infrastructure have been physically and logically separate systems with little interdependence. As a result of

advances in information, these infrastructures have become increasingly automated and inter-linked. Many, if not most, of the control, administration, and maintenance systems for the critical infrastructures are vitally dependent on information technology and information systems. Information assurance is a vital and integral part of critical infrastructure protection. That the draft National Infrastructure Assurance Plan called for by PDD 63 is titled "The National Information Systems Protection Plan" emphasizes this point.

UPDATE

The following paragraphs briefly summarize some of the key CIP and IA activities that have occurred since publication of the 3rd Edition of this report in September 1997. Details for each subject area below are included in a chapter of the main body of the report or an appendix to the report having the same subject area name.

Legal and Regulatory. Only one IA-related law was passed since publication of the 3rd Edition. The *No Electronic Theft Act* was passed in December 1997. This act strengthened copyright and trademark laws to accommodate technology considerations. While not of significant importance to IA, it does further exemplify that the law (statutes and case law) generally chases technology creating near-term operational voids and ambiguity, a point emphasized in detail in the 2nd Edition. The Administration's new policy on encryption technology that permits export of up to 56-bit Digital Encryption Standard and equivalent products and relaxes some of the key recovery requirements was codified in the Code of Federal Regulations. Executive Order 13103, *Computer Software Piracy*, was signed in October 1998. This order causes Federal departments and agencies to be much more aware of the sources of software used in the information systems employed to support key missions and functions. Finally, recent case law shows an increasing propensity to prosecute juveniles for computer crimes and for some nations to honor requests for extradition for computer crimes. In addition to providing a detailed discussion of the legal and regulatory area, the report includes a legal reference guide as an appendix.

Policy and Doctrine. The discussion above on CIP highlights the most significant policy development since publication of the 3rd Edition. Two other key developments were the publication of Change 1 to Chairman Joint Chiefs of Staff Instruction 6510.01B, *Defensive Information Operations Implementation*, in August 1998 and of Joint Publication (JP) 3-13, *Information Operations*, in October 1998. The change to CJCSI 6510.01B included a process to report computer intrusions and an IA vulnerability alerting process to provide more positive control of vulnerability alerting and tracking of approved fixes. JP 3-13 formalized the doctrine for many of the on-going information operations practices in the areas of military deception, physical attack and destruction, psychological operations, operations security, electronic warfare, computer network attack, etc. It includes doctrine for defensive information operations. The areas of computer network defense and information assurance are major elements of defensive information operations. In related developments, a Defense-wide Information Assurance Program and supporting staff were established to coordinate all DOD information assurance activities, a policy mandating the training and certification of network users and systems and network administrators was promulgated by OSD, and a top-to-bottom review of all DOD web pages and web sites was

directed by OSD in December 1998. The report also includes, as an appendix, an annotated bibliography of infrastructure protection and information assurance related policy documents.

Standards and Technology. Considerable emphasis has been given to establishing a “defense in depth” strategy for the Defense Information Infrastructure. In simple terms, DISA implements this concept at the regional and global levels and the CINCs, Services, and Defense Agencies implement the concept at the local level (and in coordination with DISA, occasionally, at the regional level). At all levels, this defense in depth concept includes techniques such as:

- Physical and logical protection of key network elements,
- Use of firewalls, filtering routers and the like to establish and protect network boundaries and protected enclaves (communities of interest such as operations, intelligence, personnel, finance) within network boundaries,
- Use of trusted computer operating systems and security-enabled computer applications,
- Use of security sensors and management tools to detect network and host-computer intrusions, to implement security policies, and to manage security configurations of systems and networks, and
- Use of digital signatures and public key encryption to provide for encryption, authentication of network transactions, integrity of data and non-repudiation of transactions.

Organizational Considerations. Restructuring and realignment of information assurance and critical infrastructure protection responsibilities have caused many organizations to reorganize. In addition, new organizations have been created to support these responsibilities. The most significant organizational development has been the activation of the Joint Task Force for Computer Network Defense (JTF-CND). Its mission is to coordinate and direct the defense of DOD computer systems and computer networks to include coordinating the DOD defensive actions with non-DOD government agencies and appropriate private organizations. The JTF is co-located with and supported by the Defense Information Systems Agency (DISA). Operationally, the Commander of the JTF (also the Vice Director of DISA) reports to the Secretary of Defense through the Chairman of the Joint Chiefs of Staff. The JTF will exercise tactical control over components forces provided by the Services.

Organizations. The following extracts from Appendix A highlight some of the specific organizational developments and activities and demonstrate the variety of these activities occurring throughout the Federal government:

- The Office of the Assistant Secretary of Defense (C3I) has established staff elements to address information assurance and critical infrastructure protection.
- The Army will incorporate lessons learned from the Bosnia experience in a forthcoming update to FM 100-6, *Information Operations*.
- The Fleet Information Warfare Center established an Information Warfare/Command and Control lessons learned database for the Navy.
- The Air Force is developing an Information Protect Operations Decision Support System. It will be used to collect, integrate, and display threat, vulnerability and system data to quantify risks and develop courses of action for information protect operations.
- The Defense Advanced Research Projects Agency is conducting an ambitious Information Survivability research and development Program.
- The Defense Information Systems Agency is assisting the Combatant Commands in assessing their information assurance posture and providing on-site training, security management, and network and systems configuration assistance.
- An Information Assurance Technology Analysis Center was established as one of 13 Information Analysis Centers in the Defense Technical Information Center. The Center serves as the DOD central point of access for scientific and technical information in support of defensive information operations.
- The Department of Energy National Laboratories are conducting network security research. One of the Laboratories conducts an information assurance outreach program.
- The Department of Justice and the National Information Protection Center have initiated InfraGard, a program to facilitate information sharing among government and industry.
- The Department of Transportation has established an active program to identify critical information systems.
- Interoperability remains the biggest information assurance issue for the United States Coast Guard.
- The General Services Administration has been designated the Executive Agent for the Federal Sector and charged with creating the Federal model for infrastructure protection. GSA is also heavily involved in the security aspects of government-wide electronic commerce and electronic messaging.

Coordinating Activities. Organizations and activities whose purpose is to coordinate infrastructure protection and information assurance activities across the Federal government are discussed in Appendix B. Some key activities include:

- National Intelligence Council is embarking on a systematic research and development program to identify broad, cross-cutting issues in the areas of warning, the future of military conflict, the information revolution, and the declining authority of Nation-states.
- The National Research Council recently released *Trust in Cyberspace*, a report that suggests a future direction in network trustworthiness research and development. One suggestion is to abandon the traditional model of “absolute security” and move to a model of “insecurity” based on three axioms – insecurity exists, insecurity cannot be destroyed, and insecurity can be moved around – and the use of vulnerability assessments to influence system and network designs.
- The National Communications System (an Interagency Group) and the President’s National Security Telecommunications Advisory Committee continue to address a broad range of information assurance issues related to national security and emergency preparedness telecommunications such as cellular priority access service, a transportation sector information assurance risk assessment, and a risk assessment of the public telephone network.

Because of the extensive organizational and reference information documented herein, this report can serve as a source book on information assurance background, stakeholders, interests, and activities. This 4th Edition does not, however, replace previous editions. Users of this document are encouraged to use this and previous editions as a point of departure for further exploration into the various dimensions of the dynamically developing domains of critical infrastructure protection and information assurance.

Finally, because of review and publication requirements, the information in this document is current as of March 1999.

This page intentionally left blank.

SECTION 1

INTRODUCTION

All of our critical infrastructures rely on computers, advanced telecommunications, and, to an ever-increasing degree, the Internet. They use these resources to control, administer, and maintain their systems, interact with other infrastructures, and communicate with suppliers and the customer base.

Because these infrastructures are critical to our national well being, adversaries will look upon them as targets.

1.1 PURPOSE AND SCOPE

The first edition of this report was published in 1995 to highlight the legal, regulatory, policy, organizational, technical and threat issues associated with information assurance and to serve as a reference document for numerous information assurance developments. Subsequent editions added depth and provided details on specific organizations and activities. They also introduced new material on information assurance operational considerations, international aspects of information assurance, and concepts of information operations. This fourth edition provides updated information on specific organizations and also provides some of the emerging critical infrastructure protection policies, concepts, and organizations. This edition is provided 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.

1.2 SIGNIFICANT EVENTS

In recent years, growing concern about terrorism led to this increased attention on information assurance and critical infrastructure protection at the highest levels of the Federal government. In response, the President signed Executive Order 13010 in July 1996. The Executive Order created the President's Commission on Critical Infrastructure Protection, which was charged with developing a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats. The Commission's report was released in October 1997. It provided over 70 specific recommendations regarding the need for increased training and awareness, government-industry cooperation and information sharing, modernization of laws related to infrastructure protection, focused research and development, and a national structure to manage implementation of the recommendations.

In May 1998, the White House released Presidential Decision Directive 63. The Directive: 1) established a national goal for infrastructure protection; 2) created a national structure much like that recommended by the President's Commission; 3) provided guidelines on infrastructure protection; 4) required each Federal department and agency to assign information assurance responsibilities to the Chief Information Officer and appoint a Chief Infrastructure Assurance

CONTENTS

Purpose and Scope
Significant Events
• President's Commission on Critical Infrastructure Protection
• CJCS Exercise Eligible Receiver 97
• Operations Solar Sunrise
Critical Infrastructure Protection and Information Assurance
Related Items
• Y2K
• Allied and Coalition Activities
Organization of the Document

Officer; and, 5) called for a National Infrastructure Assurance Plan to address specific tasks such as vulnerability analyses, warning, response, reconstitution, etc.

Recent DOD exercises and actual attacks against DOD information systems reinforced the need to focus more attention on information assurance. Exercise ELIGIBLE RECEIVER 97, a no-notice exercise conducted in June 1997, demonstrated that hostile forces could penetrate DOD networks and affect the Department's ability to perform certain missions. An expert Red Team using open source intelligence and commonly available hacker tools was able to demonstrate DOD and national-level system and network vulnerabilities and emphasized the need for effective vulnerability assessments, indications and warning, command and control, consequence management, and interagency planning, procedures, and processes.

In early February 1998, a series of intrusions nicknamed Operation SOLAR SUNRISE gave all the appearances of a well-orchestrated and concerted cyber attack against DOD systems and networks in conjunction with an escalating Middle East crisis. While the attackers were eventually shown to be US and Israeli teenagers, the sophisticated attack against DOD logistics, finance, and personnel systems reinforced the findings of ELIGIBLE RECEIVER 97 and clearly demonstrated the need for an organization to manage the defensive information battle.

The foregoing led to the following statement emphasizing the importance in critical infrastructure protection in the recently published National Security Strategy:

"Our military power and national economy are increasingly reliant upon interdependent critical infrastructures – the physical and information systems essential to the operations of the economy and government.... It has long been the policy of the United States to assure the continuity and viability of these critical infrastructures. But advances in information technology and competitive pressure to improve efficiency and productivity have created new vulnerabilities to both physical and information attacks as these infrastructures become increasingly automated and interlinked.... Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, isolated, and minimally detrimental to the welfare of the United States."¹

1.3 CRITICAL INFRASTRUCTURE PROTECTION AND INFORMATION ASSURANCE

While definitions and terms of reference have not been fully agreed to across both the public and private sectors, some basic concepts are emerging. Critical infrastructure protection in the traditional sense is protecting the critical infrastructures against physical and electronic attack. Historically, most of the nation's critical infrastructures have been physically and logically separate systems with little interdependence. As a result of advances in information, these infrastructures have become increasingly automated and inter-linked.

Many, if not most, of the control, administration, and maintenance systems for the critical infrastructures are vitally dependent on information technology and information systems. While protecting both the physical and information elements of these infrastructures is important, the vulnerability of the information systems supporting the infrastructures is of

¹ The White House, *A National Security Strategy for a New Century*, October 1998, page 20.

more immediate concern. All critical infrastructures rely on computers, advanced telecommunications, and to an ever-increasing degree, the INTERNET, for a variety of functions to include communication with suppliers and the customer base.

Information assurance is a vital and integral part of critical infrastructure protection. The report of the President's Commission on Critical Infrastructure Protection also emphasizes the need to protect the information components of the critical infrastructures.

"Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend.

The rapid growth of a computer-literate population ensures that an increasing millions of people possess the skills necessary to consider such an attack. The wide adoption of public protocols for system interconnection and the availability of "hacker tool" libraries make their task easier.

While the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm."²

That the draft National Infrastructure Assurance Plan called for by PDD 63 is titled "The National Information Systems Protection Plan" provides additional emphasis to the point.

1.4 RELATED ITEMS

It is difficult to address information assurance activities without mentioning the Y2K problem. Because of the vast amount of media attention to this issue, within DOD and throughout society, it will not be addressed in this report. It is important to note, however, that many of the activities started to address the Y2K problem are equally valid information assurance activities. For example, a critical first step in information assurance is to identify the critical missions and functions performed by an organization and the information infrastructure elements that support the critical missions and functions. This information is essential to specifying needed infrastructure protection, conducting risk analyses, drafting contingency plans, and developing rules of engagement for responding to attacks on the infrastructure. The key first step in addressing the Y2K problem is to also identify the critical systems supporting the critical missions and functions. There are many other parallels between Y2K activities and information assurance activities – awareness and training, response teams, exercises. In short, both the private sector and government organizations can get a jump-start on good information assurance planning and implementation by using the processes developed for Y2K and applying the Y2K lessons learned.

² President's Commission on Critical Information Protection, *Report Summary, Critical Foundations - Thinking Differently*. Available at <http://www.pccip.gov/summary.html>.

Several information assurance initiatives involving allies and coalition partners are beginning to emerge. Because the primary focus of this report is on US DOD and National level activities, these international activities are only briefly summarized below.

NATO has not embraced the information assurance construct but has a robust INFOSEC program that includes many of the tenets of IA. Two high-level groups share responsibility for INFOSEC within NATO. The NATO Security Committee addresses INFOSEC policy and the NATO Command Control Consultation Board (NC3B) addresses implementation issues. The ASD (C3I) is the U.S. representative to the NC3B. On behalf of the Security Committee, the INFOSEC Working Group develops policy and guidance documents. One of eight subcommittees, the INFOSEC Subcommittee addresses INFOSEC implementation issues on behalf of the NC3B. Working groups under the subcommittee work specific issues including PKI, Interconnection of networks, Encryption, and developing an INFOSEC framework.

Noteworthy initiatives underway in NATO include:

- Adopting the Common Criteria for evaluating INFOSEC products.
- Firewalls and risk assessment and intrusion detection tools are being procured.
- A NATO Certification and Accreditation Process has been adopted.
- Establishing a NATO CERT is under discussion.
- The Working Group on Interconnection of Networks addresses many of the issues that arise during the annual Joint Warrior Interoperability Demonstration (JWID). The lessons learned from JWID are related to the working group through the lead U.S. representative. The working group is drafting a NATO directive on interconnection of NATO networks to coalitions and task forces comprised of NATO and non-NATO members.

Other coalition activities include the Defense Information Technology Security Working Group (DITSWG), made up of representatives from the certification and accreditation organizations of Australia, Canada, New Zealand, the United Kingdom, and the U.S. This group serves to develop common INFOSEC policies and practices among the member nations defense elements with the aim of ensuring proper and effective secure interconnection of systems. The DITSWG is currently finalizing a five-nation Statement of Common Security Policies and a Joint National Accreditation Process.

Other allied IA coordination initiatives are underway under the auspices of the Coalition Communications and Electronics Board (CCEB) and other bilateral and multilateral agreements.

1.5 ORGANIZATION OF THE DOCUMENT

The following sections address the key issues related to critical infrastructure protection and information assurance. These include legal and regulatory (Section 2), policy and doctrine (Section 3), standards and technology (Section 4), and organizational considerations (Section 5). As previously indicated, the focus of this edition has been on updating organizations and activities.

This page intentionally left blank.

SECTION 2

LEGAL AND REGULATORY

2.1 INTRODUCTION

This section updates the Legal and Regulatory Sections of the 3rd Edition. Please note that this section builds upon the information contained in the 3rd Edition and does not reintroduce all laws and regulations presented in the earlier edition. The purpose of this presentation is to analyze recently passed legislation, the results of information-assurance-related prosecutions, and changes in Federal Regulations on important topics such as encryption. Additional information on legislation and Executive Orders can be found in Appendix C, Legal Reference Guide.

<i>CONTENTS</i>
Legal
Significant Legislation and Federal Guidelines
• Computer Fraud and Abuse Act
• No Electronic Theft Act
• 1997 Supplement to Federal Guidelines for Searching and Seizure Computers
Significant Arrests and Opinions
• Prosecuting Juveniles
• Extradition
• First Amendment Issues
• Primary Issues
• Particularly Damaging or Dangerous Cases
New Regulations
• Encryption
Executive Order 1303
Conclusions

2.2 LEGAL¹

Cybercrime is one of the most complicated investigative and prosecutive challenges facing the United States Government today. In his March 19, 1997, testimony before the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, Deputy Assistant Attorney General, Criminal Division, Robert S. Litt discussed three roles computers can play in criminal activity:

- *First, a computer can be the target of an offense, for example if a hacker tries to steal information from, or do damage to, a computer or computer network. We are all familiar with examples of these, such as vandalism of Web sites or the introduction of viruses into computers.*
- *Second, the computer can be a tool in the commission of a traditional offense. Computers can replace the telephone as a tool in an illegal telemarketing operation; they can be and are used to create and transmit child pornography. Or, to give you a specific example, Russian computer hackers in St. Petersburg broke into a Citibank electronic money transfer system and tried to steal more than \$10 million by multiple wire transfers to accounts in at least seven different countries. Members of the gang have been arrested in several countries, but according to Citibank \$400,000 has still not been recovered.*

¹ A primary Internet site for legal information is that of the U. S. Department of Justice's Computer Crime and Intellectual Property Section. Available at this site is information about statutes, prosecutions, the Federal Search and Seizure Guidelines, as well as relevant speeches and Congressional testimony of key Justice officials on information assurance topics (<http://www.usdoj.gov/criminal/cybercrime>).

- *Finally, computers can be incidental to the offense, but still significant for law enforcement purposes. For example, many drug dealers now store their records on computers, which raises difficult forensic and evidentiary issues that we don't face with old-fashioned paper records.*

Of course, a single computer could be used in all three ways. For example, a "hacker" might use his computer to gain unauthorized access to an Internet Service Provider such as America On-Line — known as an "ISP" — and then use that access to illegally distribute copyrighted software stored on his computer's hard drive.²

Concerning difficulties encountered in prosecuting computer crime, Mr. Litt raised the issue of proving the criminal's and victim's identities in networked environments, as well as establishing jurisdiction. In essence, the anonymity provided by the Internet has complicated even these most basic elements of investigating and prosecuting crime. Attacks on Department of Defense systems during 1997 and 1998 illustrate the points raised by Mr. Litt, demonstrating the interagency and international complexities of investigating and prosecuting computer crime. In addition to the issues raised by Mr. Litt, the fact that the Federal court system is unaccustomed to prosecuting juveniles makes using prosecution as a deterrent a somewhat tenuous concept.

2.3 SIGNIFICANT LEGISLATION AND FEDERAL GUIDELINES

This section begins with a review of The Computer Fraud and Abuse Act, as amended 3 October 1996, which is codified at Title 18 U.S.C. §1030. While it is not new, it remains the primary statute for computer crime prosecution and is important to understand as context for the case law analysis. Next a new statute, The No Electronic Theft Act, which is codified at Title 17 U.S.C., §§506 and 507 and Title 18 U.S.C. §§2319, 232319A, and 2320, is highlighted. The No Electronic Theft Act is the only significant Federal legislation affecting information assurance that has been passed since the 3rd Edition.

2.3.1 A Review of the Computer Fraud and Abuse Act (Title 18 U.S.C. §1030)

The Act presents the following important definitions:

A protected computer is one that is:

- Exclusively for the use of a financial institution or the U.S. Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the U.S. Government and the conduct constituting the offense affects that use by or for the financial institution or the Government
- Used in interstate or foreign commerce or communications.

² <http://www.usdoj.gov/criminal/cybercrime/sentechtes.htm>.

Damage means "any impairment to the integrity or availability of data, a program, a system, or information, that:

- Causes loss aggregating at least \$5,000 in value during any one-year period to one or more individuals
- Modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals
- Causes physical injury to any person
- Threatens public health or safety.

Two major intents of the 1996 amendment were to pull together the various statutes under which computer crime had been prosecuted in the past and to clearly define the elements of computer crime in its various manifestations for more efficient and effective application of the law. The statute generally prohibits gaining or attempting to gain unauthorized access or exceeding authorized access to computers. The acts of gaining or attempting to gain unauthorized access and exceeding authorized access to obtain information are essential elements of the crimes. National security, financial, and medical information are specifically extended protection under this section, and §1030 (a)(2)(C) protects against interstate or foreign theft of any information by computer.

The Act levies punishment ranges from one to 20 years and/or fines, with the heaviest punishments linked to unauthorized or exceeded access to and disclosure of national security information, as described in (a)(1). Civil action is allowed for compensatory damages and injunctive or other equitable relief. Civil damages are limited to economic damages. The Act uses the wording: "knowingly," "with reason to believe," "intentionally," and so forth, which must be proven in prosecutions. Also, it is worth noting that the Government must prove that a certain person or persons committed the crime, not just that a particular computer was used.

The statute specifies that it does not prohibit lawfully authorized law enforcement or intelligence agency actions. The U.S. Secret Service, the FBI, and DOD have investigative jurisdiction under this statute.

The *Computer Fraud and Abuse Act*, as amended in October 1996, is briefed in Exhibits 2-1 and 2-2 which follow.

- (1) Whoever - (1) Knowingly accesses a computer to obtain information that is protected “against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the *Atomic Energy Act of 1954*: “With reason to believe that the information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation: willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to do so, to any person not entitled to receive it;
- (2) Intentionally access a computer to obtain information concerning credit or financial transactions; information from any department or agency of the United States; information from any protected computer if the conduct involved an interstate or foreign communication;
- (3) Intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer affecting its use by or for the Government of the United States;
- (4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, to further the intended fraud and obtains anything of value, “unless the object of the fraud and the thing obtained consist only of the use of the computer and the value of such use is not more than \$5,000 in any one-year period.”
- (5) (a) Knowingly causes the transmission of “a program, information, code, or command,” and causes damage to a protected computer;
- (b) Intentionally accesses a protected computer without authorization and recklessly causes damage; or
- (c) Intentionally accesses a protected computer without authorization and causes damage.
- (6) Knowingly and with intent to defraud traffics a password or similar information through which a computer can be accessed without authorization, if:
 - (a) Such trafficking affects interstate or foreign commerce; or
 - (b) Such computer is used by or for the Government of the United States.
- (7) With intent to extort money or a thing of value, transmits in interstate or foreign commerce any threat to cause damage to a protected computer.

And, whoever attempts to commit an offense described above.

Exhibit 2-1. Computer Fraud and Abuse Act Elements of the Crime

- (c)(1)(A) “a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1), “which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (c)(1)(B) a fine and/or imprisonment for not more than twenty years for a violation of subsection (a)(1), which occurs after a conviction for another offense under this section or an attempt to commit an offense punishable under this subparagraph;
- (c)(2)(A) a fine and/or imprisonment for not more than one year committing an offense under subsection (a)(2), which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
- (c)(2)(B) a fine and/or imprisonment for not more than 5 years for an offense under subsection (a)(2) if:
 - (i) the offense was committed for commercial advantage or private financial gain;
 - (ii) “the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or
 - (iii) “the value of the information obtained exceeds \$5,000;”
- (c)(3)(A) “a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1), “which occurs after a conviction for another offense under subsection (a)(2), (a)(3), or (a)(6) of this section or an attempt to commit an offense punishable under this subparagraph;” and
- (c)(3)(B) “a fine and/or imprisonment for not more than five years for a violation of subsection (a)(1),” which does not occur after a conviction for another offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section or an attempt to commit an offense punishable under this subparagraph;” and
- (c)(3)(C) “a fine and/or imprisonment for not more than ten years for a violation of subsection (a)(1),” which occurs after a conviction for another offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) “of this section or an attempt to commit an offense punishable under this subparagraph.

Exhibit 2-2. Computer Fraud and Abuse Act Punishments

2.3.2 No Electronic Theft Act

On 16 December 1997, The No Electronic Theft Act was signed into law. The Act was passed, at least in part, in response to *U.S. v. LaMacchia*³, in which a 21-year-old MIT student set up a bulletin board and distributed pirated software through it. The wire-fraud statute, that was available at the time, required proof that the perpetrator personally profited from the crime. As the Government was unable to demonstrate this, the prosecution for copyright infringement was unsuccessful. The new Act eliminates the personal-gain requirement and strengthens the copyright and trademark laws to accommodate technology considerations. The Act amends the criminal copyright and

³ 871 F. Supp. 535 (D. Mass. 1994).

trademark provisions in 17 U.S.C. §§ 101, 506, and 507 and 18 U.S.C. §§ 2319, 2319A, and 2320 to include the following:⁴

- Individuals may be prosecuted under misdemeanor or felony provisions in cases involving large-scale illegal reproduction or distribution of copyrighted works where the infringers act willfully but without a discernible profit motive. Reproducing or distributing ten or more copies of one or more copyrighted works that have an aggregate retail value of \$2,500 or more constitutes a felony, and carries a maximum sentence of three years imprisonment and a fine of \$250,000. Reproducing or distributing one or more copies of one or more copyrighted works that have a total retail value of more than \$1,000 constitutes a misdemeanor and carries a one-year maximum sentence and a fine of up to \$100,000.
- Reproducing or distributing that constitutes small-scale non-commercial copying (copyrighted works with a total retail value of less than \$1,000) or is not done "willfully," is exempt from criminal prosecution;
- "Willful" infringement must consist of evidence of more than the mere intentional reproduction or distribution of copyrighted works;
- "Financial gain" in the Copyright Act (17 U.S.C. §101 et seq.) is now defined to include the "receipt, or expectation of receipt, of anything of value, including the receipt of other copyrighted works." This ensures that persons who illegally traffic in copyrighted works by using barter rather than cash are covered by the statute;
- "Reproduction or distribution" includes by electronic as well as tangible means;
- The statute of limitations is extended from three to five years, making the criminal copyright statute consistent with most other criminal statutes;
- There is a recidivist provision that raises penalties for second or subsequent felony copyright offenses;
- Parties who own rights in the pirated copyrighted works or in trademarks on counterfeit goods may now provide a victim impact statement to the sentencing court; and
- The Sentencing Commission is to amend the Sentencing Guideline for copyright and trademark infringement to allow courts to consider the quantity of infringing goods and the retail value of the good infringed upon, rather than the often lower value of the infringing good when sentencing.

2.3.3 1997 Supplement to Federal Guidelines for Searching and Seizing Computers

The Computer Crime and Intellectual Property Section's October 1997 *Supplement to Federal Guidelines for Searching and Seizing Computers* is available online at the Computer Crime and

⁴ This section is drawn closely from the USDOJ, Computer Crime and Intellectual Property Section's *Summary of Changes to the Criminal Copyright and Trademark Laws* (<http://www.usdoj.gov/criminal/cybercrime/netsum.htm>).

Intellectual Property Section's Internet site (<http://www.usdoj.gov/criminal/cybercrime/netsum.htm>). The supplement updates the July 1994 *Federal Guidelines for Searching and Seizing Computers* and describes relevant federal cases decided since the 1994 edition, as well as earlier decisions. New to the supplement are state cases, which were not addressed in the 1994 guidelines.

2.4 SIGNIFICANT ARRESTS AND OPINIONS OF 1997 AND 1998

As described above, new legislation is often passed in response to problems that arise as prosecutions show existing statutes to be outdated or insufficient. Such was the case with The No Electronic Theft Act, which amends the insufficiency of the law encountered in prosecuting *U.S. v. LaMacchia*. According to the Office of Policy Analysis of the US Sentencing Commission, there were 26 prosecutions under The Computer Fraud and Abuse Act in 1997.⁵ This section reviews significant arrests and court opinions that will shape the application of the law on information assurance-related cases. The section highlights the difficulties encountered in attempting to prosecute juveniles in Federal court, the trend toward international cooperation in computer crime investigations, some First amendment and privacy issues, and some particularly damaging cases.

2.4.1 Prosecuting Juveniles

As mentioned in the introduction to the Legal and Regulatory Section, prosecuting juveniles in Federal court is problematic. Often their crimes are viewed as little more than pranks of bright and promising adolescents. Also, there is not an historic body of precedents for judges to consult in deriving opinions and sentences. Even when lives were at stake, the tendency in sentencing has been leniency as shown in the following example.

2.4.1.1 Juvenile Hacker Disrupts FAA Control Tower. In March of 1997, a juvenile computer hacker used his personal computer and modem to disable a telephone company computer that serviced the Worcester, Massachusetts Airport. The juvenile, whose name remains sealed, disabled NYNEX loop carrier systems to the FAA control tower for six hours. Loop carrier systems are used by telephone companies to integrate hundreds of telephone lines for digital transmission over single, high capacity fiber-optic cables to central offices. The systems allowed remote access for repairs.

"This case, with the associated national security ramifications, is one of the most significant computer fraud investigations conducted by the US Secret Service," said Michael T. Johnston, Acting Special Agent in Charge of the Boston Office of the US Secret Service.⁶

⁵ Leibowitz, Wendy R., "Judges Having Hard Time With Computer Crime: Sentencing Standards Aren't Clear-Cut," *National Law Journal*, July 6, 1998 (<http://www.ljx.com>).

⁶ "Juvenile Computer Hacker Cuts off FAA Tower At Regional Airport - First Federal Charges Brought Against a Juvenile for Computer Crime," undated Department of Justice press release (<http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm>).

The press release describes the events that ensued on March 10, 1997, as follows:

At approximately 9:00 a.m., the juvenile computer hacker intentionally, and without authorization, accessed the loop carrier system servicing the Worcester Airport. He then sent a series of computer commands to it that altered and impaired the integrity of data on which the system relied, thereby disabling it. Public health and safety were threatened by the outage which resulted in the loss of telephone service, until approximately 3:30 p.m., to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to other related concerns such as airport security, the weather service, and various private airfreight companies. Further, as a result of the outage, both the main radio transmitter, which is connected to the tower by the loop carrier system, and a circuit which enables aircraft to send an electric signal to activate the runway lights on approach were not operational for this same period of time.

Later on the same day, at approximately 3:30 p.m., the juvenile computer hacker intentionally, and without authorization, accessed the loop carrier system servicing customers in and around Rutland, Massachusetts. Once again, he sent a series of computer commands to the digital loop carrier that altered and impaired the integrity of data on which the system relied, thereby disabling it. The second outage disrupted telephone service throughout the Rutland area, causing financial damage as well as threatening public health and safety as a result of the loss of telephone service. During this attack, the juvenile computer hacker changed the system identification to "Jester."

The juvenile also broke into a pharmacy computer on four occasions and copied patient records by sending the command that the pharmacy computer send files of all the prescriptions filled by the pharmacy over the previous week, including customer name, address, telephone number and the prescription supplied. AT&T reported the activity to the US Secret Service, which investigated the case and made the arrest. The juvenile received two years of probation and 250 hours of public service. These are the first federal charges to be brought against a juvenile for computer crime. The United States Attorney's Office called the plea bargaining, "a balanced effort, weighing the seriousness of this juvenile's computer intrusions and his lack of malevolence."⁷

2.4.1.2 Ehud Tenebaum, TooShort and Makaveli. During February 1998, the DOD detected a series of computer intrusions into its systems. The Department of Justice, FBI, Air Force Office of Special Investigation, Naval Criminal Investigative Service, and the National Aeronautic and Space Administration worked together in investigating these intrusions. Also accessed were hundreds of commercial and educational institution systems in the United States and other countries. While the attacks kept Government personnel busy for weeks, there was no loss of classified information nor disruption of military operations.

⁷ "Juvenile Computer Hacker Cuts off FAA Tower At Regional Airport - First Federal Charges Brought Against a Juvenile for Computer Crime," undated Department of Justice press release (<http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm>).

On 18 March 1998, Ehud Tenebaum, an 18-year-old Israeli citizen, was arrested by the Israelis for illegally accessing Israeli and US Government computers. Tenebaum was charged under Title 18 §1030, but not extradited. In Cloverdale, California, FBI agents seized computer equipment belonging to two accomplices known as TooShort and Makaveli, 15- and 16-year-old boys. On July 30, 1998, the teens pleaded guilty. After a court hearing concerning the role they played in causing this interagency, international investigation, their computer equipment was forfeited to the Government, they received suspended sentences, and are not allowed to use computer equipment unsupervised or obtain jobs in the computer field during the period of their probation.

2.4.2 Extradition

Eugene E. Kashpureff pleaded guilty to violations of Title 18 §1030. Kashpureff, the owner of a Washington State-based commercial registration service for Internet domain names, admitted to using DNS corruption software to interrupt service for tens of thousands of Internet users throughout the world. According to the press release:

Kashpureff, a self-described 'webslinger,' designed a corruption of the software system that allows Internet-linked computers to communicate with each other. By exploiting a weakness in that software, Kashpureff hijacked Internet users attempting to reach the Web Site for InterNIC, his chief commercial competitor, to his AlterNIC Web Site, impeding those users' ability to register Web Site domain names or to review the InterNIC's popular 'electronic directory' for existing domain names.⁸

Kashpureff, 33, was extradited from Canada where he had fled after launching Internet attacks then bragging to the media that he could "divert all communications destined for China, the 100 most visited Web Sites in the world, and the White House Web Site."⁹

2.4.3 First Amendment Issues

1997 and 1998 brought significant opinions on First Amendment rights on-line.¹⁰

- *U.S. v. Machado, No. SACR 96-142-ASH (S.D.Cal.)*. Richard Machado was a University of California at Irvine student who used a university computer and network to email hate messages threatening Asian students. Machado was convicted under Federal civil rights statutes. Machado used a university computer to send email to 59 Asian students. He told them to leave the university or he would "hunt all of you down and kill your stupid asses;" and "I personally will make it my life's work to find and kill every one of you personally. OK? That's how determined I am. Do you hear me?"

⁸ Department of Justice press release, United States Attorney, Eastern District of New York, March 19, 1998 (<http://www.usdoj.gov/criminal/cybercrime/kashpureff.htm>).

⁹ United States Attorney, Eastern District of New York, press release, March 19, 1998 (<http://www.usdoj.gov/criminal/cybercrime/kashpureff.htm>).

¹⁰ First Amendment cases are drawn from "Top Cyberspace Law Cases of 1998," The UCLA Online Institute for Cyberspace Law and Policy (<http://www.gse.ucla.edu/iclp/98cases>).

- *Compuserve Germany*. On May 28, 1998 in Munich, Germany, Felix Somm, former CompuServe Deutschland, was convicted of violating local pornography laws. Somm was blamed for not blocking access to pornographic pictures that were available on the Internet. Somm was sentenced to two years' probation and ordered to donate 100,000 marks to charity. By convicting Mr. Somm, the court appears to be saying that Internet service providers in Germany are responsible for Internet content and must take affirmative steps to block access to objectionable material. The judge disagreed with the defendant's attorney's argument that it was technically impossible to filter out all such material and said that CompuServe had let "protecting the young ... take second place to maximizing profits." The case sets the precedence of prosecuting a commercial online service for material it did not produce.
- *Loudoun v. Board of Trustees of Loudoun County Library, 1998 WL 164330 (E.D.Va.)*. In late 1997, the Loudoun County Library Board voted to require site-blocking software on all library computers to block "child pornography", and obscene material (hard core pornography)", and other materials deemed harmful to juveniles by Virginia statutes. The judge agreed with the plaintiffs that content-based site blocking was too broad to protect First Amendment rights and therefore unconstitutional as applied.
- *U.S. v. Hilton, 1998 U.S. Dist. LEXIS 5007, 1008 WL 167255 (D.Me.)*. In this case, the defendant challenged the constitutionality of 18 USC § 2252, as it included "computer or computer generated" images that are "or appear to be, of a minor engaging in sexually explicit conduct: in its definition of child pornography. The court found the definition to be overbroad, as it could include pornographic depictions of adults who appear youthful and thus would no longer fit the definition of minors.
- *Urofsky v. Allen, 1998 U.S. Dist. LEXIS 2139, 1998 WL 86587 (E.D. Va.)*. On 26 February 1998, the court found a Virginia statute prohibiting state employees from accessing sexually explicit materials on-line to be unconstitutional. The court held that sexually explicit material may contain information that could benefit the public, it is protected by the Constitution.

2.4.4 Privacy Issues

The Electronic Communications Privacy Act prohibits online service providers from disclosing subscriber information for use in a criminal investigation without a court order or the consent of the subscriber. Senior Chief Petty Officer Timothy R. McVeigh was dismissed from the Navy after investigators found that he had violated the policy against homosexual conduct in the military. On January 15, 1998, McVeigh filed suit against the U.S. Navy, claiming that Naval investigators illegally obtained confidential information about him from America On-Line where he had listed his marital status as "gay" on an Internet profile. On January 29, 1998 a Federal judge ordered the Navy to reinstate McVeigh. In June 1998, the Navy settled a civil suit with McVeigh, agreeing to grant him early retirement with full benefits and to pay his \$90,000 in legal costs.

2.4.5 Particularly Damaging or Dangerous Cases

While the next two cases have not yet set interesting legal precedents, they are examples of particularly damaging and dangerous abuse of communications systems.

2.4.5.1 Arrest Made for Interference in Radio.¹¹ On November 9, 1998 the FBI, Federal Aviation Administration and Federal Communications Commission announced the arrest of Kevin M. Kelly in Cumming, Georgia, for causing interference to radio frequencies used for communications between aircraft and the air traffic controller at the Atlanta Hartsfield International Airport. Kelly, an electronics engineer with experience in digital video satellite receiver design, was charged with four counts of violating Title 49, U.S. C §46308 (3), which prohibits knowingly interfering with the operation of a true light or signal used at an air navigation facility. Investigation began when the FAA reported sporadic and momentary radio frequency interference between aircraft and air traffic controller communications. Extensive investigation identified the point of origin as a subdivision in Cumming, Georgia. According to the press release, Kelly was upset with the noise from air traffic that flew over his house.

2.4.5.2 Disgruntled Employee Sets Off \$10 Million Computer "Bomb".¹² According to the two-count indictment returned January 28, 1998, Timothy Lloyd, a former computer network programmer for Omega Engineering Corporation intentionally caused irreparable damage to Omega's computer system by activating a "bomb" that permanently deleted all of the company's design and production software programs, resulting in a loss of at least \$10 million in sales and contracts. In addition, Lloyd is charge with interstate transportation of stolen computer equipment. Arrested by agents of the US Secret Service, Lloyd faces a maximum of five years in Federal prison on count one and 10 years on count two. Each count carries a maximum fine ranging from \$250,000 to twice the loss or gain from the crime. Lloyd could be ordered to make restitution. Lloyd's apparent motivation was that he had been fired. Omega is a manufacturer of high-tech measurement and control instruments used by NASA and the U.S. Navy.

2.5 NEW REGULATIONS

This section updates significant Federal Regulations passed since 1996 that affect information assurance. For purposes of this discussion, regulations are defined as follows:

*Regulations are rules and guidelines established by administrative agencies that, if derived from statutes, may carry the force of law, such as the income tax codes. Congress created administrative agencies, such as the Internal Revenue Service, to establish and enforce regulations. Most Federal regulations are published in the Code of Federal Regulations. Regulations may apply to the general public, business entities, and the enforcing agency. States may create their own regulations.*¹³

¹¹ "Arrest of Kevin M. Kelly," FBI Atlanta, Georgia, November 9, 1998 (http://www.fcc.gov/Bureaus/Compliance/News_Releases/1998/nrci8027.html).

¹² "Former Chief Computer Network Program Designer Arraigned for Alleged \$10 Million Computer 'Bomb,'" Department of Justice Press Release, 2 February 1998 (<http://www.usdoj.gov.criminal.cybercrime.lloydpr.htm>).

¹³ Elias and Levinkind, *Legal Research*, pp. 6/40-41.

On September 16, 1998, Vice President Gore announced a new Federal policy on the export of encryption removing export controls for "56-bit DES and equivalent" encryption hardware and software and removing key recovery clauses from export regulations. While it is obvious that such encryption in the hands of criminals could be devastating, the encryption was already available in overseas markets. The motivating force behind export control changes was an attempt to strike a balance between law enforcement interests and US businesses' ability to compete in international markets.

The US Department of Commerce Bureau of Export Administration responded with an interim rule amending the Export Administration Regulations, codified at 15 CFR Parts 730-774. The Bureau of Export Administration's summary matrix that describes the new provisions is quoted as follows:¹⁴

1. *Release up to "56 bit DES and equivalent" hardware and software. Hardware and software exports of up to "56 bits DES and equivalent" products will be eligible for license exception treatment to all users and destinations (except the seven State supporters of terrorism) after a one-time technical review. No further key recovery plans or renewals of existing key recovery plans are required. This release includes up to 56 bit DES, RC2, RC4, RC5 and CAST. Products with asymmetric key sizes up to 1024 bits will be permitted. Semi-annual post-facto reporting of end users for non-mass market exports to military and government end-users will be required.*

2. *Relax requirements for Key Recovery products*

Remove from the regulations the requirement to name and review key recovery agents for exports of key recovery products. Require post-facto reporting of key recovery agents and the end users of key recovery products (currently semi-annual). Supplement 5 (Key Recovery Agent Criteria) will be removed from regulations.

3. *Sectors*

Semi-annual post-facto reporting is required within each sector.

U.S. Subsidiaries: Approve exports of any encryption with any key length, with or without key recovery, to subsidiaries of U.S. companies (defined in Commerce regulation) world-wide (except the seven state sponsors of terrorism) under license exception, for the protection of internal business operations. This policy will also extend favorable treatment, to "strategic, partners" under license.

Insurance Companies: Treat insurance companies like banks and securities firms by adding them to the definition of "financial institution." The result is license exception treatment to institutions headquartered in nations listed in the recent amendments to the EAR relating to banks and financial institutions (63 FR 50156).

¹⁴ The primary Internet information source for the Bureau of Export Controls is <http://www.bxa.doc.gov>, through which one can also access Export Administration Regulations. The interim rule can be found at <http://bxa.fedworld.gov/whatsnew.cgi/encrypt>.

Health/Medical: Permit the export under license exception of any encryption with any key length, with or without key recovery, to organizations in the strictly defined health and medical sectors (see attached definitions) located in the nations listed in the banking regulation. Exports outside the country list found in the banking regulation receive a policy of approval under Encryption Licensing Arrangements (ELAs), recognizing that certain destinations may be denied on foreign policy or other grounds. The EAR will exclude biochemical firms, pharmaceutical firms and military agencies from eligibility for the license exception. Exports to such end users are possible under individual license.

On-Line Merchants: The EAR will permit license exception treatment for the export of client-server applications (e.g., SSL) and applications tailored to on-line transactions, with any encryption algorithm and with any key length and with or without key recovery, to on-line merchants (see attached definitions), located in the country list found in the banking regulation. Exports would be limited to those that facilitate secure electronic transactions between merchants and their customers. Exports outside the country list found in the banking regulation receive a policy of approval under ELA, recognizing that certain destinations may be denied on foreign policy or other grounds. Foreign merchants (non-US owned and controlled) that sell items and services controlled on the U.S. munitions list are excluded from this policy. For merchants having separate business units, only those business units selling munitions items are excluded from this policy of approval and license exception.

4. Recoverable Products

Permit exports, under Export Licensing Arrangements, of recoverable products (see attached definitions) to foreign commercial firms for internal company proprietary use, only (i.e. not sold for individual use) that are located in the following countries:

- 5. Austria, Australia, Belgium, Canada, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Luxembourg, The Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, and the United Kingdom.*
- 6. Anguilla, Antigua, Argentina, Aruba, Bahamas, Barbados, Brazil, Dominica, Ecuador, Greece, Hungary, Kenya, Monaco, Poland, Seychelles, St. Kitts and Nevis, St. Vincent/Grenadines, Trinidad and Tobago, Turkey and Uruguay.*

In addition, for those commercial firms headquartered in countries listed in 1 above, further permit exports, ELAs, of recoverable products to their foreign subsidiaries for internal company proprietary use in all destinations except the seven countries identified as State supporters of terrorism.

For both 1 and 2 above, this policy of approval excludes those commercial firms or separate business units of commercial firms engaged in the manufacturing and distribution of products or services controlled on the U.S. Munitions List. Service providers are also excluded from this policy. Semi-annual post export reporting of end users is required. Exports to those end users and countries not listed under this policy are possible under Validated Licenses or Export Licensing Arrangements on a case-by-case basis.

2.6 EXECUTIVE ORDER 13103¹⁵

Executive Order 13103 was written in support of the international effort against software piracy. Obligations levied by the Order are quoted as follows:

Section 1. Policy. It shall be the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of Federal law, including the Copyright Act.

(a) Each agency shall adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.

(b) Each agency shall establish procedures to ensure that the agency has present on its computers and uses only computer software not in violation of applicable copyright laws. These procedures may include:

- (1) preparing agency inventories of the software present on its computers;
- (2) determining what computer software the agency has the authorization to use;
- and
- (3) developing and maintaining adequate recordkeeping systems.

(c) Contractors and recipients of Federal financial assistance, including recipients of grants and loan guarantee assistance, should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. If agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors or recipients may affect the integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law.

(d) Executive agencies shall cooperate fully in implementing this order and shall share information as appropriate that may be useful in combating the use of computer software in violation of applicable copyright laws.

Section 2. Responsibilities of Agency Heads. In connection with the acquisition and use of computer software, the head of each executive agency shall:

¹⁵ Executive Order 13103, *Computer Science Software Pricing*, October 1, 1998 (<http://www.pub/whitehouse.gov>).

- (a) ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency's computers;
- (b) utilize performance measures as recommended by the Chief Information Officers Council pursuant to section 3 of this order to assess the agency's compliance with this order;
- (c) educate appropriate agency personnel regarding copyrights protecting computer software and the policies and procedures adopted by the agency to honor them; and
- (d) ensure that the policies, procedures, and practices of the agency related to copyrights protecting computer software are adequate and fully implement the policies set forth in this order.

Section 3. Chief Information Officers Council. The Chief Information Officers Council ("Council") established by section 3 of Executive Order No. 13011 of July 16, 1996, shall be the principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software. The Council shall provide advice and make recommendations to executive agencies and to the Office of Management and Budget regarding appropriate government-wide measures to carry out this order. The Council shall issue its initial recommendations within 6 months of the date of this order.

Section 4. Office of Management and Budget. The Director of the Office of Management and Budget, in carrying out responsibilities under the Clinger-Cohen Act, shall utilize appropriate oversight mechanisms to foster agency compliance with the policies set forth in this order. In carrying out these responsibilities, the Director shall consider any recommendations made by the Council under section 3 of this order regarding practices and policies to be instituted on a government-wide basis to carry out this order.

Section 5. Definition. "Executive agency" and "agency" have the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

Section 6. National Security. In the interest of national security, nothing in this order shall be construed to require the disclosure of intelligence sources or methods or to otherwise impair the authority of those agencies listed at 50 U.S. 401a(4) to carry out intelligence activities.

Section 7. Law Enforcement Activities. Nothing in this order shall be construed to require the disclosure of law enforcement investigative sources or methods or to prohibit or otherwise impair any lawful investigative or protective activity undertaken for or by any officer, agent, or employee of the United States or any person acting pursuant to a contract or other agreement with such entities.

Section 8. Scope. Nothing in this order shall be construed to limit or otherwise affect the interpretation, application, or operation of 28 U.S.C. 1498.

2.7 CONCLUSIONS

The legal system continues to refine the way it responds to cybercrime. The need to modify laws and regulations arises as cases are prosecuted and technologies used in committing crimes evolve. Since 1996, there has been little change in the statutes.

SECTION 3 POLICY AND DOCTRINE

3.1 INTRODUCTION

This section presents the various policy decisions, analyses, and publications over this past year responding to the more visible threats of unconventional attack.

In the Report of the President's Commission on Critical Infrastructure Protection (PCCIP) in October 1997, the Commission addressed various forms of terrorism, which the United States faces, and the much-changed approaches demanded in the post Cold War environment. In two decision directives, the President addressed the range of terrorist acts, the spread of and availability of technology for producing and using weapons of mass destruction, assaults on our critical infrastructures, and the emergence of cyber-attacks. The directives set up new policy structures for government work on implementation. The emerging mechanisms of these organizations are furthering interagency cooperation and coordination, and slowly building a new government-industry partnership. Finally, the Vice-President presented the Administration policy on use and export of encryption tools.

Within DOD several new policy directives on information assurance and the safe use of cyberspace set the course for developing doctrine and varied implementation directions.

The first was the publication of the DOD Directive on the Critical Asset Assurance Program. It requires identification and assessment of the vulnerability of all infrastructure capabilities needed to support vital Defense missions across the full range of military operations. The second was the on-going development of a new directive on Information Assurance and its implementing subordinate publications; these will replace an outdated approach to information security with the unified security posture of IA. A key development of directives into doctrine emerged with the publication of the new Joint Doctrine for Information Operations, which has updated rapidly changing concepts for offensive and defensive operations. It addresses varied IO responses across the spectrum of operations – from peace through crisis to full information warfare.

Many organizations in DOD – the Joint Staff, the CINCs, key agencies such as DISA and DARPA, and the Services – have responded with appropriate architectural plans, technological fixes, education and training as well as research and development initiatives to fulfill strategic and doctrinal mandates.

CONTENTS

National-Level Initiatives

- Report of the PCCIP
- National Security Strategy
- PDD 62/63

DOD Initiatives

- Office of the Secretary of Defense
- Joint Staff
- Licensing and Certification
- Critical Asset Assurance
- Web Security

The Chief Information Officer (CIO)

Encryption Policy

Conclusions

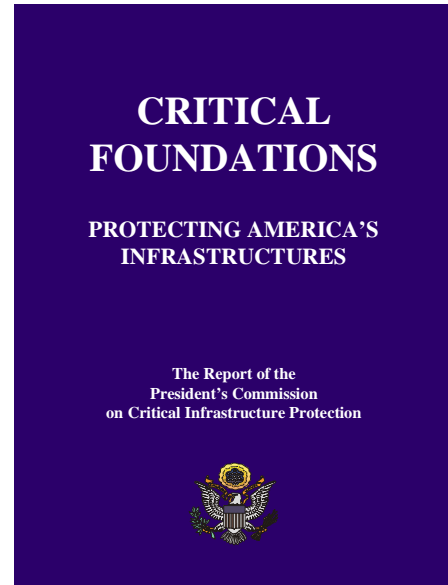
3.2 REPORT OF THE PCCIP

As mentioned in the 3rd edition (September 1997), President Clinton issued Executive Order (EO) 13010 on July 15, 1996, which established the PCCIP. After research by numerous subgroups, continuous review of their products, five public meetings to gather information from all sources, especially private providers of the eight key infrastructure services, the Commission published its report "Critical Foundations: Protecting America's Infrastructures" in October 1997.

The report notes the "blurring of traditional boundaries and jurisdictions" – between the public and private sectors, between military forces and external infrastructures, and between foreign and domestic policy. It clarifies the role of the federal government in defense against cyber threats as "collecting information about tools that can do harm, conducting research into defensive technologies, sharing defensive techniques and best practices ... and engaging the private sector by offering expertise to facilitate protection of privately owned infrastructures."¹ The report noted, however, that "protection of our infrastructures will not be accomplished by a big federal project. It will require continuous attention and incremental improvement for the foreseeable future."² These same observations have been circulating for several years in Defense channels as the Defense Science Board noted the need to implement many cheap but effective "quick fixes" with follow-on remedies planned to "raise the bar."³

The report provides a substantial listing of the many threats to the infrastructure services and equipment, including:

- Natural events and accidents
- Blunders, errors, and omissions
- Insider threats
- Recreational hackers
- Criminal activity
- Industrial espionage
- International terrorists
- National intelligence organizations
- Information warfare activities.



¹ The President's Commission on Critical Infrastructure Protection, *Summary Edition of Critical Foundations: Thinking Differently*, Washington D.C., October 1997, p. 1.

² PCCIP, *Summary Edition*, p. 1.

³ Defense Science Board, p. 6-21f.

The Commission pointed out that the United States as a nation aids and abets the problem because "the general public seems *unaware* of the extent of the vulnerabilities in the services that we all take for granted, and that within government and among industry decision-makers, *awareness is limited*."⁴ The observation is consistent with the scarcity of articles in the general press about these vulnerabilities and the relatively low number of IA or security courses provided in academia for management and computer science students.

Because the rules have changed in cyberspace – national borders are no longer relevant – the PCCIP emphasizes that new thinking is required to protect the nation's infrastructures from attacks. These computer network attacks (CNA) are inevitable as the "vulnerabilities are increasing steadily while costs associated with effective attack continue to drop."⁵

The Commission's recommendations were focused into five major areas:

- The need for a broad program of awareness and education
- Infrastructure protection through industry cooperation and information sharing
- Reconsideration and modernization of laws related to infrastructure protection
- A revised program of research and development
- A national structure [which has evolved with the PDD 63 creation of the CIAO and NIPC].

The report detailed several key technical areas for cooperation and sharing:

- A request for the National Institute for Standards and Technology (NIST) and the National Security Agency (NSA) "to provide technical skills and expertise required to identify and evaluate vulnerabilities in the associated networks and control systems."⁶
- A recommendation to share information and techniques related to risk management, especially numerical techniques like probabilistic risk assessments (PRA studies). These will help to "prevent attacks, mitigate⁷ damage, quickly recover services, and eventually reconstitute the infrastructure."
- Initiate several immediate remedies – "isolation of critical control systems from insecure networks by disconnection or adequate firewalls; adoption of best practices for password control and protection or installation of more modern authentication mechanisms; and providing for individual accountability through protected action logs or the equivalent."⁸

The Commission summary recommends structures for government-private sector partnership, a concept that has found expression in DOD as the National Information

⁴ PCCIP, *Summary Edition*, p. 5.

⁵ PCCIP, *Summary Edition*, p. 6.

⁶ PCCIP, *Summary Edition*, p. 7.

⁷ PCCIP, *Summary Edition*, p. 7.

⁸ PCCIP, *Summary Edition*, p. 7.

Assurance Partnership (NIAP). The Commission recognizes the realities of the Information Age, the new environment in the post Cold War era when the lines between enemies and allies are less clearly defined, and technology moves so fast providing both promise and danger. The bottom line is noteworthy as the Commission observes that they "do not so much offer solutions as directions – compass headings that will help navigate through a new geography and ensure the continuity of the infrastructures that underpin America's economic, military, and social strength."⁹

One Administration initiative that is under consideration to address the awareness finding of the PCCIP is a plan to allocate \$20 million in FY-00 to form a "Cybercorps" which will be modeled on the Reserve Officer Training Corps. The allocation would go to tuition assistance for funding undergraduate computer specialists in American universities; the return would be a promise of five years government service after graduation. The current government plan notes:

While [the 100 students it would finance in the first class] would hardly make a dent in the nation's information technology worker deficit, the 100 would be on the vanguard of a movement to tightly integrate and secure federal information systems across the government. Rather than just moving into a government position for a five-year stint after graduating, the Cybercorps would rotate among the federal agencies to get hands-on experience with many high-profile projects. This not only increases the attractiveness of the job, it also gives the government a cadre of highly trained IT professionals that view federal computer systems as individual nodes of a whole network – all the better to reduce redundancy, improve integration and secure the pathways between them.¹⁰

3.3 "A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY"

This annual "report on the national security strategy of the United States," was sent to the Speaker of the House of Representatives on October 29, 1998, as required by the Goldwater-Nichols DOD Reorganization Act of 1986. This report details the Clinton Administration national security strategy, which guides the efforts of the DOD, the Department of State, the National Security Council, Department of Commerce, Department of Justice, and other the federal government agencies involved in national security. Early on, the report notes that "success in countering ... varied threats requires an integrated approach that brings to bear all the capabilities and assets needed to achieve our security objectives – particularly in this era when domestic and foreign policies are increasingly blurred."¹¹

⁹ PCCIP, *Summary Edition*, p. 9.

¹⁰ Hess, Pamela, "First Cybercorps Class Would Add 100 IT Workers" in *Defense Information and Electronics Report*, Washington, DC: Inside Washington Publishers, December 11, 1998, pp. 1, 8.

¹¹ The White House, *A National Security Strategy for a New Century*, Washington D.C., October 1998, p. 7.

It notes further:

Our military power and national economy are increasingly reliant upon interdependent critical infrastructures – the physical and information systems essential to the operations of the economy and government.... It has long been the policy of the United States to assure the continuity and viability of these critical infrastructures. But, advances in information technology and competitive pressure to improve efficiency and productivity created new vulnerabilities to both physical and information attacks as these infrastructures become increasingly automated and interlinked.... Any interruption or manipulation of these critical functions must be brief, infrequent, manageable, isolated and minimally detrimental to the welfare of the United States.¹²

This national strategy drives the Quadrennial Defense Review, which last occurred in 1997 (results published in May 1997), the annual Defense Program Guidance (DPG), and the DOD Program Objective Memorandums (POMs). As would be expected, on the path from this general strategy to the DPG and POMs, the focus becomes much more specific. The strategy also ties together the thrust of the report of the PCCIP and PDDs 62/63.

Finally, it indicates that the National Infrastructure Protection Center (NIPC) will "coordinate the federal government's response to an incident, including mitigation, investigation and monitoring reconstruction efforts."¹³ This coordination role and the procedures to implement the role remain to be fully defined and worked out through dealing with actual National Defense-related incidents.

3.4 PRESIDENTIAL DECISION DIRECTIVES

As a result of the findings and recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP), President Clinton issued two new directives designed to strengthen the Nation's defenses against terrorism and unconventional threats: Presidential Decision Directives (PDD) 62 and 63. These directives address the two major risks of the post Cold War era, weapons of mass destruction, and the growing vulnerability of modern infrastructures. Since the bombings in Oklahoma City and the World Trade Center, it has become a major concern of the Federal government how to protect the country against new and more focused attacks on its internal centers. There has been a growing realization of our national dependence on various infrastructures that form the backbone of services for modern American society.

3.4.1 PDD 62

Approved on May 22, 1998, PDD-62 addresses the national problem of countering terrorism in all its varied forms. It highlights the growing range of unconventional threats that we face as a nation, including newer forms of more familiar chemical, radiological, and biological weapons, and the emergence of "cyber terrorism." The directive creates a new

¹² The White House, p.20.

¹³ The White House, p.20.

and more systematic approach to defending against them. The first step is to create within the Executive Office of the President a new National Coordinator (for Security, Infrastructure Protection and Counter-Terrorism). This official is responsible for coordinating the government and private partnership, which will assure the national and economic security, as well as the well being of its citizenry. The new National Coordinator for Security, Infrastructure Protection and Counter-Terrorism reports to the President through the National Security Advisor and when the NSC Principals Committee meets on security issues, he serves as a full member of that Cabinet-level committee. This new "Security Czar" will coordinate with other presidential advisors in their area of expertise to address key infrastructure support issues, especially: the Director of the Office of Scientific Technology and Policy; and cabinet secretaries in their roles as lead agencies for various sectors. The new national IA structure is shown in Exhibit 3-1.

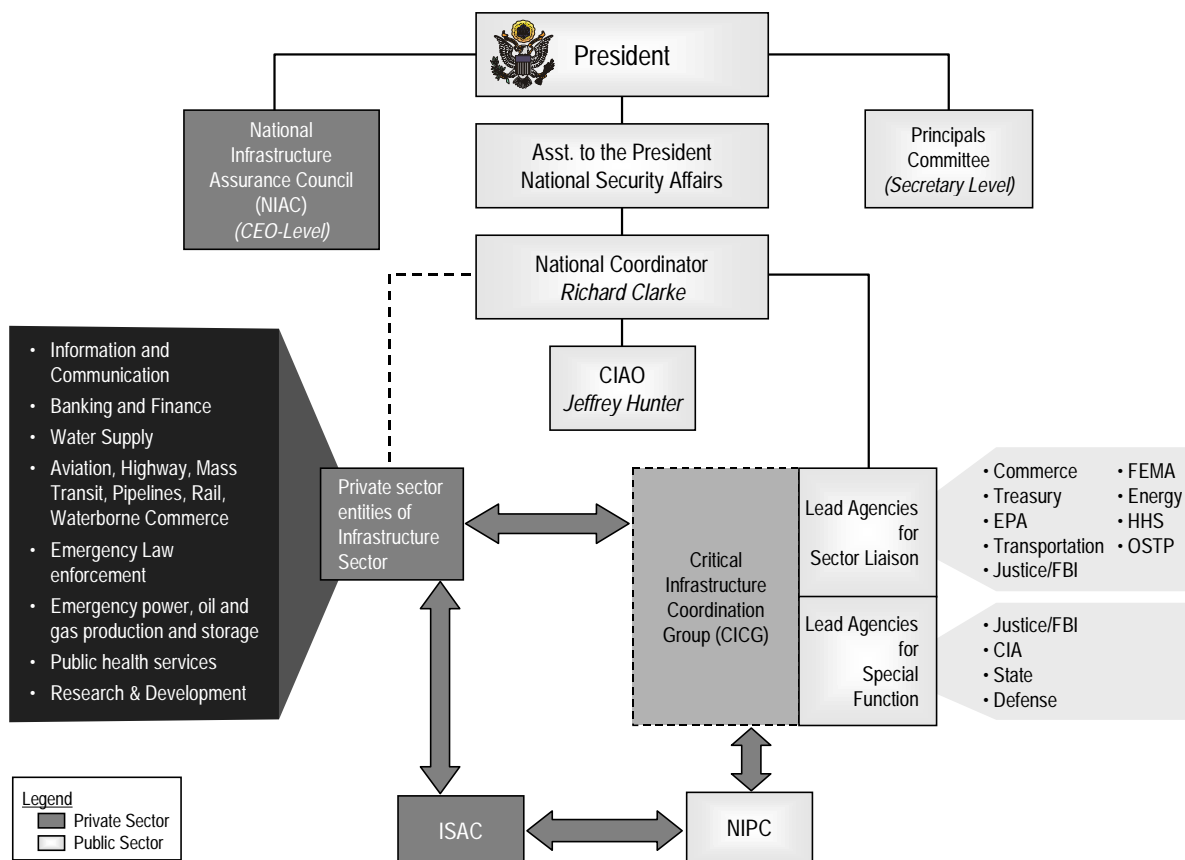


Exhibit 3-1. National IA Structure

3.4.2 PDD 63

Also released on May 22, 1998, PDD-63 focuses specifically on protecting the Nation's critical infrastructures from both physical and "cyber" attack. These attacks may come from foreign governments, foreign and domestic terrorist organizations, and foreign and domestic criminal organizations.

The National Coordinator oversees the efforts of the government in formulating the Federal Critical Infrastructure Protection (CIP) Plan and coordinating the National Plan for CIP with the private sector. The new national security structure for CIP brings together the efforts of the National Infrastructure Assurance Council, the Critical Infrastructure Coordination Group, the National Security Telecommunication Advisory Committee, the Manager of the National Communications System, and lead cabinet agencies for special functions and infrastructure industries. The infrastructure sectors and their respective federal lead agencies are:

<i>Infrastructure Sector</i>	<i>Lead Federal Agency</i>
Banking and Finance	Department of Treasury
Transportation	Department of Transportation
Electric and Gas & Oil Pipelines	Department of Energy
Information/Communications	Department of Commerce
Government Services	General Services Administration
Fire and Other Emergency Services	Federal Emergency Management Agency
Public Health Services	Department of Health and Human Services
Water Supplies	Environmental Protection Agency

The proponents of special functions are:

<i>Special Function</i>	<i>Lead Federal Agency</i>
Law Enforcement and Internal Security	Department of Justice
National Defense	Department of Defense
Intelligence	The Central Intelligence Agency
Foreign Affairs	Department of State

The directive set up the Critical Infrastructure Assurance Office (CIAO) under the Department of Commerce and the National Infrastructure Protection Center (NIPC) under the sponsorship and guidance of the Federal Bureau of Investigation (FBI). The directive lays out the framework for a voluntary Information Sharing and Analysis Centers (ISACs), which will help to coordinate information and efforts toward addressed CIP issues.

3.5 OFFICE OF THE SECRETARY OF DEFENSE (OSD) INITIATIVES

Throughout 1998 the Secretary (SecDef) and especially the Deputy Secretary of Defense (DepSecDef) have been active in issuing focused directives, especially memos to address immediate IA concerns. On January 30, 1998, the DepSecDef published a memo, which directed the implementation of a Defense Information Assurance Program (DIAP). He specified that initial plans, processes, procedures, and staffing should be completed in 90 days and full operational capability reached in six months. In conformity with the national direction on Information Technology management presented in the ITMRA,¹⁴ the DepSecDef charged the DOD Chief Information Officer with overseeing the DIAP and

¹⁴ P.L. 104-106.

reviewing the budget process. The memo also spelled out roles and responsibilities of many DOD officials and components:

- The DOD CIO Council will expand its activities to meet DOD IA program requirements.
- The Senior DIAP Steering Group composed of representatives from the Services, Joint Staff/J6, DISA, and NSA will provide strategic direction and guidance to the DIAP staff.
- The National INFOSEC Manager (the Director, National Security Agency) and the Director DISA will serve as advisors to the CIO on IA and the Defense Information Infrastructure respectively.
- The Joint Staff, the Services, DISA, and NSA will develop detailed implementation plans for the DIAP.
- The CIO will tailor Five Year Defense Plans (FYDPs), Defense Planning Guidance, and Program Objective Memorandums (POMs) to meet IA responsibilities
- The Director, DISA will develop and codify DOD IA operational "best practices" for developing doctrine and performance standards.
- The Joint Staff will develop performance-based metrics for periodic assessment of IA operational readiness of all combat, combat support, and combat services. These measures will be integrated into the operational readiness reporting (OPREP) system and existing DOD policy.¹⁵

On February 19, 1998, the DepSecDef published another memo directing all components to develop Cyber Intrusion Detection Plans. The staff of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) as the Department CIO provided a comprehensive assessment and report on the Department –wide responses.

3.6 JOINT PUBLICATION 3-13

The Joint Staff published Joint Pub 3-13, *Joint Doctrine for Information Operations*, on 9 October 1998, which codifies, for the Warfighter, how IO will serve as an integral part of all military operations. Its relationship to other operations is clarified in its links to the Crisis Action Planning Process, the Joint Operations Planning and Execution System, and Annexes C and K of the Joint OPORD/CONPLAN/OPLAN of any Joint Force.

First, JP 3-13 formalizes the close ties between information and the management of violence through physical assets. Throughout the publication, there is a strong and constant emphasis on the relationship of IO to military missions and objectives – the Warfighter.

¹⁵ DepSecDef Memo, *Management of the Department of Defense (DOD) Information Assurance (IA) Program*, January 30, 1998.

Second, it addresses more directly the issues of offensive IO as an adjunct of defensive IO. When the publication was first circulated, the trade press noted offensive IO with a buzz. The notion of computer network attack (CNA) has long connoted the work of "bad hackers" and subversives. Previous editions of 3-13 did prepare the way for introduction of this idea by addressing the notions of Information Warfare (IW) although most of the prior discussions were an extension of C2W, EW, and jamming (mostly communications oriented). With so much of crisis and warfare decision-making depending on information systems and networks, the time was right to advance the concept of CNA as a legitimate means of warfare.

Although US military forces temper the means of warfare with considerations of the laws of armed conflict, domestic and international law, national treaties, and rules of engagement, various real and potential adversaries of the US have made clear their intention to use all means, including CNA. Many entities throughout the world, especially independent computer experts, publicize their varied intentions and capabilities, as this entry in *Wired News*, the on-line version of *Wired* magazine, recently noted:

A global group of 24 hackers and crackers spent Monday night probing, mapping, and preparing to attack computer networks owned by the government of Iraq. Quoting at one point from the Declaration of Independence, Steve Stakton, a member of the seven-year-old Legions of the Underground group, called for a concerted one-week cracking campaign against Iraq.

"Iraq has treated human rights issues as poorly as China has," said Stakton in a meeting of the group that was held Monday night on Internet Relay Chat. "We need to carry out what the government won't, and can't, do." Stakton, 24, quoted from the group's mission statement: "We are ready to commence, and take [part] in electronic warfare if requested."

... The Legions said that the attack was a legitimate act of protest against a rogue dictator. "It's a crime in itself to build weapons of mass destruction when the children of the country are starving," said a group member who goes by the name "kInGbOnG." [sic]

In recent months, Legions of the Underground, whose members are largely in their 20s, has launched numerous attacks against China to draw attention to that nation's human-rights record. Last July, in a demonstration of their technical abilities, members claimed to have remotely moved a satellite dish owned by Time Warner Cablevision. The company confirmed a security breach in that incident.¹⁶

¹⁶ Glave, James, "Crackers Set Sights on Iraq" in the *Wired News Update*, 30 December 1998 found at URL: http://www.wired.com/news/print_version/politics/story/17074.html?wnpg-all. Source originally found from InfoSec News (ISN) bulletin board. Although the Legions called off this approach after opposition from several hacker groups, the threat of "private" enactment of foreign policy is still real.

Third, there is a full chapter detailing the IO organization, a typical Joint Information Operations Cell. In many ways it parallels the classic notion of a Crisis Action Team or a Battle Staff. The Cell is normally headed up by an IO officer from J-3 with supporting representatives of: the J-2, J-4, J-5, J-6, J-7 functions; the Public Affairs Office, the Staff Judge Advocate (for legal questions); Civil Affairs; Electronic Warfare, Joint PSYOPS Task Forces, Joint Special Operation Task Forces, Special Technical Operations, and other traditional C2W players.

3.7 CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION (CJCSI) 6510.01B, CHANGE 1

To illustrate the fast pace of technological change and its impact on policy and doctrine, the Chairman of the Joint Chiefs of Staff published a significant Change 1 in August 1998 to the CJCSI 6510.01B, *Defensive Information Operations Implementation*, originally published as recently as August 1997. This contrasts with other directives and manuals, which still date from the 1970s and 1980s. In that era the main emphasis of security directives included in order of importance, confidentiality, integrity, and authenticity. In addition to laying out new priorities, policies, and procedures, the instruction re-emphasizes many familiar disciplines of those early decades, which are still valid for the new threat environment.

Reflecting the latest change in doctrine, the first policy paragraph states:

Information, information-based processes, and information systems such as command, control, communications, and computer (C4) systems; weapons systems; and information infrastructures used by US military forces, will be protected relative to the value of the information contained therein and the risks associated with its compromise or loss.¹⁷

Complementing JP 3-13 discussed above, this instruction addresses more directly the issues of defensive IO as an integral part of IO. The instruction addresses the four interrelated processes of defensive IO – processes to: protect information and information systems; detect attacks or intrusions; restore services and mitigate the effects of incidents; and respond. These processes are in full agreement with other OSD, Joint, and Service publications in terms and tone.

Finally, the most significant change was the result of several lessons learned from Solar Sunrise – the need for an effective and efficient incident and vulnerability reporting system. The new reporting structure has four levels: Global, Regional, Service and Local. All local control centers (whether in operational locations – OPLOCs, Intelligence, C4 or Law Enforcement facilities at bases, camps, posts, and stations) will report upward through either or both of the two functional/command chains (see Exhibit 3-2):

¹⁷ CJCSI 6510.01B CH1, 26 August 1998, para 1a.

- DISA Regional Operations and Security Centers (ROSCs), many of which are collocated with warfighting CINCs.
- Service/Regional CERTs or CIRTs, some of which are collocated with Headquarter staffs of the Services.

Both of these levels will report upward to the DISA Global Operations and Security Center (GOSC). These reports are consistent with the traditional network management process for reporting network outages. This reporting process augments other operational reporting through the chain of command, such as OPREPs.

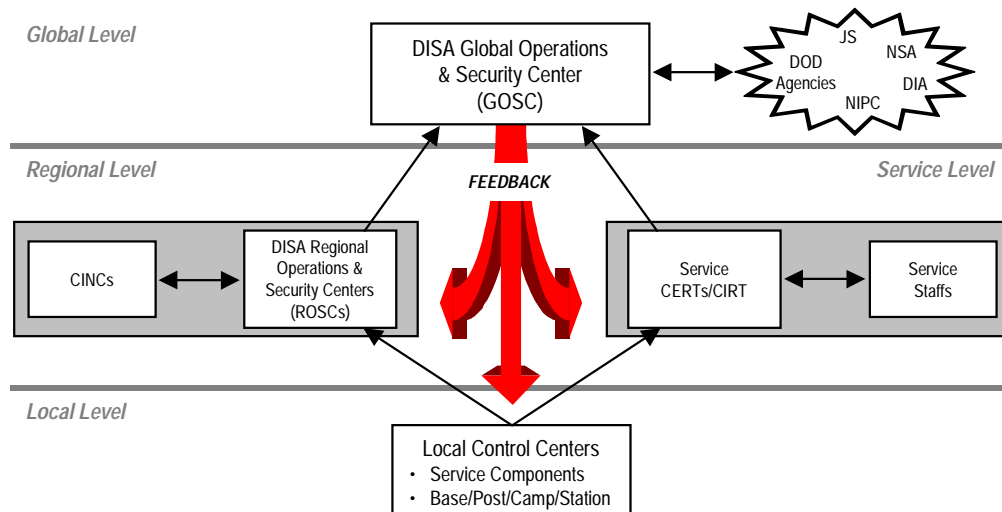


Exhibit 3-2. Incident Reporting Structure

At the global level, the GOSC will notify and coordinate with the Joint Staff, the NSA National Security Operations Center (NSOC), Information Protection Cell (IPC), and the National Infrastructure Protection Center (NIPIC, mentioned earlier). The GOSC will assure that analysis and correlation of events and incident data, as well as coordination occurs at all levels. Detection, analysis, and correlation can originate in manual or automated tools, such as the Joint Intrusion Detector System (JIDS). The military coordination chain will ensure notification of all military organizations that need the pertinent information. The Joint Staff will provide briefings to National Command Authorities through the Chairman's role as military advisor. The NIPIC will provide mutual threat assessments, warnings and indications, vulnerability advisories, law enforcement investigations, and response liaison to the FBI.

While the upward transmission of vulnerability and incident information is traditional to military operations, the reverse flow is equally important. The Security Incident Support Team (ASSIST) will implement a comprehensive distribution for alerts and countermeasures using the Information Assurance Vulnerability Alert process. The publication of a secure Website for this information will require acknowledgement of receipt within a nominal 5-day period. Then every local control center will assess the impact of their alert and report compliance through the normal chain of command within a nominal 30-day period.

In addition to these reporting procedures, the Joint Staff has been developing and staffing an instruction on declaring Information Operations Conditions (INFOCONs) analogous to the DEFCONs that already exist in standard DOD practice.

3.8 LICENSING AND CERTIFICATION OF COMPUTER PERSONNEL

The Joint Staff-chaired Military Communications Electronics Board (MCEB) *IA Roadmap*,¹⁸ addressed 16 key issues with a combination of general guidance and specific directions. One key area in which it provided detailed procedures was licensing and two types of certification for personnel working with DOD computers. Specific deadlines for licensing different classes of computer personnel were set as well as certification requirements. Later, ASD (C3I) published a memo¹⁹ on training and certification which formally ratified the MCEB guidance, provided additional guidance, and noted that the Undersecretary of Defense for Personnel and Readiness was asked to address overall training and professionalization needs.

3.9 CERTIFICATION AND ACCREDITATION OF SYSTEMS AND NETWORKS

The MCEB recommended on March 20, 1997 that all C/S/As begin to implement the current draft of the "Defense Information Technology Security Certification and Accreditation Process (DITSCAP)." The process received formal approval with the issuance of DODD 5200.40 on December 30, 1997. The MCEB directed that the C/S/As immediately implement this DODD since the well-defined DITCAP requirements have now replaced the interim network requirements. Additionally, they directed that all Secret and Below Interoperability (SABI) implementations be approved by the end of fiscal year 1998, or be disconnected from the SIPRNET. Finally, the Roadmap stipulated numerous requirements such as intrusion detection capabilities, virus protection, security checklists, and installation of firewalls or filtering routers.

3.10 CRITICAL ASSET ASSURANCE PROGRAM (CAAP) AND THE DOD CRITICAL INFRASTRUCTURE PROGRAM

On January 20, 1998, OSD updated the previous DOD Directive on the CAAP. This directive expanded the already existing "requirement to identify Critical Assets and assure their integrity, survivability, and capability to support vital DOD missions across the full range of military operations."²⁰ This policy provides for an integrated infrastructure vulnerability assessment and assurance program using risk management principles.

This directive acknowledges the need for "providing ... protection from all hazards, mitigating the effect of their loss or disruption; and planning for timely restoration or

¹⁸ Military Communications Electronics Board (Chaired by Joint Staff/J6), *IA Roadmap*, released December 1997.

¹⁹ ASD (C3I) memorandum, *Information Assurance (IA) Training and Certification*, 29 Jun 98. Signed by both ASD(C3I) and USD(P&A).

²⁰ DoDD 5160.54, Critical Asset Assurance Program (CAAP), January 20, 1998, para 1.3.

recovery."²¹ This reflects the DOD Defense in Depth strategy, which calls for "protect, detect, react."

An important recognition in the directive is that critical DOD equipment, facilities, and services depend on international and national infrastructures many of which are operated, maintained, and managed by other countries, other government agencies, and the private sector. It also addresses the need for DOD officials to plan for emergency preparedness and provide varied kinds of assistance in case of natural disaster, physical or technical attack, or other emergencies.

This policy mandates an integrated asset and infrastructure vulnerability assessment and assurance program. In order to work with other government bodies and private industry to provide for national security emergency preparedness, the directive provides for the ASD(C3I) and the Under Secretary of Defense (USD) for Policy to establish and support the Critical Infrastructure Protection Working Group (CIPWG). The ASD(C3I) and the USD(P) co-chair this working group.

Finally, to achieve these objectives, the directive assigns roles and responsibilities for these program requirements. It establishes the Secretary of the Army as the DOD Executive Agent for the CAAP. The Executive Agent is to coordinate the program with the Services, DOD agencies, and other components. The Director, Defense Security Service (DSS)²² will assist by conducting on-site surveys with vulnerability analyses of physical and technical threats. The Intelligence Community (CIA, DIA, NSA, DSS, and FBI) will provide continuous analysis of hostile sources and support special operations to protect these Critical Assets. The Director, DISA will: provide for the assurance of the Defense Information Infrastructure (DII) and coordinate with the Office of the Manager of the NCS to identify critical assets in the NII; and coordinate the activities of all DOD Computer Emergency Response Teams (CERTs), as well as interface with other CERT-related activities (such as the NIPC, the Carnegie Mellon University CERT/CC®, and the still-to-be-defined Information Sharing and Analysis Center).

3.11 DOD POLICY ON WEB SECURITY

After the intrusions into Defense computers encountered during Solar Sunrise, all levels of command addressed the need for stringent remedies through both formal and informal actions. Many commanders and CINCs recognized the need to control the proliferation of Defense websites, avoid having information of intelligence value in page content, and limit technical entry points into the DII. Countering the need to exert greater control over publicly available websites are the many information advantages provided to military members performing their missions and the legitimate needs/rights of contractors, allies, and the general public.

²¹ DODD 5160.54, January 20, 1998, para 4.1.

²² Formerly the Defense Investigative Service (DIS).

In September 1998, DepSecDef Hamre called for a full top-to-bottom review of the contents of all DOD Webpages (and other Web security measures). He directed the CINCs, Services, and Defense Agencies to remove all references to individuals' personal data and sensitive operational matters. Moving this information to NIPRNET/SIPRNET with their better security controls serves the interests of efficiency and information availability for Defense personnel in performing their mission while denying our adversaries key indicators.

Finally, on December 7, 1998, the DepSecDef signed a memorandum promulgating as DOD policy the ASD(C3I) "Web Site Administration Policies & Procedures."²³ This publication defines the policy and responsibilities of all Defense officials who have oversight of DOD webpages and websites. It sets up the requirement for including websites in the standard process of security certification and accreditation, the Defense Information Technology Security Certification and Accreditation Program (DODD 5200.40, the DITSCAP).

The policy stipulates items that are inappropriate for public-access websites: any "For Official Use Only (FOUO)" designated information; analyses and recommendations regarding sensitive military operations, exercises, or vulnerabilities; personal information (such as SSANs, dates of birth, home addresses and telephone numbers, dependent information) about military and civilian personnel, especially those assigned overseas, to sensitive duties, or routinely deployable units; proprietary contractor information, trade secrets, certain commercial and financial information – in short, any OPSEC information or data considered to be private by the offeror.

Most significantly, the publication provides a major section on "Examples and Best Practices" which provides detailed guidance on content review, security, and access controls.

3.12 THE CHIEF INFORMATION OFFICER (CIO)

The Information Technology Management Reform Act of 1996 (also called the Clinger-Cohen Act)²⁴ directed all government departments and agencies to "establish goals for improving the efficiency and effectiveness of agency operations ... through the effective use of information technology." The key benefit of the act for DOD was its repeal of the cumbersome acquisition structures of the obsolete Brooks Act; it allows each agency to acquire commercial computer technology through its own planning mechanisms with only the final oversight of the Office of Management and Budget. The OMB Director was directed to:

- Oversee the financial impact of this decentralization
- "Encourage ... executive agencies to develop and use the best practices in the acquisition of information technology"
- Use performance-based and results-based management.

²³ Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence), November 25, 1998. Also available on the Internet at <http://www.defesnelink.mil/admin/about.html#WebPolicies>.

²⁴ P.L. 104-106, sec 5123

A significant mechanism to achieve the streamlining and control benefits envisioned by the Congress is the ITMRA provision that each Federal agency will have a Chief Information Officer (CIO). The CIO is to provide management coordination, oversight, and guidance for the agency on all aspects of procurement, operation, maintenance, and security of information systems. For DOD, the CIO is the ASD(C3I).²⁵

An example of a means used by the DOD CIO to provide guidance is the DOD CIO Help Desk. It serves as the whole Department's point of entry for any BPR/CIO questions or requests on Policy, Methodology, Security Issues, Tools, Training, Documentation, and Software.²⁶

Since CIOs and their staff cannot have knowledge of every aspect of this critical area, each is to have a CIO council. The DOD CIO Council parallels the Federal CIO Council (of which the DOD CIO is a member), which is the principal interagency forum to improve the design, modernization, use, sharing, and performance of Federal resources. The CIO Council's role includes: developing recommendations for IT management policy, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government for an information technology workforce.²⁷ It is to provide corporate advice on requirements, conditions, problems, and other issues of their organizations. The DOD CIO receives this information and other insights from the CIOs of the CINCs, the Services, and the Defense agencies, their respective staffs, and the staffs of other component C4I functions.

3.13 ENCRYPTION POLICY

Establishing an encryption policy is a very fine balancing act that will never gain the unanimous support of everyone traveling on the Information Highway. The opinion spectrum runs the gamut from Professor Dorothy Denning,²⁸ who advocates strong government control for law enforcement purposes, to the Electronic Freedom Frontier (EFF)²⁹ which advocates strong individual privacy rights attained through encryption. Setting a government encryption policy is indeed complicated by the necessity to mediate the following rights and needs:

²⁵ Information about the CIO provided at <http://www.c3i.osd.mil/>

²⁶ Information provided the CIO website at http://www.dtic.mil/bpr-helpdesk/dod_support/

²⁷ This statement for the Federal CIO (found at <http://cio.gov/>) describes the role of the DOD CIO Council.

²⁸ Professor Denning's statement of philosophy on encryption and anarchy can be found at <http://www.cs.georgetown.edu/~denning/crypto/Future.html>.

²⁹ The commentary of the release of the Administration policy on encryption (September 16, 1998) and the EFF philosophy on encryption and individual privacy can be found at http://www.eff.org/pub/Privacy/ITAR_export/1998_export_policy/HTML/19980916_policy.html

- Individual privacy which has been established through case law up to the Supreme Court
- The ability of American companies to sell encryption software that is truly competitive with foreign companies not limited by *their* governments
- The ability of law enforcement agencies to recover data from domestic terrorists and criminal organizations.

The Administration policy was presented and clarified further by a White House press conference on September 16, 1998 led by Vice-President Gore with representatives of the Departments of Justice, especially the FBI, Commerce, Defense, and the National Security Advisor. The current provisions as briefed by the Vice-President include:

- Exports of 56-bit DES and equivalent products (hardware and software) will be streamlined (under license exception). Requirements for key recovery plans are eliminated.
- Exports of unlimited-strength encryption products (with or without key recovery) will be streamlined (under license exception) in certain industries. The industry sectors are:
 - Subsidiaries of U.S. companies, worldwide (except those in seven terrorist nations)
 - Insurance companies for the same 45 countries, which were recently approved for crypto exports to banks and financial institutions
 - Health and medical organizations (including civilian government health agencies) in the same 45 countries (does not include biochemical/pharmaceutical manufacturers)
 - On-line merchants for client-server applications, in the same 45 countries, with the purpose of securing electronic transactions between merchants and their customers.
- Key Recovery products will continue to be exportable under license exception worldwide (except in the seven terrorist nations). Review of foreign key recovery agents is eliminated.
- Exports of "recoverable" products will be approved to most commercial firms, and their wholly-owned subsidiaries, in a broad range of countries under encryption licensing arrangements. This group of countries covers most major commercial markets including Western Europe, Japan, and Australia.
- Exports to end users or destinations outside this policy are possible on a case-by-case basis. Prior to export, products are subject to a one-time product technical review.³⁰

³⁰ Taken from a Fact Sheet (September 16, 1998) "Administration Updates Encryption Policy", issued by the White House Press Secretary, found at <http://www.jya.com/wh091698.htm>, 31 December 1998.

At the same press briefing the DepSecDef stated the DOD position and requirements for a workable encryption policy:

We in DOD had four goals when we entered these discussions. First was to strengthen our ability to do electronic commerce. We're the largest company in the world. Every month we write about 10 million paychecks. We write about 800,000 travel vouchers. One of our finance centers disburses \$45 million an hour. We are a major, major force in business. And for that reason, we can't be efficient unless we can become fully electronic....

Second, we must have strong encryption and a security structure ... to protect ourselves in cyberspace. Many of you know that we have experienced a number of cyber attacks during the last year. This will undoubtedly increase in the future. We need to have strong encryption because we're operating over public networks; 95 percent of all of our communications now go over public infrastructure – public telephone lines, telephone switches, computer systems, et cetera. To protect ourselves in that public environment, we must have encryption and we must have a key recovery system for ourselves.

The third goal that we had was to help protect America's infrastructure. One of the emerging national security challenges of the next decade is to protect this country, the homeland defense of this country, against attack. We must have strong encryption in order to do that, because most of this infrastructure now is being managed through distributed computer-based management systems....

Finally, it is very important that the Department of Defense and our colleagues in the national security establishment have the ability to prosecute our national security interests overseas. Terrorists and rogue nations are increasingly using these tools to communicate with each other and to lay their plans. We must have the ability to deal with that. And so this policy is a balanced and structured approach to be able to deal with all four of those problems.³¹

3.14 CONCLUSIONS

Most of the policy initiatives noted in this section center upon immediate responses to problems and gradually building a structure of "protect, detect, and react." To assure a greater measure of long term effectiveness, these short-term, quick fixes have to result in significant changes in doctrine. The basis of shifting the Warfighter's long term combat direction to include the cyberworld and information is fully grounded in Joint Vision 2010.

Key doctrinal developments include the realization that IO are an integral part of all military operations across the spectrum from peacetime to total war. As a crisis develops through the various levels, the focus changes in combat operations, combat support, and

³¹ Dr. Hamre's remarks taken from the release of the press briefing, September 16, 1998 found on the Internet at <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/9/16/11.text.1>.

combat service support functions – from defensive to increasingly offensive-oriented actions. Since JV 2010 has clearly spelled out the role played by IO, most leaders throughout the echelons are coming to understand that IO must ultimately shift to the offense as well as maintain a strong defense. Although legal and other considerations may preclude the fullest range of offense-oriented actions in certain circumstances, joint-minded Warfighters must develop this capability.

Another realization that has matured with the events over this past year is that a reporting structure for IO must parallel that of other operations, which have had a full, working system for decades. Just as operational readiness in the areas of direct mission capabilities, logistics, personnel strengths, and training have been measured for unit combat readiness (C-ratings) for a long time – from FORSTAT to UNITREP, so also must IO readiness be measured and reported. The creation of a reporting system for IO does not have to develop "from scratch" since the mechanisms of tracking outages of key C3 systems provide a working basis from which to start.

A significant problem of any of these reporting and measurement systems in today's high-tech world is that senior leaders do not fully understand this new dimension of warfare. As one very senior military leader admitted to a conference of technical security experts, he and his peers have a unique challenge "with a short fuse" – to include into a mentality of planes, ships, and tanks, a range of computer network attacks. Those military schools, which help form the senior leadership of the future are beginning to incorporate this new dimension into their curricula. But mission constraints, speed of change in technical developments, and developing sophistication of the technology involved prevent even the best minds from "getting smart fast" at a significant depth. Finally, new doctrinal elements of IA and CNA have entered the military lexicon as large parts of the solution lie outside of DOD. Protection of our *National Information Infrastructure* "from all enemies, foreign and domestic" is crucial to military success in the new global battlespace. Fitting together all of these pieces will require a national-level effort matched only by the sense of national purpose displayed most everywhere during World War II.

SECTION 4 STANDARDS AND TECHNOLOGY

4.1 INTRODUCTION

The Standards and Technology section of the third edition focused on detailed external factors driving the DOD efforts to protect the Defense information infrastructure. The section examined helpful factors such as the encryption initiatives, virtual private networks, firewalls, and other assistance available from survivability research, both by government and commercial firms.

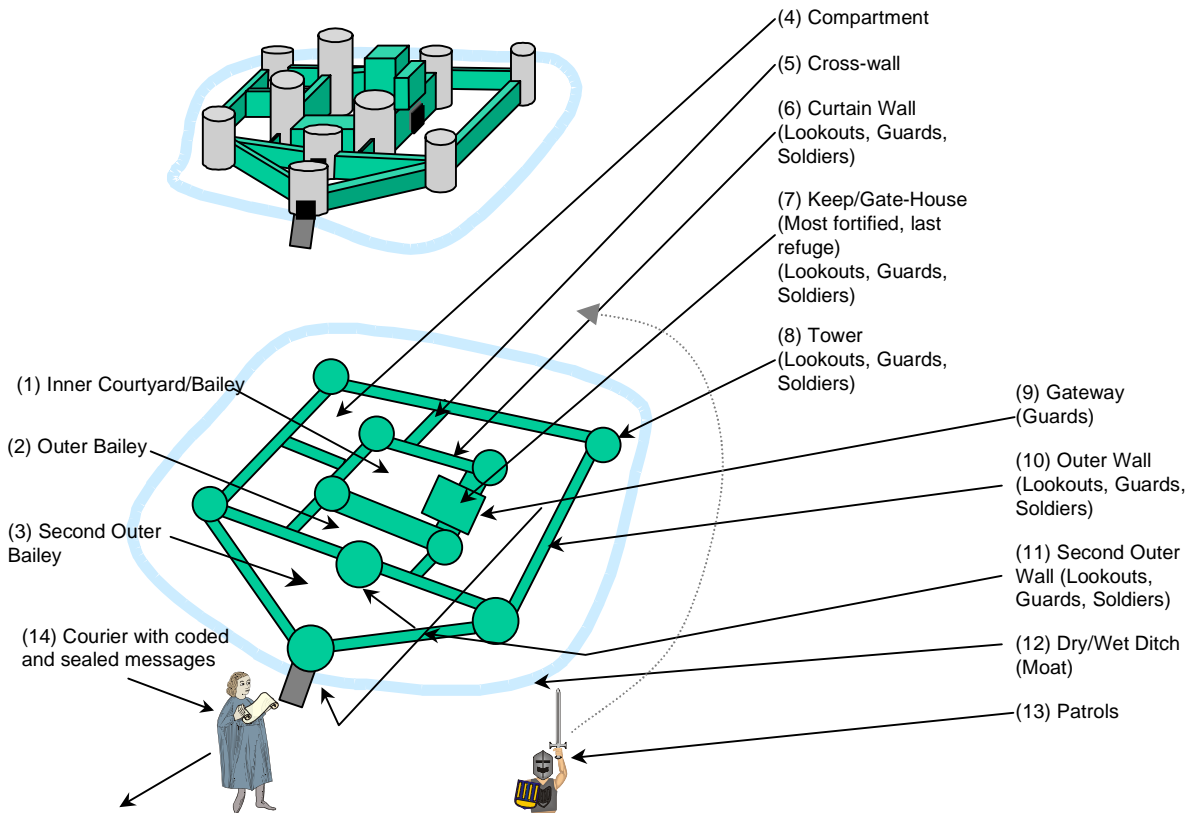
This current section examines the strategies that DOD is using to fight threats, eliminate vulnerabilities and weaknesses, reduce risk, and enhance efficiency. These strategies integrate many of the initiatives reviewed in the third edition and build a strong counter to the many problems that multiply with technology. The four strategies examined are:

- Implement a Defense-in-Depth strategy to reduce reliance on a single technology and the chance of a technical breakthrough
- Build a Public Key Infrastructure, which will secure and authenticate at multiple levels
- Develop a framework of joint standards architectures to guide the evolutionary path of all C4I information systems and networks toward a secure and interoperable realization of Joint Vision 2010
- Secure and strengthen DOD electronic commerce for greater combat support efficiency.

4.2 DEFENSE-IN-DEPTH

Frederick the Great, as a strong military theorist, explicitly reminded military planners everywhere that it is impossible to defend against every possible attack. It has been a principle of warfare for centuries that no defense can be absolutely impregnable. Layering defenses and surrendering them only gradually to create a time and space layer to guard the "inner sanctum" goes even further back in history. The idea was well known in the Middle Ages; the lord of a castle laid out villages strategically so that they presented "stumbling blocks" to the enemy, and built two walls and a moat around the castle as another defense. Exhibit 4-1 shows this concept.

<i>CONTENTS</i>
Defense-in-Depth Strategy
• Layered Approach
• Like a Medieval Fortress
• Modern Methods of Depth
• Shared Risk and Failure
Public Key Infrastructure
• Symmetric and Asymmetric Cryptography
• Certification, Distribution, Trust
• A Measured Beginning
Joint Standards Architectures
• <i>Evolutionary Path to a Framework</i>
• Operational, Systems, Technical
Electronic Commerce
• DOD Progress
• Need for Standards
Government Networked Information Exchange
Conclusions



Defense in Depth	Medieval Castle Analogy
Secure Protocols	14
Protect Enclave Boundaries (sensors, firewalls)	5,6,7,10,11,12
Protect Host Computers (antivirus software)	7
LAN Monitoring/Detect and Prevent Attacks on Enclave	7,8,10,11,13
IW Situation Awareness (Intrusion Detection and Reporting)	6,7,8,10,11,13
Multi-level Secure Interoperability	1,2,3,7,9
Non-Repudiation Services (by Digital Signatures)	9,14

Exhibit 4-1. Analogies Between the Medieval Castle and the Defended C4ISR

The table relates various information protection means to portions of the medieval castle's defenses. For example, the command, control, communications, computers, Intelligence, surveillance and reconnaissance (C4ISR) strategy dictates that systems and networks processing information use secure protocols such as the Public Key Encryption (PKE). This will enable them to attain confidentiality and integrity for data, whether it is stored within a host device or being conveyed through the network. A comparable means used in the medieval castle would be to use a courier who carries all messages in coded form. Notice that the castle itself was built as a layered fortress with many distinct defenses. The enemy would have to breach all of these defenses before reaching the innermost keep, the bailey. At that point the siege would be over; the castle would be won. If the IW enemy is able to penetrate the many layers of IA, the mission critical information is compromised – in availability, confidentiality, integrity and reliability, authenticity and trustworthiness, or verifiability of the true source.

This image serves well as an analogy for protecting the integrity of the Defense Information Infrastructure (DII) and critical information moving within the DII. The protections used from medieval times apply to DII survival and information assurance through the well-known security services of availability, integrity of data, and confidentiality. As the *Joint Pub 1-02* describes it, the principle of Defense-in-Depth is "The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve."¹

The layers of defense for the DII include the following technical means.

- ***Protecting the Wide Area Networks (WAN)***, especially the Defense Information System Network (DISN), the Secret Internet Protocol Router Network (SIPRNET), and the associated unclassified NIPRNET. The main means will be hardening through encryption of the DII routers, the Asynchronous Transfer Mode (ATM) switches, and the Domain Name Servers, which were a key target during Solar Sunrise.
- ***Securing Host Computer Operating Systems***, which will help to protect the host computers themselves. The cooperating layers here will be assured-quality, standardized anti-virus software; securable operating systems (such as newer versions of Windows NT and UNIX); and other protective hardware and software.
- ***Using Security-Enabled Applications***, integrated through standards such as the Application Security Service Application Programming Interface (API). This standard will be added to the DII Common Operating Environment (COE) and used with other secure protocols for end-user identification, authentication, and privacy (confidentiality).
- ***Protecting the Enclave or Local System Boundaries***, especially communities of interest, such as theater operational networks, logistics networks, or intelligence networks. The barrier here will be firewalls using one or more of several effective methods.
- ***Monitoring Defense Networks***, using state-of-the-art commercial products that capture major events in near-real time. Research and development work will concentrate on those tools which give the Enterprise view for security, the larger Common Operational Picture (COP); and provide Situation Awareness/Response capabilities for extensive analysis and visualization, central visibility, and high-tempo response.

¹ Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 23 March 1994.

- **Monitoring Host Computers**, with reliable Intrusion Detection Devices. These will detect attacks on known vulnerabilities; collect summary status information; and enable an accurate overall assessment.
- **Employing Key Management Infrastructure Services**, which will tie Digital Signatures to a simple but powerful structure of certificates. The certificate hierarchy will provide a trusted verification by command-related authorities (Central and Local Registration Authorities).²

Several facets of the Defense-in-Depth strategy are somewhat new for those who have worked in the past with simpler secure systems. The first is the evolving realization of the Department "shared risk." With so many computers, communications systems, networks, diverse software, as well as varying levels of awareness and competency in practice, risks accepted by any user or group become the risks assumed by all others. Likewise, for perhaps the first time, commanders and their staffs are beginning to realize that they must expect some failures owing to viruses, flooding, and other attacks. These low-level penetrations and major frontal assaults can originate from "script kiddies" (novice crackers who use sophisticated attack software for fun, often without understanding their mechanisms), genuinely sophisticated crackers, organized criminals, and state Information Warfare agents.

The Defense-in-Depth concept uses the old approach of onion-skin layering of security tools, mechanisms, structures, and knowledge. No layer of the onion has really great strength or invulnerability in itself, but the combined whole can work to make penetration and destruction tasks formidable, or even undoable. DOD is very active in building and increasing the layers of its Defense-in-Depth onion.

As illustrated in Exhibit 4-2, a protected enclave (an Intelligence network, a logistics network, a Headquarters building wired into a common LAN, or a local control center) can be isolated and protected from most outside threat intruding into an unauthorized area by the use of a firewall. Joint Intrusion Detector (JID) sensors provide an early warning of an intruder threatening an imminent attack on a local area network. The SIPRNET portion of the DISN itself serves as a barrier to intruders who might try to penetrate the enclave. Finally, the Intrusion Reporting network/system is composed of the Regional Operations and Security Centers, and the Global Operations and Security Center. These have normal outage and operational chains of command, which serve to protect and provide suitable responses in case of a breach of defenses. As in the medieval analogy, an "outpost" can communicate being overrun to the "liege lord" who can send reinforcements.

² This structure and explanation based upon several Defense-in-Depth briefings given by Dr. Frank Perry of DISA.

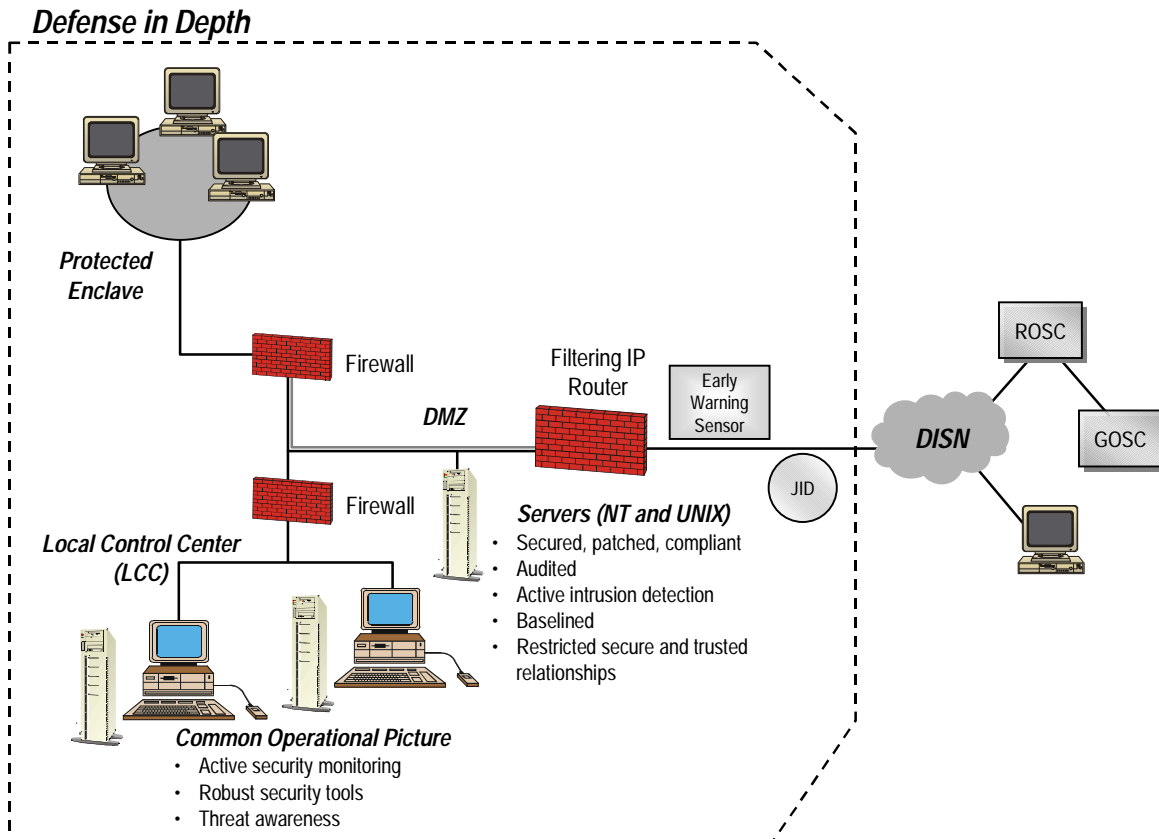


Exhibit 4-2. The CAISR Defense in Depth Protections

Firewalls/filtering IP routers, JID systems devices, secured operating systems, commonly available security software suites, and anti-virus software are receiving Defense-wide attention. DISA conducted the DIO Review Program to assist the combat and support CINC's in assessing and improving their IA posture. In addition to identifying and helping to solve problems, the teams installed some of these devices and provided necessary training. An emphasis on education, training, and awareness; joint security architectures, standards; and proper engineering tools will continue the deepening process. In summary, DOD components have addressed the technical status of their systems and networks as well as those remedies that would "raise the bar" for security capabilities.

4.3 PUBLIC KEY INFRASTRUCTURE

There are two types of message cryptography: **symmetric** and **asymmetric**. In both types, a sender encrypts or scrambles a message using a key, and then the receiver decrypts or unscrambles the message using a reversing key. With symmetric cryptography, the key used by both parties is the same but reversed: A and A'. The sender uses the key A to change plaintext (readable, clear text) into ciphertext (unreadable, scrambled text); the receiver uses the reverse key A' to change the ciphertext back into plaintext. This type of cryptography provides confidentiality, authentication, and non-repudiation.

Because of its widespread and open standards configuration, the asymmetric type is often called public key encryption. With public key cryptography the mathematical methods behind the process are totally different. As a result, the keys used are not merely reversed but are different. They are designated as public key and private key. The public key is published for the whole world, or a specialized subset, to have "knowledge" or access to, while the private key is "known" or available only to the using party. For confidential transmissions the originator's software uses the receiver's public key so that the *en route* message is encrypted; the intended receiver at the distant end uses the "receive" private key to decrypt the message. Since **only** the receiver has the complementary private key, only the receiver can decrypt the message.

For authentication of signature and accompanying non-repudiation of transmission, the originator's software uses the sending private key, available **only** to that originator/machine, and encrypts the message. Anyone in the whole world, or a specialized subset, that has "knowledge" or access to the originator's public key can decrypt the message. Since the public key is known to belong to the originator, the fact that the message can be decrypted means that it must have been encrypted by the originator's private key.

Each of these methods of cryptography has its own unique problems. Symmetric cryptography demands a closely controlled distribution network for both keys, and both parties involved in the transmission must coordinate beforehand to ensure possession and use of a common key. With public key cryptography the distribution of private keys must be well controlled, and the match of the private and associated public keys must be assured. Distribution of the public key should be fairly wide (even if it is not desired to make it available to all possible receivers); the critical element is assure all users that the public key is indeed the correct public key for the published user, not for someone else.

Standard "crypto-control" channels ensure the distribution of symmetric keys, whether by hardcopy (paper) or by softcopy means (electronic key distribution systems). With public key encryption methods, a recognized authority must validate and certify the match of public and private key; the same authority must certify the registration of the published public key as belonging to the designated user. Furthermore, higher levels of authority will provide a valid certification of this lower, local registration authority (LRA); the certification hierarchy must in turn work up to an ultimate authority, trusted by all. The ultimate certification authority (CA) certifies the operation of the entire hierarchy, down to the lowest LRA.

While on paper it may not seem difficult to establish a trusted hierarchy of CAs, for networks as large as those within the DOD the problem is daunting. Not only must the certifications be continually updated, but also users must be notified of compromises and expirations of registrations. These and other large-scale administrative practices must work flawlessly if the system is to retain a high degree of trust. Establishing this system demands careful implementation in several phases to ensure that problems are resolved before the infrastructure grows to full stature.

The Deputy Secretary of Defense has directed that DISA and NSA take lead and work together with the Joint Staff, the CINCs, the Services, and all Defense Agencies to ensure that the public key infrastructure grows quickly. But this growth can never be at the expense of compromising the necessary trust that the system must have and retain. The public key infrastructure will be implemented starting at the sensitive unclassified and lower classified levels. When the infrastructure proves to be totally trustworthy and reliable, it can be developed fully for higher classification levels and mission criticality. While this highest assurance (classified and mission critical) infrastructure will probably originate from NSA research and development, commercial public key cryptography will likely find wide use for sensitive but unclassified information requiring a basic or medium degree of assurance.

4.4 PKI ROADMAP

In August 1997, the DepSecDef issued Management Reform Memorandum (MRM) #16 directing DISA and NSA to establish a DOD PKI. To define key concepts and establish an overarching framework, the combined staffs published the DOD Public Key Infrastructure Roadmap, Version 1.0 in August 1998. It introduced the following key framework elements:

- Certificate management
- Registration (through central and local authorities)
- Implementation of the cyber-mechanisms at the application level.

DOD published its Public Key Infrastructure Roadmap, Version 2.0 in February 1999. A key change that emerged in this milestone document was the incorporation of four levels, designated as classes, of information assurance. These classes and the intended applications are shown below. The Roadmap does not identify a Class 1.

- DOD Class 2 (formerly Basic): intended for applications handling low value (unclassified) information or system high information in a low to medium risk environment such as the SIPRNET. This does not require that the end-user register in person. Cryptography can be software based.
- DOD Class 3 (formerly Medium): intended for applications handling medium value information in a low to medium risk environment where individual identity is needed for authentication and non-repudiation (such as financial transactions). This requires that the end-user register in person. Cryptography can be software based.
- DOD Class 4 (formerly High): intended for applications handling medium to high value information in any environment or system high information in a low to medium risk environment such as the SIPRNET. This requires that the end-user register in person. Cryptography must be hardware based.
- DOD Class 5 (a new category): intended for applications handling classified information in a high-risk environment (over open or unprotected networks). Cryptography must be NSA approved and hardware based.

This strategy to achieve the target DOD PKI is intrinsically linked to the overall DOD strategy for achieving IA. Key to the successful implementation of both is the ability to begin immediate leveraging of the existing IA capabilities afforded by commercial technology. Since traditional GOTS-based implementations cannot keep pace with fast-paced change in commercial technology, the DOD PKI strategy must employ an open standards approach while still maintaining appropriate levels of security for the information being protected.

4.5 JOINT STANDARDS ARCHITECTURES

Effective military operations rely on a mix of forces that can be deployed to anywhere in the world, at a moment's notice. The ability of the information technology systems supporting these operations to interoperate – work together and exchange information – securely is critical to their success. Real-world experience from Grenada to the Persian Gulf has taught us much about the necessity of having interoperable, secure command and control as well as command-support information systems. The lessons learned from the events of Desert Shield/Desert Storm and post-Gulf War actions have resulted in a new strategy for DOD operations. Joint Vision 2010 is the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people, and leverage technological opportunities to achieve new levels of effectiveness.

To fight jointly, the military and industry must work together to convert the many legacy or stovepipe systems used today into seamless networks with security that is invisible to the Warfighter. This will result from building commonality into all new systems and retiring those systems that cannot migrate. The integration of the National Command Authorities, the Joint Staff, the CINCs, the Services, and the many Defense Agencies into a streamlined whole relies upon commercial, robust, proven, and secure technologies. The wise selection of solid standards and architectures started with the development of the DII in the late 1980s and the early 1990s. In those days the Defense Technical Architecture Framework for Information Management (the TAFIM) formed the basis of profiling standards into usable patterns. TAFIM Volume 7 became in time "The Standards Book" for designing new systems and networks as well as acquiring hardware and software.

The Information Technology Management Reform Act of 1996³ directed all government departments and agencies to "establish goals for improving the efficiency and effectiveness of agency operations ... through the effective use of information technology." Since DOD had already laid a strong foundation of standards, acquisition management, and architectures, and since it had also established a worldwide reputation as the security leader, it was necessary to make only minor refinements in regulations, such as DOD Directives and the various C/S/A implementations. A series of key developments that spanned the publication of the ITMRA strengthened the Defense drive toward its goals:

³ P.L. 104-106, sec 5123.

- The continuing evolution of the "best of breed" selections from the Services' Command and Control systems (e.g., from the Joint Maritime Command Information System to the Global Command and Control System) in the early 1990s.
- The ongoing development and refinement of the DII COE, and the growing suite of integrated application software to serve many Defense requirements in the mid-1990s.
- The growth of industrial standards and the incorporation of commercial off-the-shelf products based on them, such as public key encryption software (Verisign™, RSA, and other software based on protocols like Secure Sockets Layer or Secure Electronic Transaction), Windows NT® and various Microsoft Office®-based software suites.
- The publication of *The C4ISR Architecture Framework*.

The *C4ISR Architecture Framework* provides a base methodology for developing architectures. It mandates neither specific techniques nor automated tools. Its guidelines allow sufficient flexibility for organizations to achieve their own mission needs. It provides for a foundation of three architectural "views" – operational, system, and technical. These views integrate "the accomplishment of agency missions through the use of the best practices in information resource management."⁴ The three architectural views, or simply architectures, tie together the critical components of mission performance (operational architecture), mission support (systems architecture), and mission technology (technical architecture). Exhibit 4-3 shows the unity and interoperability of these three key building blocks.

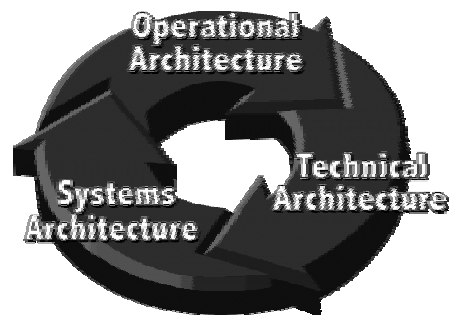


Exhibit 4-3. The Unity of the Three C4ISR Architectures

The C4ISR framework lives up to IEEE's definition of an Architecture as "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time."⁵ The clear separation and integration of the three basic architectures is seen clearly in their respective definitions (and their functions, as illustrated in Exhibit 4-4):

⁴ The tie to meeting the legal requirements of the ITMRA, section 5112j.

⁵ Institute of Electrical and Electronics Engineers (*IEEE*) *Standard 610.12*.

- **Operational Architecture.** Descriptions of the tasks, operational elements, security requirements and information flows required to accomplish or to support a warfighting function. It is a disciplined approach and methodology to review baseline requirements, assess doctrinal impacts, and examine and assess alternatives through phases of functional and process improvements.
- **Systems Architecture.** Descriptions, including graphics, of systems, security devices, and interconnections providing for or supporting warfighting functions.
- **Technical Architecture.** A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements. The purpose of these rules is to ensure that a conformant system satisfies a specified set of requirements (such as the Defense Goal Security Architecture – DGSA).



Exhibit 4-4. The Functions of the Three C4ISR Architectures

The definitions in this Framework provide for continued evolutionary development from the TAFIM to the practical implementation of the Joint Technical Architecture (JTA). This defining work is helping to set common standards and "building codes" to allow the flow of information in support of the Warfighter. This especially reflects the Warfighter's need for secure processing of battlespace information. The JTA is continually being updated to reflect both the state of the art and the Warfighters' changing requirements, both of which are crucial to achieving JV2010. The standards and guidelines in the JTA are stable, technically mature, and publicly available. Wherever possible, they use off-the-shelf commercial implementations from multiple vendors. Standards and guidelines that do not yet fully meet these criteria, but that are expected to mature in the near-term, such as Secure Electronic Transactions (SET), are cited as "emerging standards" in the expectation that they will be mandated in future versions of the JTA.

4.6 ELECTRONIC COMMERCE

As a result of Congressional Guidance provided in the Federal Acquisition Streamlining Act (FASA) of 1994,⁶ DOD has taken the lead in achieving extensive capabilities in

⁶ P.L. 103-355, October 10, 1994.

Electronic Commerce. The Department is the lead agency for many industries and companies doing business with the Federal government. Two key illustrations are: DOD's operation of the Central Contractor Registration for all entities desiring to do business with the Federal Government; and DOD's operation of the Electronic Commerce Information Center. In less than four years the ECIC has provided almost 35,000 information packets, and helped almost 17,000 business to complete their CCR registration.

In addition to using publicly available websites, a key procedural foundation used for purchases under \$100,000 is the use of value-added network (VAN) service-providers and the technical protocols established by the American National Standards Institute (ANSI) X-12 committee. A key standard is the use of ANSI X-12.58 security protocols for transactions requiring confidentiality, integrity, authentication, and non-repudiation. (For these last requirements, digital signatures and hashing provide state-of-the art services.) DOD is studying Secure Sockets Layer (SSL), SET, which is in early use by VISA, MasterCard, and other credit card companies, and other commercial initiatives. These initiatives may be used as DOD security standards for transactions that are unclassified but sensitive in nature.

The DOD initiatives in electronic commerce include several Department efforts to use electronic data interchange (EDI) message formats for commercial-type Defense enterprises. Most noteworthy are the efforts to streamline the Defense Travel Service system through electronic means. Also, the Defense Logistics Agency (DLA) and the Defense Finance and Accounting Service (DFAS) have pursued widespread efforts to make the supply system and many payroll services cheaper and more efficient. Critical to these systems is the security of many of the transactions. A significant development in establishing these secure services has been the mandate of a DOD-wide Public Key Encryption/Public Key Infrastructure (PKI) which is being installed into the DII.

4.7 GLOBAL NETWORKED INFORMATION EXCHANGE (GNIE)

In November 1998, OASD(C3I) announced a new strategy and framework to modernize the DOD approach to information management at the Enterprise level, the GNIE. With its emphasis on information vice infrastructure facilities, the GNIE approach realizes the Business Process Re-engineering values of the 1990s and addresses the weaknesses cited in the 1996 Quadrennial Defense Review (QDR).

The GNIE sets the stage for transitioning away from legacy systems, massing technology investments to achieve life cycle returns, and prepare a sound posture for the Y2000 QDR. In the specification of an "Information Enterprise" the central value of information as a resource emerges. Now ranked on a par with the other mission focuses of Strategy, Tactics, and Logistics, Information is recognized as a key implementer. The drive for compatibility becomes more than just hardware and software interfaces, but rather includes compatibility between technologies, operational processes, and mission partners.

Some key elements of the GNIE strategy include:

- Aligning the various DII initiatives within the PPBS
- Developing a senior management method to prioritize all supporting efforts
- Managing the process to support the DOD mission Enterprise through building the DII to integrate technologies, customers, suppliers
- Defining a collaborative effort for developing policies and components.

To achieve this evolving vision, the DOD Deputy Chief Information Officer (CIO) convened the first meeting of the GNIE Senior Steering Group (GSSG) composed of flag-level representatives of the CINCs, Service, and Agencies in December 1998. They drew up a charter to structure their efforts and required organizational support. The GNIE Overarching Integrated Project Team (OIPT), which has three working groups focused on the activities and products shown below, supports the GSSG:

- Computing and Communications Infrastructure WG
 - Mid-tier Computing Policy
 - Network Policy
 - Information Assurance Policy
- Enterprise Management WG
 - Network Control Hierarchy
 - Information Management Strategy
 - Configuration Management Policy
- Resourcing the Enterprise WG
 - Funding Strategy
 - Business Case Guidance.

The efforts of the GNIE OIPT will integrate with other parallel efforts such as the Defense Information Assurance Program.

4.8 CONCLUSIONS

The DOD implementation of a Defense-in-Depth strategy will reduce reliance on a single technology and the chance of a technical breakthrough. The continuing development of the Public Key Infrastructure from concept to fielding will protect and ensure mission critical information at multiple levels. As mature frameworks of operational, systems, and technical architectures meet the direction of National Security Policy, sustainable development will guide the evolutionary path of all C4I information systems and networks toward Joint Vision 2010. Finally, growth of electronic commerce within DOD will serve as an engine of business process engineering helping to increase efficiency of combat support (and indirectly, combat and combat service support) activities.

SECTION 5

ORGANIZATIONAL CONSIDERATIONS

5.1 GENERAL

The operational concepts for information operations are evolving rapidly. The understanding of how to integrate IA into both defensive and offensive IO is increasing. Critical infrastructure protection has emerged as a new requirement. Because of these changes, commanders must now review their organizational structure to ensure they can properly plan, coordinate, and execute in these environments.

When reorganizing, there are three primary options to consider: whether to remain the same, reorganize, or create a new organization. Commanders consider things such as chain of command, manning, staff and coordinating procedures, both internal and external, training and responsibilities. This chapter reviews some of the more significant reorganizations and the emerging organizations. The section discusses considerations in determining if organizational change is necessary.

<i>CONTENTS</i>
General
Reorganization
• ASC(C3I)
• Joint Staff
• TWI
New Organizations
• JTF-CND
• DIART
• DIO for IO
• NIAP
• CIAO
• NIPC
• JWRAC
Considerations
• Education and Training
• Requirements
• Working Relationships
Conclusions

5.2 REORGANIZATION

5.2.1 Assistant Secretary of Defense for Command, Control, Communications and Intelligence

One of the major organizations to reorganize was the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I). OASD (C3I) is charged with policy development, planning, resource management, and fiscal and program evaluation responsibilities in the areas of IA, IO, and CIP. The organization restructured to handle the present and future developments within IO. Appendix A shows a wiring diagram, mission, points of contact, and ongoing activities. One of the more significant changes was the placement of the IA, IO, and CIP directorates under one supervisor, the Deputy Assistant Secretary of Defense (DASD) for Security and Information Operations. Since the three fields overlap, this allows for more complete coordination and provides a more complete picture of the information operations environment to the decision-maker when it applies to policy and operational issues. The other significant change was the consolidation of the various security sections under the same DASD. Many of the IO issues require a security review and this allows the security decision to occur simultaneously with the policy or operation.

5.2.2 Joint Staff

The Joint Staff Director for Operations (J3) changed its organization to meet the growing requirements for IO. Within the J3, the IO staff elevated from a division organization to a deputy directorate, the Deputy Director for Operations (Information Operations), J39. As part of the reorganization, an Information Strategy Division was formed. This change indicates the realization that IO missions are likely to occur separate from other military operations, which requires a separate staff section to monitor. As a part of this change, the deputy directorate established its own crisis action planning cell. The cell manning depends on whether the directorate is augmenting the existing crisis action team or a separate information operation. Included in the change was the requirement for the National Military Command Center to review reports concerning information system intrusions and related topics. Appendix A provides a more detailed look at the organization. It is important to note that while the J3 organization is responsible for both offensive and defensive operation, the IA responsibility remains within the J6 Directorate.

5.2.3 Transnational Warfare Office for Information Warfare Support (TWI)

To handle the growing intelligence requirements for IO, the Defense Intelligence Agency (DIA) established the TWI office under the Transnational Warfare Group. This office is given the mission to collect, analyze, produce, and disseminate all-source intelligence supporting offensive and defensive operations. A primary reason for the establishment of this office acknowledges that the intelligence requirements for IO vary from traditional intelligence requirements. For example, developing the indications and warning procedures for attacks against information systems requires technical expertise in computers, the networks that link them, and the tools that protect them. The granularity of the analysis and technical expertise of information systems is not typical of traditional intelligence requirements. Another major function for this office is the requirement for providing the influence of cultural, psychological, and other human factors on decision making. This relies heavily on HUMINT requirements. A Defense HUMINT Service and a Human Factors Center emerged to provide the intelligence gathering and analysis. Appendix A provides more details of the TW organization.

5.3 NEW ORGANIZATIONS

5.3.1 Joint Task Force (JTF) Computer Network Defense (CND)

One of the more significant new organizations to emerge with IO is the Joint Task Force Computer Network Defense (JTF CND). During exercise ER97 and Operation Solar Sunrise, it became apparent that, to defend computer networks properly, a commander was needed.

The threat to the Defense Information Infrastructure and the computer networks which control and operate within it continues to grow. This threat knows no traditional boundaries. The attacks can come from all different phases, from all different directions.

To defend against that type of threat requires an organization focused on the "How to?" For the Department of Defense, that organization is the JTF CND.

This organization, still in the infancy stage, has the mission of coordinating and detecting the defense of DOD computer networks and systems. This includes coordinating DOD defensive actions with non-DOD government agencies and appropriate private organizations. The purpose is to develop a unified means to protect these systems and networks – an underwriting task considering the amount of computers, networks, and systems within DOD. Combining that task with the likelihood that these attacks will cross traditional command relationship lines increases the difficulty of the tasks. The final factor to consider is that the threat includes individuals, state and non-state entities, or could even be anonymous.

The Commander of this joint task force will exercise coordination authority over the service component commanders. In addition, the command will coordinate authority with unified command, DIA, NSA, and other government agencies. Exhibit 5-1 depicts the JTF organization. Exhibit 5-2 shows how the organization fits in with these other agencies.

The JTF collects data on an organized information attack against critical DOD information networks, formulates courses of action (COA) to threat attacks, coordinates and directs DOD actions for defense, and prioritizes survey actions and mission critical "workarounds" for the DII.

The JTF CND achieved initial operational capability (IOC) in January of this year. The command is collocated at DISA headquarters and commanded by the Deputy Director of DISA. The JTF CND will execute its responsibilities primarily through its interaction with the DISA GOSC and assigned service components. To orchestrate a coherent defense against operationally significant computer network attack, the JTF will establish and maintain oversight of OSD, Services, CINCs, and DOD agencies' CND efforts.

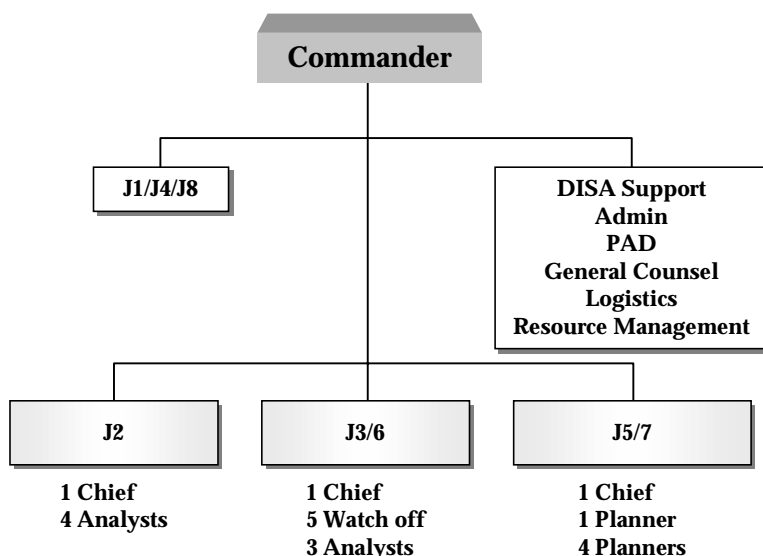


Exhibit 5-1. JTF Organization

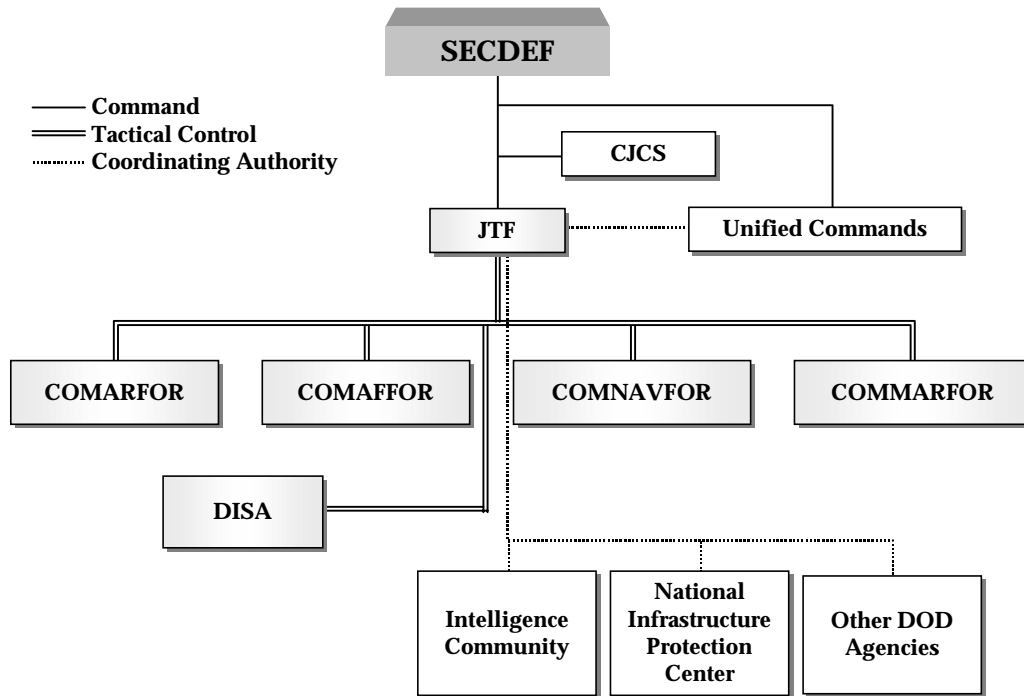


Exhibit 5-2. How JTF Fits Into the Overall Organization

5.3.2 Defense-wide Information Assurance Program (DIAP)

The DIAP is a management process and structure established to centralize information assurance efforts within DOD. The program was designed to integrate and provide oversight of DOD IA activities; provide a structure to monitor and coordinate IA readiness; and establish IA responsibilities and authorities DOD-wide. The program includes integrated planning, programming, and budgeting with decentralized execution but centralized oversight. The OASD(C3I) Director for Information Assurance is responsible to the DOD CIO for the overall operation of the DIAP.

In order to execute these activities, a DIAP staff was formed. The OASD(C3I) Director of Information Assurance will supervise the DIAP Staff director and oversee the daily operation of the DIAP Staff. The DIAP Staff Director is responsible for integrating DIAP into the Defense Planning, Program, and Budgeting System (PPBS); assessing DOD IA investments and perform oversight of policy, function, and program IA execution. OSD occupies key DIAP Staff management positions. The Services, Joint Staff, OSD, and Defense Agency personnel make up the rest of the staff. The DIAP Staff consists of two major teams: the Functional Evaluating and Integration Team and the Program and Development Team. Appendix B discusses the specific roles of these teams, but their primary functions are to monitor and represent Component IA programs and determine the optimal mix of IA functions.

The DIAP crosses into various organization groups and coordinating agencies within DOD. The DIAP will assist the DOD CIO in ensuring IA information technology and resources are effectively managed to meet operational requirements. Since the DIAP includes

programming and budgeting, there is a need to ensure the DOD CIO Council includes all DOD components with significant IA responsibilities. A Senior DIAP Steering Group assists in these functions. The membership consists of the DOD CIO, the Director, DISA, the Joint Staff J6, the Director, NSA and the Service C4 Chiefs. The purpose of the group is to provide strategic direction and guidance in all IA issues.

Within the DIAP management system, there is the National Manager for National Security Telecommunications, Information Systems Security, and the Defense Information Infrastructure (DII) Advisor. The Director, National Security Agency (DIRNSA), is the National Manager. As part of that responsibility, DIRNSA provides INFOSEC technical guidance, advice, and support to U.S. Government departments and agencies. The DIRNSA will also disseminate threats to and assess overall security posture and vulnerability of national security systems.

The Director, Defense Information Systems Agency, serves as the DII Advisor and is responsible for the planning, development, and support of command, control, and communications and information systems that serve the NCA. The Director, DISA, also serves as the DOD DII System Engineer and provides system engineering and direction, including network management and security to the DII.

5.3.3 Defense Intelligence Officer (DIO) for Information Operations (IO)

Another change within DIA was the establishment of a DIO for IO. The position provides a senior intelligence officer reviewing IO requirements and actions for the Director. This change does not create a new organizational staff but provides senior leadership for an intelligence field. The officer reviews resources, requirements, and the overall status of how the agency handles IO. With only eight of these positions existing before the creation of the new position, this position is indicative of the growing importance IO and related fields are to the senior leadership of DOD. This year the DIO has an additional responsibility that of providing input into the DOD Intelligence plan. The plan assigns responsibility to intelligence agencies and units. This year's document will have a separate section for IO—another indicator of IO greater importance in the intelligence field.

5.3.4 National Information Assurance Partnership (NIAP)

The NIAP is an NSA/NIST sponsored forum through which industry and government organizations can collaborate to develop security metrics, tests, test methods, tools, reference implementations, and protection profiles. These can be used by independent testing laboratories in the private sector to conduct product test and certification. In this way the government will be able to procure and deploy security technologies and products that have been independently tested. NIAP will also serve as the mechanism for mutual international recognition of evaluation tests conducted under the "Common Criteria" program, an internationally agreed-upon means to specify security functionality and assurance so that the systems can be tested for conformance.

5.3.5 The Critical Infrastructure Assurance Office (CIAO)

PDD-63 calls for a national plan coordination office [the CIAO]. In a statement before the House of Representatives, the new director of the CIAO made clear his office's mission:

PDD-63 charges this Office with integrating the various sector plans into a National Infrastructure Assurance Plan and coordinating analyses of the U.S. Government's own dependencies on critical infrastructures. The Office will also assist in coordinating a national education and awareness program as well as associated legislative and public affairs [efforts]. ... We hope to assist the National Coordinator to achieve the creation of a successful national plan to protect the nation's critical infrastructures from intentional, debilitating attacks.¹

In an October 1998 briefing the Director laid out a number of key principles for working national priorities of industry-government partnerships, increased national awareness, better national structures to cope with problems, and increasing research and development investments in protection:

- Work with the Congress
- Don't think that Washington has the answers
- Avoid additional regulation
- Encourage market forces to provide solutions
- Don't throw more money at the issue
- Protect privacy rights and civil liberties
- Be results oriented.²

These principles which embody key doctrinal concepts illustrate the quandary of government in addressing infrastructure risks in peacetime when private industry controls the structures under free market, economic-driven, demands.

5.3.6 The National Infrastructure Protection Center (NIPC)

PDD-63 also calls for a national infrastructure protection center. Located in the FBI headquarters building in Washington, D.C., the NIPC brings together representatives from the FBI, Department of Defense, the Intelligence Community, other federal government agencies, state and local governments (especially law enforcement), and the private sector in a partnership to protect the nation's critical infrastructures. Its mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response to threats or attacks against our critical infrastructures, the foundation upon which our

¹ Dr. Jeffrey Hunker, Director, Critical Infrastructure Assurance Office, remarks to Congress, June 1998, reported on the CIAO webpage, observed at <http://www.ciao.gov/about.html> on 31 December 1998.

² Dr. Jeffrey Hunker, Director, Critical Infrastructure Assurance Office, Briefing on "Critical Infrastructure Protection – An Overview and Agency Roles," October 13, 1998, observed at <http://www.ciao.gov/about.html> on 31 December 1998.

industrialized society is based. It serves as both a national security and law enforcement focus to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and "cyberspace" related. The concept for the NIPC grew out of both the recommendations of the PCCIP and the government's experiences in dealing with illegal intrusions into government and private sector computer systems over the last five years. A preliminary NIPC-like organization proved this working concept in its investigation and triage efforts during the Solar Sunrise attack in February 1998. The NIPC's job, however, is not simply to investigate and respond to attacks *after* they occur, but to learn about them *beforehand* and prevent them. As PDD-63 notes:

"The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means for facilitating and coordinating the Federal Government's resources to an incident - mitigating the attack."

The NIPC works under the realistic philosophy that:

No computer or networked system can be one hundred percent attack proof and the job of securing a system against an illegal intrusion will never be complete. But using best practices and recommended security measures can move us forward to a more secure environment for securing the nation's infrastructures.³

5.3.7 Joint Web Risk Assessment Cell (JWRAC)

DOD has created a 22-member Reserve component team to monitor and evaluate web sites. The cell will locate at DISA. Their role is to ensure sites do not compromise national security by revealing any sensitive information. In addition, the team will search for information and trends of data that could be used to breach security or pose a threat to operations and personnel. They will evaluate site contents for compliance, procedures and best practices as well.

The 22-member cell will consist of two full time Reservists and 20 drilling reserve component positions. The two full-time Reservists, an officer and enlisted member, will provide the daily administrative support, perform operational scheduling and ensure training and technical proficiency is maintained. The positions will rotate among the military reserve components. The remaining 20 positions will consist of: five officers and three enlisted from the Army National Guard; three officers and two enlisted from the Army Reserve; two officers from the Naval Reserve; one Marine Corps Reserve officer; two officers and one enlisted from the Air National Guard; and one enlisted from the Air Force Reserve.

5.4 COMBATANT COMMANDS

Since publication of the 3rd Edition, a considerable body of information operations and information assurance policy has been promulgated. The policy initiatives represent a

³ Philosophy of the NIPC was found at <http://www.nipc.gov/nipc/nipc.htm>.

fairly significant departure from business as usual and the Combatant Commands are busy digesting the policies, determining applicability to their area of operations or functional responsibilities, and beginning to implement key policy requirements. With a few exceptions, information operations responsibilities are assigned to the J3's and information assurance responsibilities are assigned to the J6's. Responsibilities for critical infrastructure protection are not as consistently assigned. In some commands, the J4 has the lead because of the emphasis of the Critical Asset Assurance Program on protecting physical assets. In other commands, the responsibilities are divided among the staffs based on the functional aspect of the critical infrastructures.

By and large, the information operations, information assurance, and critical infrastructure protection activities are integrated with one another and with the deliberate and crisis action planning process through an information operations cell. The cell membership consists of representatives from the primary and supporting staff directorates.

Since publication of the 3rd Edition, many of the Commands have been developing long-range strategic plans and near-term action plans to add information operations, information assurance, and critical infrastructure protection capabilities to the Command. Traditionally, the forces assigned to the Command provide such capabilities. In the information age, however, many of the Commands are recognizing the need for the Command Headquarters to provide some of these capabilities. For example, many of the Command Headquarters elements operate their own local area networks and command and control systems; by necessity, information assurance for these networks and systems must also be provided by the Command Headquarters. To ensure some consistency in protecting vital networks and systems, most Commands have established a coordinating mechanism (e.g. working groups, conferences, etc.) to share information assurance best practices with the sub-unified commands, assigned joint task forces, and component commands.

While much remains to be done in working out detailed implementation, operating, and reporting procedures for providing information assurance capabilities at the tactical, operational, and strategic levels, the Commands are becoming sensitive to the need and beginning to work toward the solutions.

5.5 CONSIDERATIONS

Since IO, IA, and now CIP have continued to develop, many organizations have restructured to handle the new requirements. When reorganizing, commanders consider many factors before making changes: chain of command, responsibilities, functions, manning, internal and external relationships, and many more. This section discusses some issues, as determined from interviews with representative from various organizations, for commanders to consider in the future.

5.5.1 Education and Training

The issue most raised in our interviews, from an IA perspective, was education and training. There are two levels to consider; system administrator and user level. Both are equally important.

As a result of ER97, system administrator training needed improvement and actions continue today to resolve that issue. This particular issue, though, requires continuous monitoring. As technology continues to advance, newer, faster equipment and more advanced security tools are being developed. To maintain the proper security level of their systems, system administrators and their assistants will require sustainment training security level of their systems.

The same is true for users, but not to the same degree. Users need awareness training so they understand the security requirement and can identify problems in the system as being possible penetrations. Users with remote access must be conscientious in following security practices.

For system administrators, formal education and training are available. Making time for training and hiring adequate assistants to fill in are the only considerations. For users, however, the solution is not as simple. Many organizations have instituted on-line training modules for users. While this system is convenient, it may prove to be inadequate without monitoring. Users may not understand how to implement a security practice properly or may even underrate the importance of that practice. Just as system administrators require verification, so do users. The best-trained system administrator cannot prevent a penetration caused by an untrained user. While training may take time and cause inconvenience, the results may alleviate possible major inconveniences.

5.5.2 Requirements

New concepts generate new requirements. A review of the new requirements, along with the current functions for the staff, will determine whether reorganization is necessary. For example, the establishment of the new organizations in DIA is indicative of new requirements that were not addressed completely under the current structure. Another consideration is that the staff section should be able to complete their work. With CIP as a new requirement, commanders will need to consider the workload of the current organization to determine how to handle the responsibilities.

5.5.3 Working Relationships

The staff process is an important consideration when deciding to reorganize. In many cases, the reorganization occurs because the staff has to adapt to meet the demands of the new task. Since that is already occurring, being able to identify the working relationships resulting from the change and instituting them will ease the reorganization process. The process change could be internal or external. An internal staffing change, for example, occurred as a result of Operation Solar Sunrise. Because IA has an everyday responsibility,

the tendency was to view the topic as a more administrative function. After Operation Solar Sunrise, operations personnel became more aware of the IA function. These personnel now understood the importance of the links between computers and the tools in place to protect them. Since that time there has been increased staff coordination between operators and IA personnel. With the advent of computer network defense, the IA responsibility takes on an operational aspect. This new aspect does not necessarily require a staffing change, but presents a point to consider in the process flow.

External working relationships change as well. Operation Solar Sunrise showed the need to coordinate with law enforcement when dealing with unidentified intruders in an information system. Even after the intruders are identified, the issue could remain law enforcement. Adjusting the staff process to deal with such a change is difficult but important. The treatment of an intrusion as a criminal investigation is different than responding to a military "attack." Understanding and adjusting to these types of changes are important considerations when reorganizing.

5.6 CONCLUSIONS

The continued development of IA, IO, and the emergence of CIP have caused many organizations to reorganize in order to meet increasing requirements. In some cases, almost a complete restructuring was necessary. As technologies advance, leaders will continue to review their structure to ensure they can handle the demand.

Appendix A Organizations

APPENDIX A
ORGANIZATIONS

This page intentionally left blank.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
Department of Defense	
Office of the Assistant Secretary of Defense (OASD(C3I)).....	A-6
Defense-wide Information Assurance Program (DIAP).....	A-14
Information Assurance Group (IAG)	A-18
The Joint Staff (JS).....	A-20
School of Information Warfare and Strategy (SIWS)	A-26
Department of the Army (DA)	A-30
Land Information Warfare Activity (LIWA).....	A-34
Department of the Navy (DoN)	A-36
Fleet Information Warfare Center (FIWC)	A-40
Naval Information Warfare Activity (NIWA)	A-44
United States Marine Corps (USMC)	A-46
Department of the Air Force.....	A-50
Air Force Information Warfare Center (AFIWC)	A-56
Defense Advanced Research Projects Agency (DARPA)	A-64
Defense Information Systems Agency (DISA)	A-68
Information Assurance Technology Analysis Center (IATAC)	A-78
Defense Intelligence Agency (DIA)	A-82
National Security Agency (NSA)	A-86
Executive Branch	
Executive Office of the President	
National Economic Council (NEC).....	A-92
National Security Council (NSC) Staff.....	A-94
Office of Management and Budget (OMB).....	A-96
Office of Science and Technology Policy (OSTP)	A-100
Department of Commerce (DoC).....	A-106
National Institute of Standards and Technology (NIST).....	A-110
National Telecommunications and Information Administration (NTIA)	A-116
Department of Energy (DOE).....	A-120
Lawrence Livermore National Laboratory (LLNL)	A-128
Los Alamos National Laboratory (LANL)	A-132
Oak Ridge National Laboratory (ORNL)	A-136
Pacific Northwest National Laboratory (PNNL).....	A-140
Department of Health and Human Services (DHHS).....	A-144
Department of Justice (DoJ)	A-148
National Infrastructure Protection Center (NIPC)	A-154
Department of State (DoS)	A-158
Department of Transportation (DOT)	A-162
United States Coast Guard (USCG).....	A-164
Department of the Treasury (Treas)	A-168

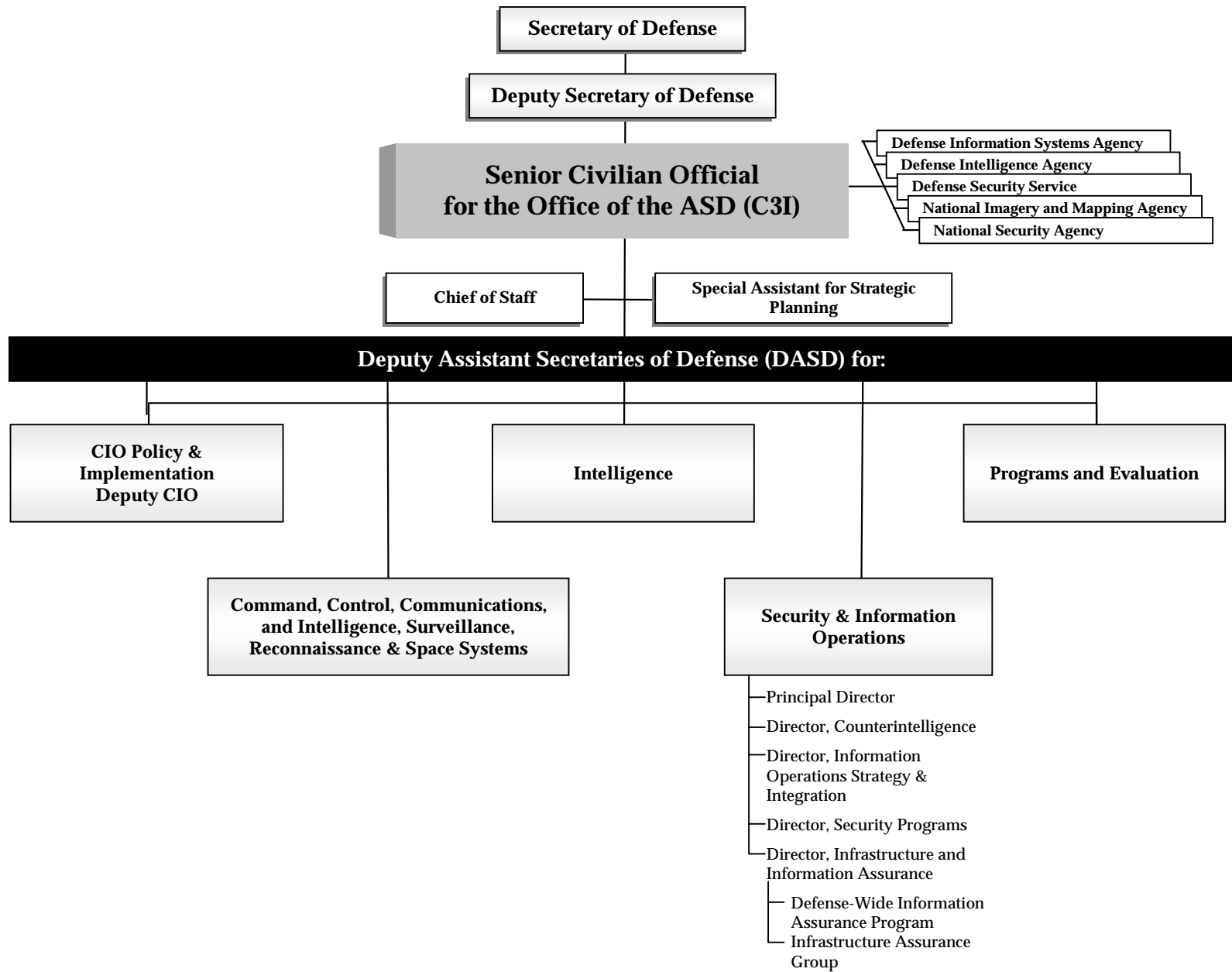
TABLE OF CONTENTS (Continued)

<u>Section</u>	<u>Page</u>
Independent Establishments and Government Corporations	
Central Intelligence Agency (CIA).....	A-174
Environmental Protection Agency (EPA).....	A-176
Federal Communications Commission (FCC)	A-180
Federal Emergency Management Agency (FEMA).....	A-184
Federal Reserve System (FRS)	A-188
Federal Trade Commission (FTC).....	A-192
General Services Administration (GSA)	A-196
National Aeronautics and Space Administration (NASA)	A-202
National Intelligence Council (NIC).....	A-206
National Research Council (NRC)	A-210
Nuclear Regulatory Commission (NRC)	A-216
United States Information Agency (USIA)	A-220
Legislative and Judicial	
Committees of the Senate.....	A-224
Committees of the House of Representatives	A-228
General Accounting Office (GAO).....	A-232



Department of Defense

This page intentionally left blank.



Organization: Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence (OASD(C3I))

Senior Information Operations Official:

Mr. Arthur L. Money (Acting), Assistant Secretary of Defense (C31)

Information Operations Point of Contact:

Col Robert J. Blunden, Jr., Director, Information Operations Strategy and Integration,
703-693-2157

Senior Information Assurance Official:

Mr. Richard Schaeffer, Director, Information Assurance, 703-695-8705,
shaefferr@osd.pentagon.mil

Senior Critical Infrastructure Protection Official:

Bonnie Hammersley, 703-697-3215

On-Line Resources:

OASD(C31) Homepage: <http://www.c3i.osd.mil>

Missions and Functions:

OASD(C3I) is charged with policy development, planning, resource management, fiscal, and program evaluation responsibilities in the areas of information assurance, information operations, and infrastructure protection.

Under the direction of the Secretary of Defense, the ASD(C3I) is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for C3I, information management (IM), information operations (IO), counter-intelligence (CI), and security countermeasures (SCM) matters, including warning, reconnaissance, and intelligence and intelligence-related activities conducted by the Department of Defense. In the exercise of these responsibilities, the ASD(C3I):

- Serves as principal staff assistant in carrying out the responsibilities of the Secretary of Defense as Executive Agent for the National communications System (NCS).
- Serves as the Department's Chief Information Officer.
- Serves as the Department's senior information security official.
- Serve as the principal DOD official responsible for establishing software policy and practices.

- Establishes and implements IM policies, processes, programs and standards to govern the development, acquisition, and operation of information technology (IT) and information systems by the DOD.
- Chairs the Major Automated Information System Review Council (MAISRC).
- Provides program management for the General Defense Intelligence Program, the Foreign Counterintelligence Program, and the Security and Investigative Activities Program.
- Serves as the principal DOD official responsible for preparing and defending the Department's C3I, CI, SCM, IM, and IT programs before the Congress.
- Assesses the responsiveness of intelligence products to DOD requirements.
- Participates, as appropriate, in the DOD planning, programming, and budgeting system for C3I, IM, IT, CI, IO, and SCM activities by reviewing proposed DOD resource programs, formulating budget estimates recommending resources allocations and priorities, and monitoring the implementation of approved programs.

In addition, the ASD(C3I) exercises authority, direction, and control over the following:

- Defense Information Systems Agency, (DoDD 5105.19)
- Defense Intelligence Agency, (DoDD 5105.21)
- Defense Investigative Service, (DoDD 5105.42)
- Defense Support Project Office
- C4I Integration Support Activity
- Defense Polygraph Institute
- DOD Security Institute
- Defense Personnel Security Research Center.

Exercises overall supervision over the:

- National Imagery and Mapping Agency (DoDD 5105.60).

Exercises staff supervision over the following:

- National Security Agency/Central Security Service (DoDD 5100.20)
- Air Force and Navy Special Intelligence Programs
- Electromagnetic Compatibility Analysis Center
- Defense Courier Service.

Goals for OASD (C3I):

- Ensure the continuity of mission-essential DOD operations despite Y2K disruption
- Implement effective programs for information assurance (IA) and critical infrastructure protection
- Build a coherent global network based on efficient and effective DOD information architectures and procedures (this includes establishing the internal technologies

processes within C31 as a model for information technology (IT) use within the government)

- Plan and implement joint and combined end-to end C3ISR and space integration
- Promote the development of a knowledge-based workforce within DOD
- Establish policies and budget priorities that will lead to the reinvention of intelligence for the twenty-first century (includes support to tactical forces, and renewal of clandestine capabilities)
- Develop and implement revised policies for information operations (IO), Security counterintelligence (CI)
- Promote electronic commerce and business process change throughout the functional areas of the department
- Foster the development of an advanced technology plan for information superiority.

Activities:

Information Operations Strategy and Integration

- Published DoD Directive (S) – 3600.2 Information Operations Security Classification Guidance
- Bilateral Information Operations Steering Group (BIOSG) established between DOD and Intelligence Community. Provides policy recommendations on Information Operations of mutual interests. ASD C3I performs secretariat function. Members include Community Management Staff, Deputy Director for Community Intelligence (DDCI), DDCI for Community Management, DCI General Counsel, Under Secretary of Defense (Policy), ASD, C3I, Joint Staff J3 and DOD General Counsel. The group acts on recommendations and resolving of issues raised by the Bi-lateral Information Operations Working Group (BIOWG).
- Assisted in the establishment of the Information Operations Technology Center (IOTC).

Information Assurance and Infrastructure Protection

As shown in the organization chart, OASD(C3I) is one of the few federal departments in which the functions of information assurance, information operations, and infrastructure protection are administered within a single staff agency. This assignment of responsibilities aids significantly in coordinating the many issues which are common to all three functional areas. The activities for information operations and information assurance are addressed in separate sections.

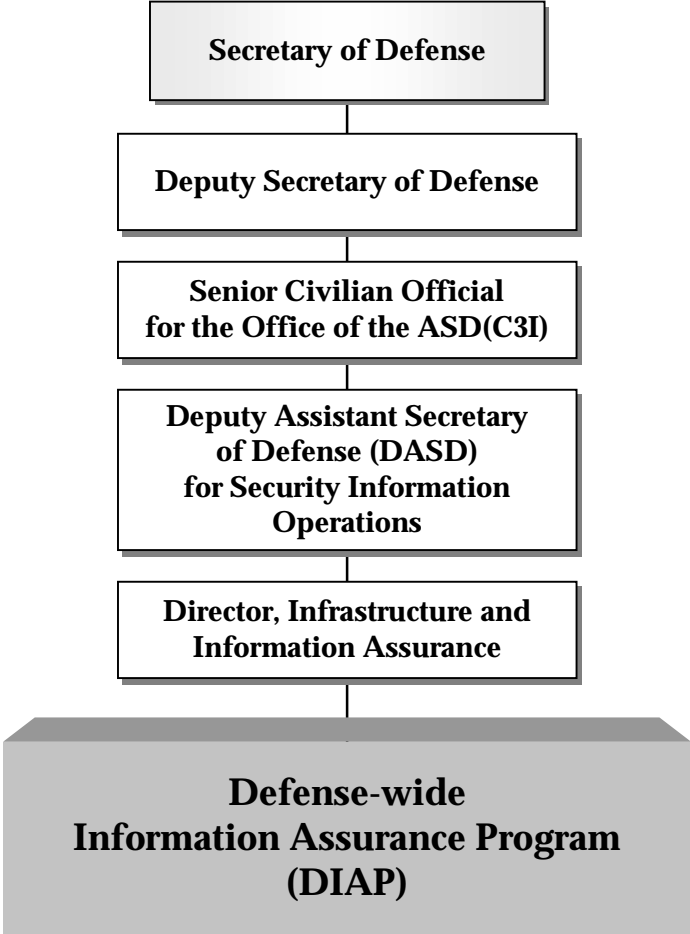
- The primary role for the office has been to oversee the preparation of the DOD Critical Infrastructure Protection Plan that was delivered to the national-level Critical Infrastructure Assurance Office in November 1998. The DOD plan will be coordinated with similar plans prepared by other federal Departments and Agencies through the efforts of the Critical Protection Working Group. Within the Department, the Critical

- Infrastructure Protection Working Group is coordinating the infrastructure protection activities.
- The plan provides responsibilities, coordinating instructions, and a life-cycle approach to protecting those functional infrastructures deemed critical by DOD in performing assigned missions and functions. These functional infrastructures include:
 - Space
 - Public works
 - Logistics
 - Transportation
 - Financial Services
 - Personnel Affairs
 - Health Affairs
 - Emergency Preparedness
 - Defense Information Infrastructure
 - Command and Control and Communications
 - Intelligence, Surveillance, and Reconnaissance.
- Functional infrastructure experts serve as Liaison Officials between the Office of Critical Infrastructure Protection and those organizations and activities having responsibilities for operating and maintaining the functional infrastructures. These experts serve as the Critical Infrastructure Protection Coordinating Activity and are co-located with the offices of the Defense Information Assurance Program to capitalize on the DIAP expertise in the area of information systems security. The Liaison Officials will also draw on the products of the Information System Security Program. These experts will be responsible for preparing plans to implement the DOD infrastructure protection plan. These “sector” plans will identify the relation of the infrastructure to DOD missions and functions. These plans will be similar to operational architectures.
- In addition to the above efforts, the Department has initiated a Critical Asset Assurance Program (CAAP) as outlined in DoDD 5160.54. The CAAP will provide a comprehensive and integrated decision support environment to represent the relationship between critical assets and force readiness and operations in peace, crisis or war that can be used to assess the dependencies, vulnerabilities and effects of disruption or loss of critical assets or supporting infrastructures on their plans and operations.
- Instituted Defense-wide Information Assurance Program (DIAP). This organization spans across stovepipes to help level out IA. This organization will provide advice to senior steering group on such things as POM submission and resources, and requirements.
- The Department recently established the Defense Information Assurance Program and a supporting staff. The DIAP is intended to:
 - Integrate and provide effective program oversight of the Department’s IA activities.
 - Provide the structure that will enable the Department to monitor and coordinate the IA readiness of the Department.
 - Establish IA responsibilities and authorities of DOD Components and other personnel and organizations.
 - Ensure a partnership between OS and DOD Components based on integrated planning, programming and budgeting, decentralized execution, and continuous centralized oversight.

- The DIAP and associated activities will be organized around the following functional areas:
 - Readiness
 - Human Resources
 - Operational Policy
 - Acquisition Support and Product Development
 - Architectural Standards and System Transformation
 - Security Management
 - Operational Monitoring
 - Research and Technology.
- The existing Information Assurance Group and its working groups identified below will be incorporated over time and based on experience into the DIAP structure:
 - IA Policy Working Group
 - Joint IA Tools Working Group
 - Joint IA Operations Working Group
 - Multilevel Security Working Group
 - Secret and Below Interoperability Working Group
 - Education, Training, Awareness, and Professionalization Working Group
 - Certification and Accreditation Working Group.
- The US Security Policy Board will be reconstituted based on a study being conducted by General Larry Welch, President of the Institute of Defense Analyses. It is also likely that a security commission similar to the Joint Security Commission will be established to review current security issues.
- Roles and responsibilities among the players in the IA, IO, and IP areas are still emerging and being defined. One of the major impediments to a clear definition of roles and responsibilities is the lack of common terms and definitions. The IO office is considering revising DoDD S-3600.1 to provide the needed terms and definitions.
- Issues common to IA, IO, and IP are being addressed by the three respective offices in OASD(C3I). The head of Security and Information Operations and the Principal Director have made coordination of these issues and integration of the areas a major focus of their efforts.
- The IA strategy has evolved over time and includes concepts such as defense-in-depth, awareness, training, and education, dealing with shared risk. The DIAP will provide an operational approach to implementing the concepts.
- Some of the primary activities of the past year include:
 - More leadership emphasis on information assurance. The DEPSECDEF has been a visible and vocal proponent of information assurance which helps increase awareness throughout the Department.
 - Establishing information assurance training and certification requirements for users, administrators, and maintainers of DOD information systems. A follow-on Integrated Product Team has been formed to examine the detailed requirements and solutions to IA professionalization, education, training.
 - Establishing an information assurance vulnerability alert system which provides for the timely dissemination of vulnerability alerts, acknowledging receipt of the alerts, and reporting corrective action.

- The development of an information assurance series of directives to replace those dealing with automated information systems security. The first in the series, DoDD 8500.XX is working.
- Establishing a rigorous information assurance red teaming methodology. This will ensure a consistent approach, in part, to measuring IA readiness.
- Opening up a dialogue on IA with Allies and Coalition Partners. Some representative activities include a Quadripartite (US, UK, France, and Germany) IA Experts Group and a Y2K Experts Group.
- The Department of Defense established the Office of Critical Infrastructure Protection in June 1998 to guide the DOD implementation of Presidential Decision Directive 63 and serve as the primary interface between the national-level Critical Infrastructure Coordinating Group and the Department. The Office is staffed with eight personnel and was created with billets from the former Infrastructure Protection Directorate in the Office of the Under Secretary of Defense (Policy), the Information Operations Office within OASD(C3I), and the Communications Interoperability Support Agency.
- Several Components have conducted or sponsored a number of "Red Team" assessments of their operational readiness to protect against, detect, and react to potential adversarial information operations. These teams provide a highly skilled "opposing force" (OPFOR) and support the individual commanders with an additional measure of risk management.
 - The Department, in gauging the IA-component of unit and force operational readiness, intends to conduct additional periodic independent assessments of the IA processes, systems, and organizations. Such independent assessments provide an impartial appraisal of some of the vulnerabilities that could be exploited by an adversary.
 - To ensure that the use of Red Teams is consistent, two documents have been drafted to support DOD Red Teams. The first document provides a methodology for designing, developing, assembling, and conducting Defense-Information Assurance Red Teams (D-IART). The purpose, commonality of structure, and meaningful and comparable results. This document is in the process of review prior to promulgation. The second draft document is the DOD Information Operations Policy concerning Red Teams. These activities are consistent with and implement the recommendation of the DSB concerning development of procedures for employment of Red Teams (recommendation #2.e.(2)).

This page intentionally left blank.



Organization: Defense-wide Information Assurance Program (DIAP)

Senior Information Operations Official:

CAPT J. Katharine Burton, USN, DIAP Staff Director, 703-602-9988, DSN 332-9988,
katharine.burton@osd.pentagon.mil

Information Operations Points of Contact:

Ms. Marjorie York, Human Resources, 703-602-9974, DSN 332-9974,
marjorie.york@osd.pentagon.mil

Ms. Marti Pickens, Policy Integration, 703-602-9981, DSN 332-9981,
pickensm@osd.pentagon.mil

Mr. Mark Viola, Security Management, 703-602-9984, DSN 332-9984,
mark.viola@osd.pentagon.mil

Mr. Jim Christy, Operational Environment, 703-602-9982, DSN 332-9982,
james.christy@osd.pentagon.mil

Mr. Ben Gaddy, Operational Environment, 703-602-9993, DSN 332-9993,
benjamin.gaddy@osd.pentagon.mil

Ms. Martha Leonette, Architectural Stands and System Transformation, 703-602-9969,
DSN 332-9969, leonettm@osd.pentagon.mil

Mr. Marvin Jennings, Acquisition Support and Product Development, 703-602-9978,
DSN 332-9978, marvin.jennings@osd.pentagon.mil

Ms. Chris McBride, Research and Technology, 703-602-9985, DSN 332-9985,
christina.mcbride@osd.pentagon.mil

Mr. Steve Clark, Program Development and Integration, 703-602-9975, DSN 332-9975,
steve.clark@osd.pentagon.mil

Missions and Functions:

The DIAP Staff consists of a core cadre of OSD personnel, augmented by participating Component representatives. The DIAP Staff combines functional and programmatic skill to build a comprehensive Defense-wide approach to IA. The Staff will leverage its expertise to ensure the protection, detection and response capabilities required for the DII are continuously maintained to support the spectrum of Defense operations and activities.

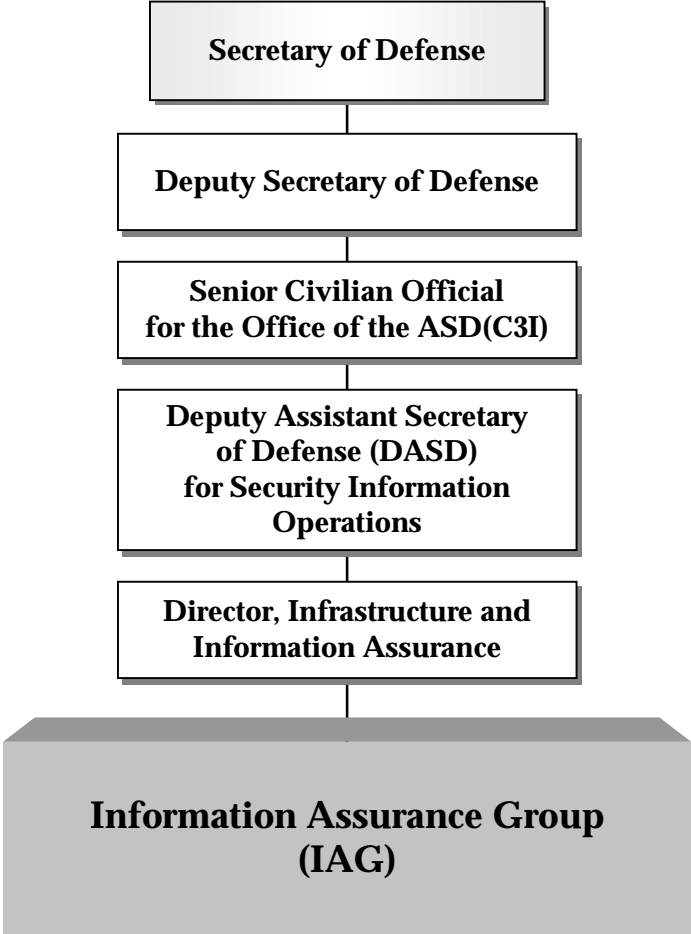
The DIAP will establish the DOD management processes and structure that will:

- Integrate, and provide effective program oversight of, the Department's IA activities.
- Provide the structure that will enable the Department to monitor and coordinate IA readiness.
- Ensure the DIAP is a partnership between OSD and its Components based on integrated planning, programming and budgeting, decentralized execution and continuous centralized oversight.

Activities:

- Provide for sufficient, adequately trained and educated personnel to conduct IA functions throughout the DOD.
- Provide for consistent implementation of IA-related policies throughout the DOD.
- Provide for the incorporation of appropriate security services which allow and promote global interoperability while preserving legitimate law enforcement and national security purposes.
- Provide for the continuous visibility of the Department's and the IC's IA operational readiness postures through the appropriate monitoring of enterprise information systems and through other intelligence and law-enforcement sources.
- Provide for the integration of adequate IA technologies, products and supporting procedures in the information technologies and information systems and networks acquired by the DOD.
- Provide continuous improvement in the Department's IA readiness posture through disciplined, performance-based investments in security-enabled IT acquisitions.
- Provide for the research and development of IA technologies and techniques consistent with current and anticipated DOD mission needs and changes in information technologies.
- Provide for the oversight, coordination and integration of the Department's IA resource program.
- Provide a "big picture" of the Department's IA posture that identifies redundancies, incompatibilities and general shortfalls in IA investments, and deficiencies in resources, functional and operational capabilities.

This page intentionally left blank.



Organization: Information Assurance Group (IAG)

Senior Information Assurance Official:

CAPT J. Katharine Burton, USN, DIAP Staff Director, 703-602-9988, DSN 332-9988,
katharine.burton@osd.pentagon.mil

Information Assurance Points of Contact:

Ms. Marti Pickens, Policy Integration, 703-602-9981, DSN 332-9981,
pickensm@osd.pentagon.mil

On-Line Resources:

IAG Homepage: <http://www.disa.mil/infosec/iag.html>

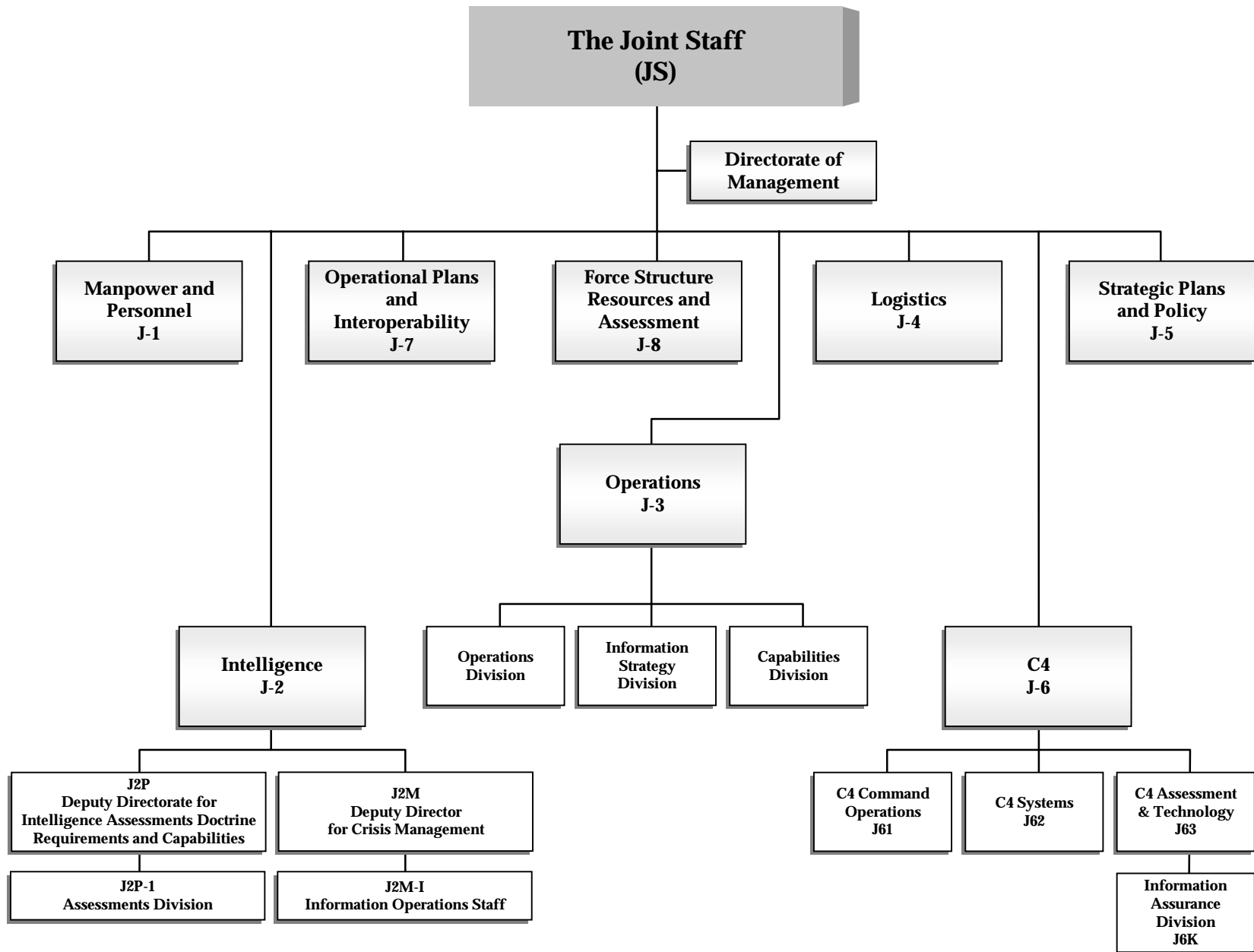
Missions and Functions:

Serve as the Department's principal IA forum to:

- Provide coordinated IA advice and recommendations to the Director, Information Assurance, through the Defense-wide Information Assurance Program (DIAP) Staff Director.
- Recommend and support coordinated Defense-wide IA policies, strategies and technologies to mitigate information systems vulnerabilities.
- Recommend coordinated and synchronized DOD positions, and develop and implement plans and programs on all issues involving the protection of the Defense and supporting non-Defense information systems.
- Strengthen Defense IA expertise and involvement in the consideration of equities and interests in areas of IA policy, security and defensive countermeasures.
- Review DOD IA programs and recommend initiatives to ensure the provision and optimization of resources consistent with IA policies, strategies and implementation plans.

Activities:

- Consider the issues, problems and equities presented during meetings and other IA fora and provide guidance or direct specific actions to be taken.
- Bring to the attention of the Director, Information Assurance, and the Senior DIAP Steering Group, as appropriate, issues that require their review or resolution.
- Identify responsible Services, Agencies and individuals to ensure action is taken to implement IAG decisions.
- Authorize the establishment of IAG working groups and integrated process teams to address various functional issues.



Organization: Joint Staff (JS)

Senior Information Operations Official:

Bruce A. Wright, Brig Gen, USAF, J-39, 703-695-0375
Thomas F. Enright, CAPT, USN, DJ-39, 703-614-9496

Information Operations Points of Contact:

John Brownell, CAPT, USN, Capabilities Division, 703-695-3332, brownejm@js.pentagon.mil
Thomas McCaffrey, CAPT, USN, Programs Branch, 703-695-3348,
mccafftm@js.pentagon.mil
Timothy McCully, CAPT, USN, Policy Branch, 703-695-3343, mcculltv@js.pentagon.mil
Robert Trost, COL, USA, Information Strategy Division, 703-695-5080,
trostrw@js.pentagon.mil
David Valcourt, COL, USA, Operations Division, 703-614-2092, valcoudp@js.pentagon.mil

Information Assurance Points of Contact:

Patrick Lusk, COL, USA, Information Assurance Division, 703-614-2918

On-Line Resources:

JS Homepage: <http://www.dtic.mil/jcs>

Missions and Functions:

Intelligence, J-2

The Directorate for Intelligence, J-2, provides all-source intelligence to the Joint Chiefs of Staff, Office of the Secretary of Defense, Joint Staff, and unified commands.

J-2 is unique on the Joint Staff in that it is also part of the Defense Intelligence Agency, a combat support agency. J-2 draws deeply on the DIA's broad range of capabilities to accomplish its mission and functions.

The J-2 appraises the chairman of foreign situations and intelligence issues relevant to current operational interests and potential national security policies, objectives and strategy. This includes providing indications, warning and crisis intelligence support, supporting unified command intelligence requirements, developing joint intelligence doctrine, developing joint architecture, coordinating support requirements, and providing targeting support.

Operations, J-3

The J-3 Operations Directorate is where all the Joint Staff's planning, policies, intelligence, manpower, communications and logistics functions are translated into action.

This is the directorate that moves military forces, conducted detailed operational briefings to the national leadership and serves as the operational link between the warfighting commanders in chief and the National Command Authority.

The J-3 assists the chairman in carrying out his responsibilities as the principal military advisor to the National Command Authority by developing and providing guidance to the combatant commands and by relaying communications between the authority and the unified commanders regarding current operations and plans. J-3 is involved in every aspect of the planning, deployment, execution and redeployment of U.S. strategic and conventional forces in response to worldwide crises.

The director for operations, a three-star flag officer, is supported by a two-star vice director and four principal deputy directors for operations – a one-star deputy director for current operations, a two-star deputy director for national systems support a one-star deputy director for current readiness and capabilities and a one-star deputy director for information operations.

The deputy director for current operations is responsible for the National Military Command Center operations and command and control systems, ongoing current operations and future plans in support of the regional and functional commanders in chief. Five one-star deputy directors for operations and their operations watch teams manage ongoing operations and National Military Command System emergency action procedures.

The deputy director for national systems support organization provides guidance on the effective operation of national systems.

The deputy director for readiness and capabilities provides functional expertise on joint readiness and key warfighting capabilities and in the areas of special operations, reconnaissance operations, space operations, counternarcotics, and nuclear operations.

The deputy director for information operations is responsible for IO policy and doctrine; provide support to regional and functional commanders in chief; and provide functional expertise in military deception, operations security (OPSEC), counterintelligence, electronic warfare, computer network attack/defense, and psychological operations.

C4 Systems Directorate, J-6

As the Joint Staff experts on C4, the mission is to:

- Provide the CJCS advice and recommendations on C4 matters.
- Support warfighters from the CINC to the shooter.

- Lead the C4 Community.
- Oversee support for the National Military Command System.
- Lead in identifying and resolving military aspects of information-based issues of national importance.

The Information Assurance Division (J6K) mission is to be the lead element for the Director, J6 in all matters of Command, Control, Communications and Computer Systems related to Information Assurance. J6K also provides technical C4 and IA expertise to the Joint Staff Deputy Director for Information Operations (IO) (J39).

The IA issues addressed by J6K range from current, near-real-time computer network attacks to long range IA policy development affecting DOD CINCs, Services and Agencies. The number of IA issues requiring Joint Staff attention has rapidly expanded over the last few years as DOD has strengthened its efforts to protect and defend its information and information systems.

Activities:

Intelligence, J-2

J-2 is the focus for crisis intelligence support to the national defense leadership and military commanders. It fields requests for information or analysis and ensures military commanders receive intelligence reports as quickly as possible.

During crisis operations, J-2 raises the level of support to the warfighters and decisionmakers by marshaling increased analytic focus in Washington and by providing a multiagency national intelligence support team directly to the warfighter.

Operations, J-3

- Doctrine: Joint Publication 3-13, *Joint Doctrine for Information Operations* published 9 October 1998. Working JP 3-51, *Electronic Warfare in Joint Military Operations*. Studying the future direction of JP 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*.
- CJCSI 3210.01A, *Joint Information Operations Policy* published 6 November 1998.
- The Joint Warfighter Capability Assessment (JWCA) process includes studies of offensive and defensive capabilities employed to conduct information operations, emerging technologies, and intelligence support to IO. Additionally, the JWCA includes an effort to examine Service and Agency Program Objective Memorandum submissions relative to the Defense Planning Guidance and CINC requirements.

C4 Systems Directorate, J-6

J6K's IA strategy addresses eight primary issue areas: threat, personnel and training, policy and doctrine, assessments, technology, exercises, requirements, and operations:

- Ongoing assessments of current threats include evaluating recent cyber attacks, coordinating with JTF/DISA ASSIST, and providing technical support to PAO, legal or law enforcement organizations.
- Ongoing training and education initiatives include providing periodic visits and IA-related briefing to a broad defense academic community, and publishing this annual Information Assurance Legal and Regulatory publication, and the monthly Information Assurance Digest.
- Supports human resources-related efforts to develop certification standards for network operators and system administrators that will define the training to maintain/retain quality network security personnel.
- Represents IA requirements for review in the Joint Staff Joint Warfare Capabilities Assessment (JWCA) process within primarily the C2 JWCA and IO JWCA when required. Solicits and collects IA requirements from CINCs, Services and Agencies to represent joint concerns in the various formal PPBS/Requirements processes (Defense Planning Guidance, Program Review Group, Defense Resources Board, Chairman's Program Assessment, Chairman's Program Review, Joint Requirements Oversight Committee, and Joint Requirements Board).
- Updating the various Joint Staff publications (for example CJCSI 6510.01, Defensive Information Warfare Implementation, and CJCSI 3210.01, Information Warfare Policy) to reflect current IA policies and doctrine. Recent activities involve drafting publications concerning Computer Network Defense/Attack (CND/CNA) Rules of Engagement (ROE), Information Conditions (INFOCON) and IA Vulnerability Alert (IAVA) reporting criteria.
- Supporting various international efforts to include acting as the US Representative to NATO INFOSEC SC (8 sub groups), the US Delegation Head to CCEB INFOSEC ISME.
- Supporting various national efforts to include acting as the NSTISSC Joint Staff representative (six sub groups), and contributing to the Critical Infrastructure Program (CIPWG, CICG, CIAO WG), and the Cryptologic Senior Oversight Group.
- Within the DOD, J6K is responsible for the GNIE IA working group, acts as the SABI/T-SABI coordinator, is assigned as MCEB INFOSEC Panel Chairman, and participates in the ASD(C3I)'s IA Group (IAG) (5 major working groups), MLS/Education, Training, Awareness, & Professionalization/IA Policy/IA Tools/Operations, Critical Infrastructure Program, Defense-wide IA Program (DIAP), Joint Key Management Infrastructure Working Group (PKI, EKMS, etc.), and the Web Review Task Force.
- In the area of assessments, J6K is supporting the development of IA readiness metrics, coordinating with NSA/JC2WC concerning Red Teaming efforts, advocating the use of the Vulnerability Assessments Program, increasing the IA impact to PBBS (DPG, JSCP, PRG, etc), and coordinating the Joint COMSEC Monitoring Activity.

- In the technology area, J6K coordinates the GCCS Security Testing and Evaluation activities, the Automated Intrusion Detection Environment (AIDE) ACTD IA activities, the Public Key Infrastructure (PKI) implementation, and the Electronic Key Management System (EKMS) standup.
- In the area of exercise support, J6K provides National/DOD IA exercise coordination to implement information warfare in exercises and encourage greater involvement with the JBC.

**School of Information
Warfare and Strategy
(SIWS)**

Organization: School of Information Warfare and Strategy (SIWS)

Senior Information Operations Official:

LTG Dick Chilcoat, President, National Defense University, 202-685-3922

Dr. Robert D. Childs, (Acting) Dean of the Information Resources Management College,
202-685-3886

Dr. Daniel T. Kuehl, Chair, Information Operations Department, 202-685-2257

Information Operations Points of Contact:

Tom Czerwinski, Professor, SIWS, 202-685-2245

Dr. Fred Giessler, Professor, SIWS, 202-685-2258

Dr. Charles E. Tompkins, Professor, IRMC, 202-685-3629

Lt. Col. Michael S. Wills, USAF, Professor, SIWS, 703-614-3586

On-Line Resources:

NDU Homepage: <http://www.ndu.edu>

Missions and Functions:

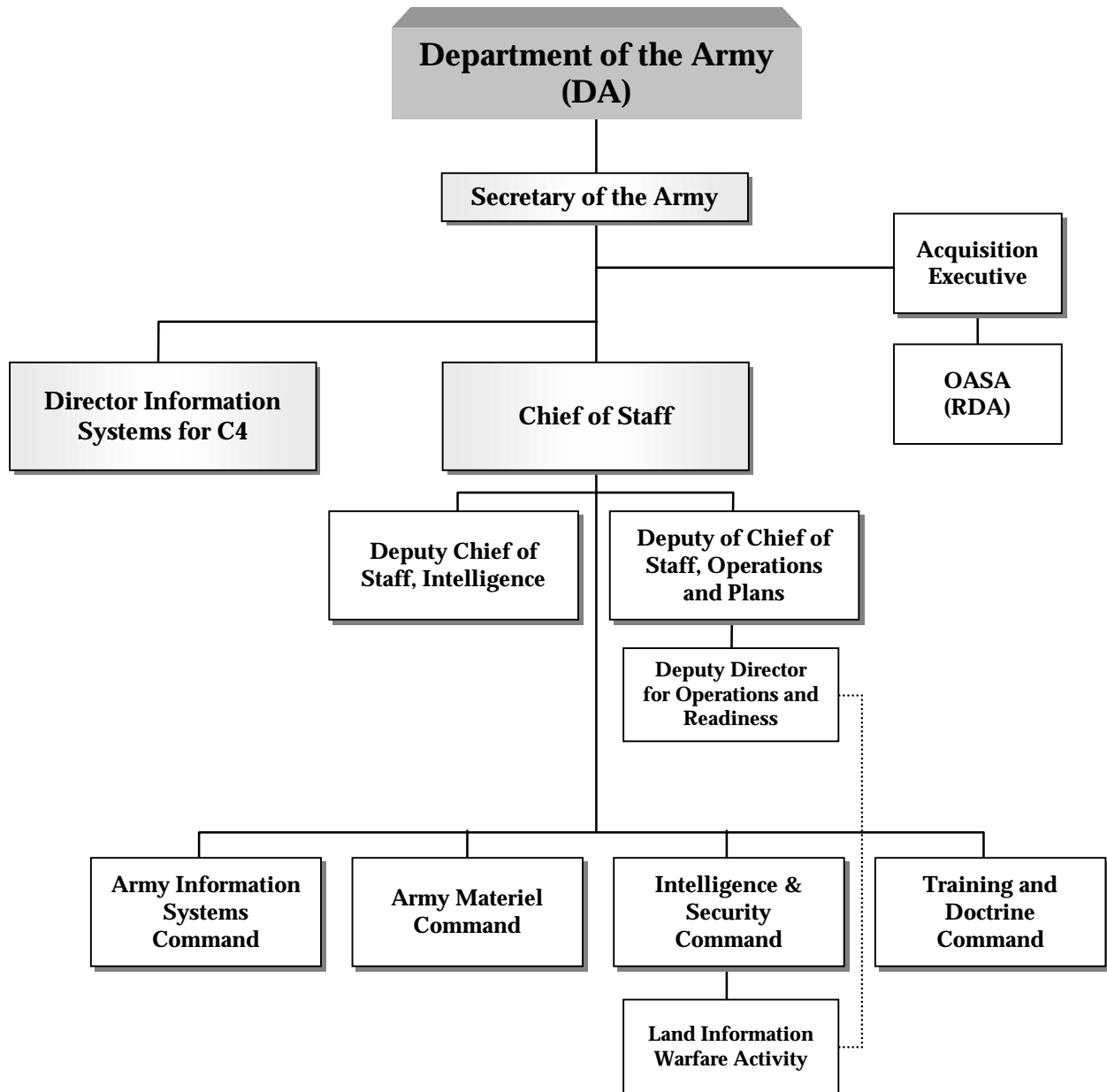
School of Information Warfare and Strategy (SIWS) is administratively organized within the Information Operations Department, Information Resources Management College (IRMC), National Defense University (NDU), located at Fort McNair, Washington DC.

The School of Information Warfare and Strategy was chartered by the CJCS in August 1994 to teach an experimental two-year pilot program dedicated to the study of the information component of national power. This senior joint professional military education program graduated a total of 48 students (16 in Academic Year 95, 32 in AY 96) from its 10-month senior level (war college) program. The stand alone senior-level program was then terminated, but in recognition of the importance of information strategies, the President of the University assigned a new mission to the School of Information Warfare & Strategy, emphasizing 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. In the third tier, the SIWS manages the Information Strategies Concentration Program (ISCP), a focused group of elective courses and other activities that concentrate on the information component of national power. The School of Information Warfare and Strategy will continue to offer its very popular 5-day Introduction to Information-Based Warfare 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. As part of IRMC's Chief Information Officer Certificate program, SIWS offers a 5-day intensive course in Information Operations, and another in Information Assurance.

Activities:

- The Information Strategies Concentration Program (ISCP) is the keystone of the National Defense University (NDU) effort to prepare strategic leaders for the national security implications of the information age. The ISCP offers resident students of the Industrial College of the Armed Forces (ICAF) and the National War College (NWC) an opportunity to explore the information component of national power--the capabilities, vulnerabilities and limitations of information tools, their application to national security--through a blend of concentrated electives and field studies. The ISCP traces its roots back to the 10-month senior-level joint Information Warfare and Strategy pilot program chartered by the Chairman, Joint Chiefs of Staff in 1994.
- The pilot program was completed in 1996 and its charter revised by the Vice Chairman to increase the opportunities for all NDU students to study the national security implications of the information age, its associated technologies, and synergistic societal developments. In addition to incorporating information age concepts into the ICAF and NWC core curricula and electives, the new NDU approach--the ISCP--immerses approximately 50 ICAF and NWC students in a program designed to complement and enrich the core curriculum of their respective college with four elective courses and a two week field study focused on the information component of national power. By the end of Academic Year 99 the ISCP will have graduated nearly 150 students, many of whom serve in critical information-related positions across the DOD.

This page intentionally left blank.



Note: Dashed line represents operational testing authority.

Organization: Department of the Army

Senior Information Operations Official:

LTG Thomas Burnette, Deputy Chief of Staff, Operations and Plans (DCSOPS),
703-695-2904

LTG Claudia Kennedy, Deputy Chief of Staff, Intelligence (DCSINT), 703-695-3033

LTG William Campbell, Director of Information Systems for C4 (DISC4), 703-697-7494

Information Operations Points of Contact:

COL Brian Fredericks, ODCSOPS, Chief Information Operations Division, DAMO-ODI,
ODCSOPS, 703-695-1119

COL Day, Director, ODCSINT, Intelligence Policy, DAMI-PO, ODCSINT, 703-604-2475

COL Brown, ODISC4, Chief Information Assurance Division, ODISC4, 703-604-7575

Senior Information Assurance Official:

LTG William Campbell, Director of Information Systems for C4 (DISC4), 703-697-7494

Information Assurance Points of Contact:

COL Brown, ODISC4, Chief Information Assurance Division, ODISC, 703-604-7575

On-Line Resources:

Army Homepage: <http://www.army.mil>

External Relationships:

In fulfilling its oversight responsibilities for Information Operations the Department of the Army closely coordinates with the following agencies and organizations:

- Office of the Secretary of Defense
- Various Defense Agencies & Activities
- The Joint Staff
- Joint Command and Control Warfare Center (JC2WC)
- The Department of the Navy
- The Department of the Air Force
- National Infrastructure Protection Center (NIPC).

Information Operations (IO) 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 IO throughout the Army.

The Army uses several steering groups to help integrate IO into the Service and to provide executive oversight of the program:

- The monthly Council of Colonels (CoC) is attended by all major players with a vested interest in IO. This recurring meeting: identifies IO related issues, monitors IO plans, coordinates actions and resolves outstanding issues.
- The General Officer Steering Committee (GOSC) is hosted quarterly. This meeting is chaired by DAMO-OD, DCSOPS and includes representatives charged with implementing IO. The GOSC validates IO strategy, resolves issues, and prioritizes IO events.
- The Senior IO Review Committee (SIORC) consists of the principle members of the IO Triad: DCSOPS, DCSINT, and DISC4. Additionally, the Commander of the Combined Arms Command (CAC). The SIORC provides overall IO direction and approves Army IO vision.
- Currently the DISC4 hosts and conducts separate CoC and GOSC for C2 protect. This allows technical and funding issues relating to C2P to be discussed in greater detail.

Mission and Functions:

To ensure unity of effort, Headquarters, Department of the Army has established an IO triad consisting of the offices of the DCSOPS, DCSINT, and DISC4, with DCSOPS as the lead.

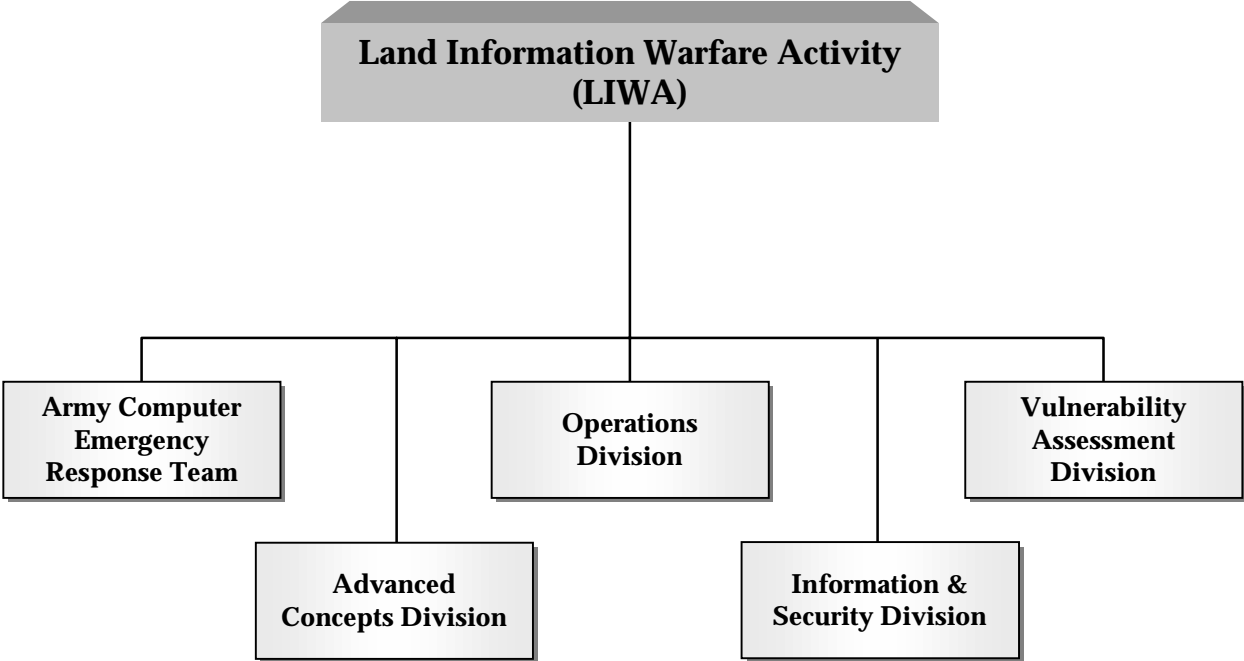
- The DCSOPS coordinates, integrates resources and prioritizes IO in the Army. He ensures the Army in the field is organized, trained, and equipped to conduct IO. Operational issues concerning IO are handled within the Directorate for Operations, Readiness, and Mobilization (DAMO-OD). DAMO-OD through its Information Operations Division (DAMO-ODI) has operational tasking authority and oversight of the Land Information Warfare Activity (LIWA).
- The DCSINT ensures that the intelligence community provides timely support to Information Operations. In coordination with DCSOPS and DISC4, the DCSINT is responsible for threat definition, establishment of policy and integrating counter-intelligence support into IO.
- The DISC4, as the Army's Chief Information Officer, is responsible for Defensive Information Operations, initiatives and policy to include the education and training of users and system administrators to address growing information system threats.

Activities:

- The Army has aggressively pursued the integration of Information Operations for two reasons: First, in this increasingly technological era, the Army recognizes the inherent value of information as both a combat multiplier and as a target to be exploited or attacked. Secondly, information issues permeate the full range of military operations, from peace through war; and are critical for force protection at the tactical and operational echelons. 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, the right place, and with the right weapons or resources.

- The Army's current doctrinal framework for the conduct of IO is contained in FM100-6. The three components of IO are: Information Systems, Relevant Information and Intelligence, and Operations. These integrated components apply to all facets of the Army mission and are part of both offensive and defensive operations. The recently approved JP 3-13, Doctrine for Joint IO, will be incorporated into the next edition of FM100-6, scheduled for initial draft publication in the third quarter of FY 99.
- As a result of the Army's involvement in Bosnia, and with the LIWA at the forefront of the Army's IO effort, significant lessons learned have been captured. These lessons have been refined into tactics, techniques and procedures (TTP), and will be incorporated into the next edition of FM100-6. These products are available through the Center for Army Lessons Learned at Ft. Leavenworth, KS.



Organization: Land Information Warfare Activity (LIWA)

Senior Information Operations Official:

COL James Gibbons, Director Land Information Warfare Activity, 703-706-1791

Information Operations Points of Contact:

Mr. Anthony Portare, Deputy Director, LIWA, 703-706-2263
LTC Robert Vrtis, Director of Operations, LIWA, 703-706-2262

On-Line Resources:

<http://www.acert.belvoir.army.mil>

External Relationships:

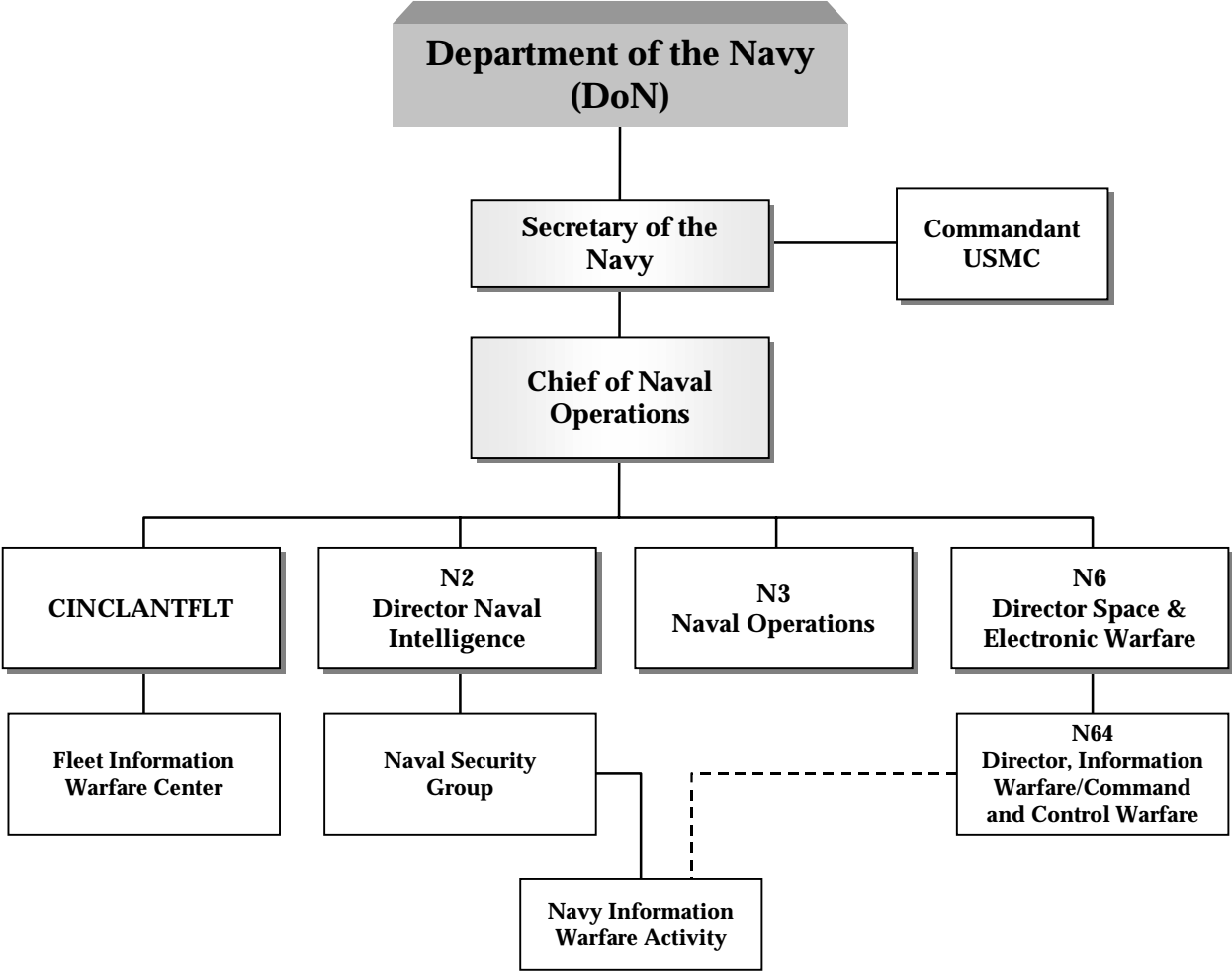
The LIWA coordinates with National, Joint, and Service IO centers to synchronize operations and to exchange information across the operational continuum.

Missions and Functions:

- LIWA's mission is to integrate Information Operations into the Total Army. Assist the warfighter in successfully executing the mission by planning and synchronizing information operations in support of the Commander's Intent. Simultaneously, LIWA enhances Total Army Force Protection by coordinating a proactive defense of command and control infrastructure.
- Established in May 1995, the LIWA is a subordinate element of the U.S. Army Intelligence and Security Command, Fort Belvoir, Virginia. LIWA is not however, an intelligence organization. LIWA receives its' mission tasking and guidance directly from the DCSOPS.
- LIWA is the operational focal point for Army IO and provides "full spectrum" IO to the Army's Land Component Commanders. Additionally, the Army Computer Emergency Response Team (ACERT), as a subordinate element of LIWA, has been designated as the Army component for the JTF-CND.

Activities:

- The Army is in the process of incorporating LIWA capabilities into day-to-day operations. LIWA capabilities are addressed in the FM100-6 and an official Table of Distribution and Allowance; to refine LIWA staffing, has been developed.
- ACERT: One of LIWA's key functions is to provide computer emergency response support to Army forces.



Organization: Department of the Navy (DoN)

Senior Information Operations Official:

VADM Thomas B. Fargo, Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5), 703-695-3709

VADM Robert J. Natter, Director, Space, and Information Warfare, Command and Control, (N6), 703-695-3239

Commander, Naval Security Group Command/EA for IW

Information Operations Points of Contact:

Capt James Newman, USN, Director, Information Warfare Division (N64), Office of the Chief of Naval Operations, 703-601-1262

Capt Robert West, USN, Deputy Director, Information Warfare Division (N64B), Office of the Chief of Naval Operations

Louise M. Davidson, Defensive Information Warfare/INFOSEC Branch (N643), Office of the Chief of Naval Operations, 703-601-1278

Staff Ops 7 Plans, Special Warfare Objective (OPNAV N513)

Assistant Chief of Staff for IW/C2W, CNSG (CNSG N6)

Senior Information Assurance Official:

Mr. Dan Porter, DoN Chief Information Officer

Information Assurance Points of Contact:

Louise M. Davidson, Navy, CNO N643, 703-601-1278

Gilda MacKenna, USMC, C4I/CPM, CNO N34

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>

N6 Homepage: <http://copencus.hq.navy.mil>

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, Information Warfare, Command and Control (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 designed 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 October 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 Team (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,

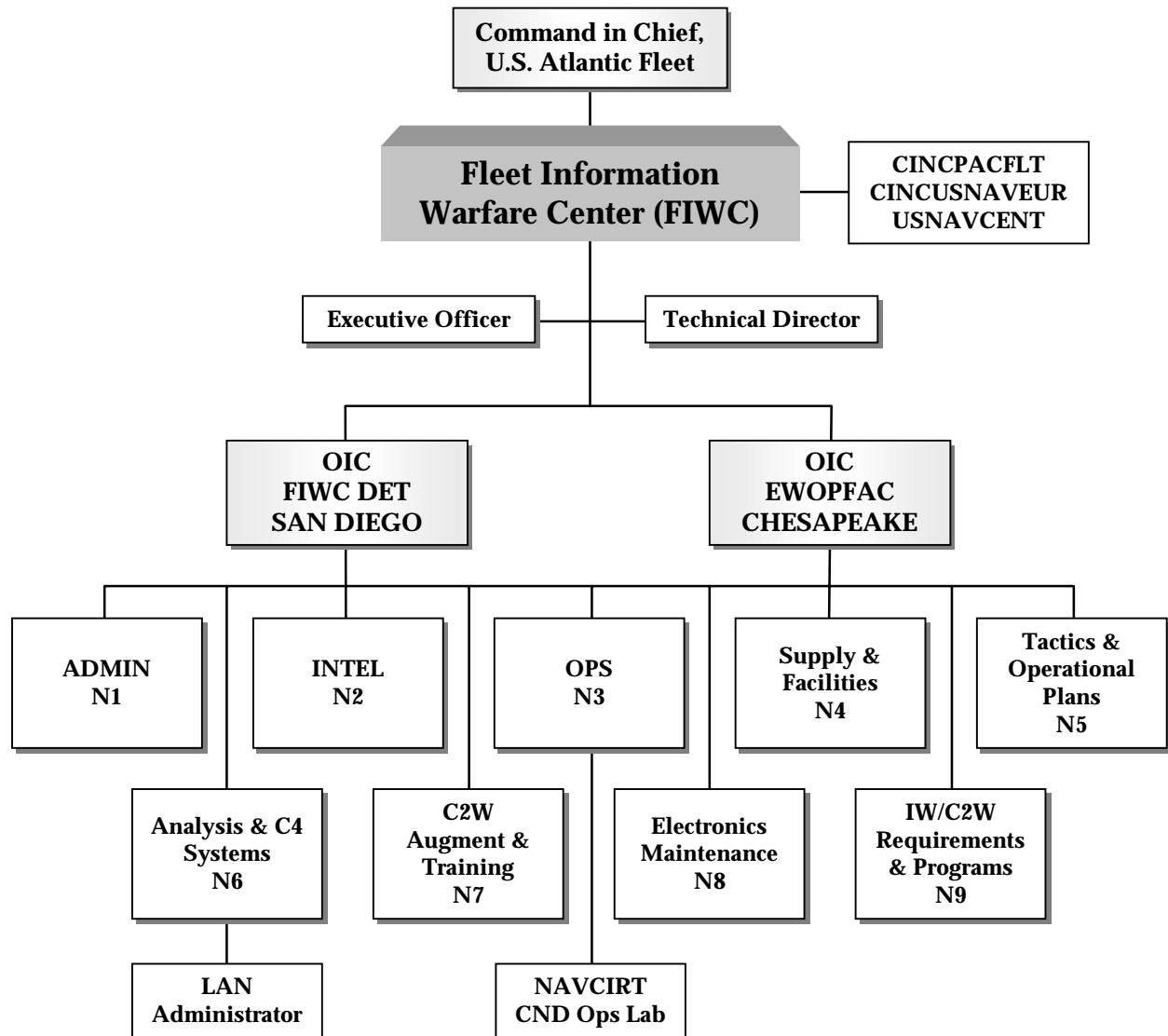
and evaluates/assesses new information technologies, competitive architectures, and advanced concepts for Navy defensive IW systems.

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.

Activities:

- To continually reduce and manage the overall risk to Naval systems by improving the performance and their ability to “counter” evolving threats to reduce the cost and operational impact of maintains fielded systems security, of converting fielded non-secure systems to secure systems, and fielding secure systems.
- To continually reduce the acquisition cycle time to field secure systems and systems enhancements.
- IA information is disseminated through INFOSEC web site at SSA Charleston.



Organization: Fleet Information Warfare Center (FIWC)

Senior Information Operations Official:

CAPT M.V. Sherrard, Commanding Officer, 757-417-4006

Information Operations Points of Contact:

Dan Walters, Technical Director, 757-417-4002

LCDR Chuck Kasinger, Operations Officer, 757-417-4030

Jim Granger, Assistant Operations Officer, 757-417-4032

Senior Information Assurance Official:

CDR Dennis Popiela, Director of Systems, 757-417-4073

Information Assurance Points of Contact:

Bill Jones, Deputy Director of Systems, 757-417-4073

Senior Critical Infrastructure Protection Official:

LCDR John Pagona, Systems Department Head, 757-417-4101

Critical Infrastructure Protection Points of Contact:

ETCS Paul Titus, N62 Division Officer, 757-417-4103

ETC John Kovac, 757-417-5000

On-Line Resources:

FIWC NAVCIRT Homepage:<http://www.fiwc.navy.mil> (NIPRNET)

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 attack 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. On-line surveys are conducted on unclassified and classified networks.
- Network Intrusion Device Monitoring. Navy has initiated the use of NetRanger sensors on classified and unclassified networks at the Network Operating Centers (NOC). The NetRanger 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. NetRanger, centrally monitored at FIWC, recognizes attempts by unauthorized personnel to gain access to Navy networks, notifies appropriate personnel of the intrusion attempt, and automatically records the intrusion.

Activities:

- 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.

**Naval Information Warfare Activity
(NIWA)**

Organization: Naval Information Warfare Activity (NIWA)

Senior Information Operations Official:

CAPT Daly, Commanding Officer, 301-669-2103, daly@niwa.navy.mil

J.T. Dale III, 301-669-2100

LT Neils Mateo, 301-669-2184

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.

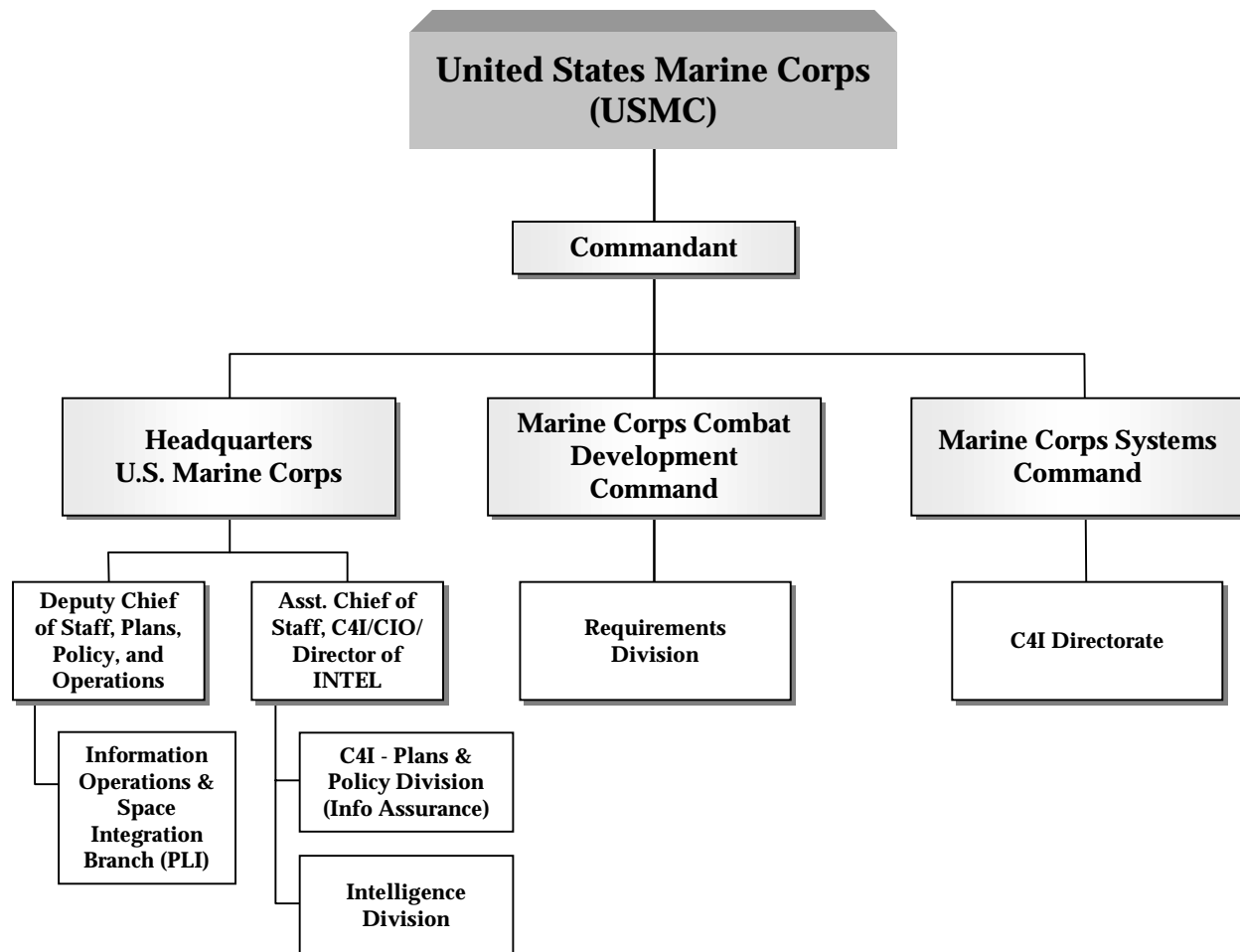
The NIWA also serves as the Navy's technical agent for appropriate simulation and modeling activities supporting IW.

NIWA mission is to:

- Acts 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/databases 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-sponsored 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.

Activities:

- For information on activities contact the Point of Contact.



Organization: United States Marine Corps (USMC)

Senior Information Operations Official:

LtCol J. J. Cuff, DSN: 614-3707

Information Operations Points of Contact:

Major V. Kucala, DSN: 614-4221

Senior Information Assurance Official:

Ms. G. McKinnon, DSN: 664-7036

Information Assurance Points of Contact:

Mr. T. Steinhauser, DSN: 664-7014

MSgt J. Driscoll, DSN: 664-7037

Ms. E. Morgan, DSN: 664-7038

Senior Critical Infrastructure Protection Official:

Ms. G. McKinnon, DSN: 664-7036

Critical Infrastructure Protection Points of Contact:

Mr. T. Steinhauser, DSN: 664-7014

MSgt J. Driscoll, DSN: 664-7037

Ms. E. Morgan, DSN: 664-7038

On-Line Resources:

USMC Homepage: <http://www.usmc.mil>

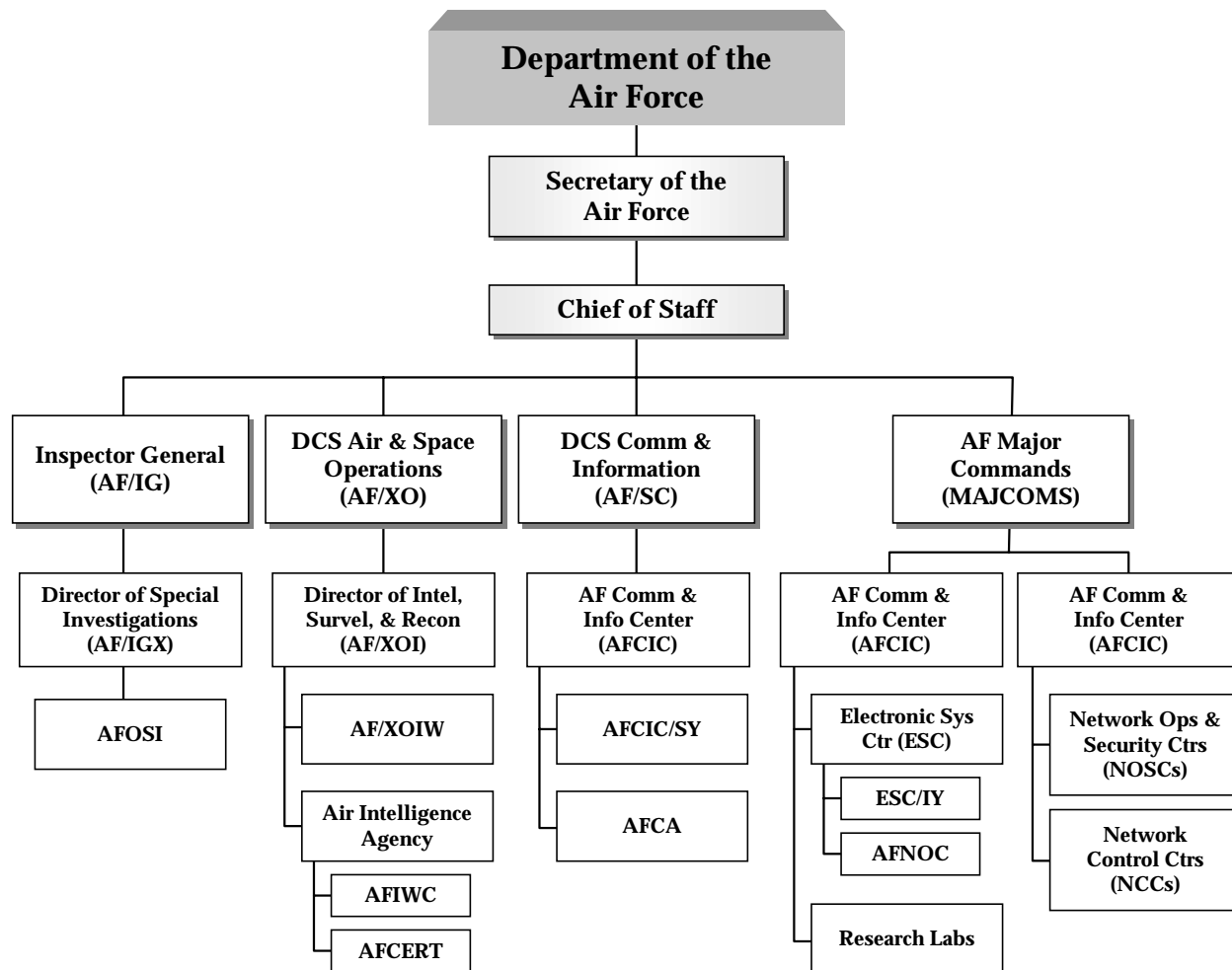
Missions and Functions:

Headquarters, Marine Corps (HQMC) is responsible for IO policy. The Information Operations and Space Integration Branch within the Strategy and Plans Division which is part of Plans, Policy and Operations Department, HQMC is responsible for IO, IW, and C2W policy. The C4I Department, HQMC is charged with Defensive IO and Information Assurance policy. HQMC/C4I is also the Marine Corps' component Headquarters for the Joint Task Force for Computer Network Defense. Combat Development Command is responsible for requirements and Systems Command is responsible for development and acquisition.

Activities:

- HQMC is currently in the process of updating and repromulgating Marine Corps Orders both Information Operations, Command and Control Warfare, and Information Assurance.
- 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 service participation and receive a share of the services provided by these organizations.
- Panels and Working Groups: HQMC has established an IO working group to coordinate IO activities between all HQMC departments, the Marine Corps Combat Development Command (MCCDC), and the operating forces.
- Protect: The Marine Corps is an active component of the Joint Task Force for Computer Network Defense. The Marine Corps Enterprise Network is a closely coordinated regionalized system, administered by the Network Operations Center, Quantico, it maintains a high degree of network security through stringent policies and state of the art intrusion prevention equipment. Intrusion detection devices are currently being implemented.
- Detect and React: The Marine Corps Network Operation Center works closely with the FIWC; the Navy's Computer Incident Response Team, to receive computer emergency response support.

This page intentionally left blank.



Organization: Department of the Air Force

Senior Information Operations Official:

Lt Gen Marvin Esmond, Deputy Chief of Staff/Air and Space Operations (HQ USAF/XO),
703-697-9991

Information Operations Points of Contact:

Brig General Glen Shaffer, Director of Intelligence, Surveillance and Reconnaissance
(HQ USAF/XOI), 703-695-5613

Col Sammy Pierce, Deputy for Information Warfare (HQ USAF/XOIW), 703-697-2795

Lt Col John Levy, Chief Defensive Information Warfare Division (AF/XOIWD),
703-697-8701

Senior Information Assurance Official:

Lt Gen William Donahue, Director, Communications and Information (HQ USAF/SC) and
Commander, Air Force Communications and Information Center (AFCIC/CC),
703-695-6324

Information Assurance Points of Contact:

Col Bernie Skoch, Director of Systems (AFCIC/SY), 703-588-6176

Col Roger Robichaux, Chief, Networks Division (AFCIC/SYN), 703-697-8590

Lt Col David Warner, Chief, Information Assurance Branch (AFCIC/SYNI), 703-588-6173

Senior Critical Infrastructure Protection Official:

Lt Gen Gregory S. Martin, Air Force Chief Information Officer (AF-CIO), 703-697-6363

Critical Infrastructure Protection Points of Contact:

Lt Gen John Handy, Deputy Chief of Staff Installations and Logistics (HQ USAF/IL),
703-697-2405, AF Representative to the Critical Asset Assurance Program (CAAP)

Capt Douglas Hardman, Readiness Programs Branch (AF/ILEOR), 703-604-3745, AO Level

Lt Gen William Donahue, Deputy, Air Force Chief Information Officer (Dep AF-CIO),
703-695-6324, AF Representative on the Defense-wide Information Assurance Program
(DIAP) Senior Steering Group

Capt Helen Lento, Information Assurance Branch (AFCIC/SYNI), 703-588-6171, AO Level

On-Line Resources:

USAF Homepage: <http://www.af.mil>

Missions and Functions:

HQ USAF/XOI. The Directorate of Intelligence, Surveillance and Reconnaissance (AF/XOI) is the Air Force lead for Information Superiority – the ability to gain, exploit, defend and attack information. AF/XOI formulates and integrates intelligence, surveillance, reconnaissance (ISR), information warfare (IW) and security policies and plans; programs, defends and employs ISR and IW resources and capabilities; and interfaces with congressional, OSD, Joint and MAJCOM staffs to ensure warfighting requirements are met.

HQ USAF/XOIW. The Deputy Directorate for Information Warfare (AF/XOIW) is the Air Force functional manager for offensive and defensive Information Warfare. XOIW formulates and oversees AF IW policy, doctrine, investment, strategy and force structure, managing approximately \$5B of AF TOA aligned with IW, and ensuring the availability of AF IW assets for use by the warfighting CINCs.

AFIWC. The Air Force Information Warfare Center (AFIWC) is the Air Force Center of Excellence for Information Warfare. With a staff of approximately 1000 information operations professionals, its mission is to explore, apply, and migrate offensive and defensive Information Warfare (IW) capabilities for Air Force and Joint operations, acquisition and testing. AFIWC is the provider of advanced IW training for the Air Force. The Commander, AFIWC, is also the Commander of Air Force Forces (COMAFFOR) supporting the Joint Task Force - Computer Network Defense (JTF-CND).

AFCERT. The Air Force Computer Emergency Response Team (AFCERT) is the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities. The mission of the AFCERT is to process and respond to all Air Force users' incident reports from intruder and malicious logic incidents. AFCERT processes and coordinates countermeasure development and disseminates countermeasures for all reported Information Protection (IP) vulnerabilities, establishes and maintains Information Protection (IP) databases, assists unit commanders with computer attack damage control and recovery procedures, and distributes AFCERT Advisories, AFCERT Advisory Compliance Messages, AFCERT IP Bulletins and DISA ASSIST Bulletins. AFCERT is the assigned Air Force Forces (AFFOR) supporting the Joint Task Force – Computer Network Defense (JTF-CND).

AFNOC. The Air Force Network Operations Center (AFNOC) mission is to monitor and maintain data networks for the Total Force, in-garrison and deployed. Its major activities include wide area network (WAN) operations and maintenance, network troubleshooting and proactive assessments, information protection, and other systems and contingency support

AFOSI. The Air Force Office of Special Investigations (AFOSI) provides professional special investigative services for the protection of Air Force and DOD people, operations, and materiel worldwide. AFOSI priorities include exploiting counterintelligence activities for force protection, resolving violent crime impacting the Air Force, combating threats to

Air Force information systems and technologies, and defeating and deterring acquisition fraud. This includes investigating the crimes of espionage, sabotage, subversion, terrorism, technology transfer, computer infiltration and other specialized counterintelligence operations.

HQ USAF/SC. The Air Force Directorate of Communications and Information provides innovative communications and information services and solutions – efficient in peace...effective in war. This is accomplished by exercising Air Force Communications and Information core competencies – Combat Ready Communications and Information Forces, Connectivity – Global Grid, Network Operations, Information Assurance, and Information Resource Management. It ensures information and information networks are managed as strategic resources; considering policy, life cycle management, and improvement of Air Force core business processes. AF/SC provides Information Assurance support for the Air Force enterprise through policies, tools, and processes.

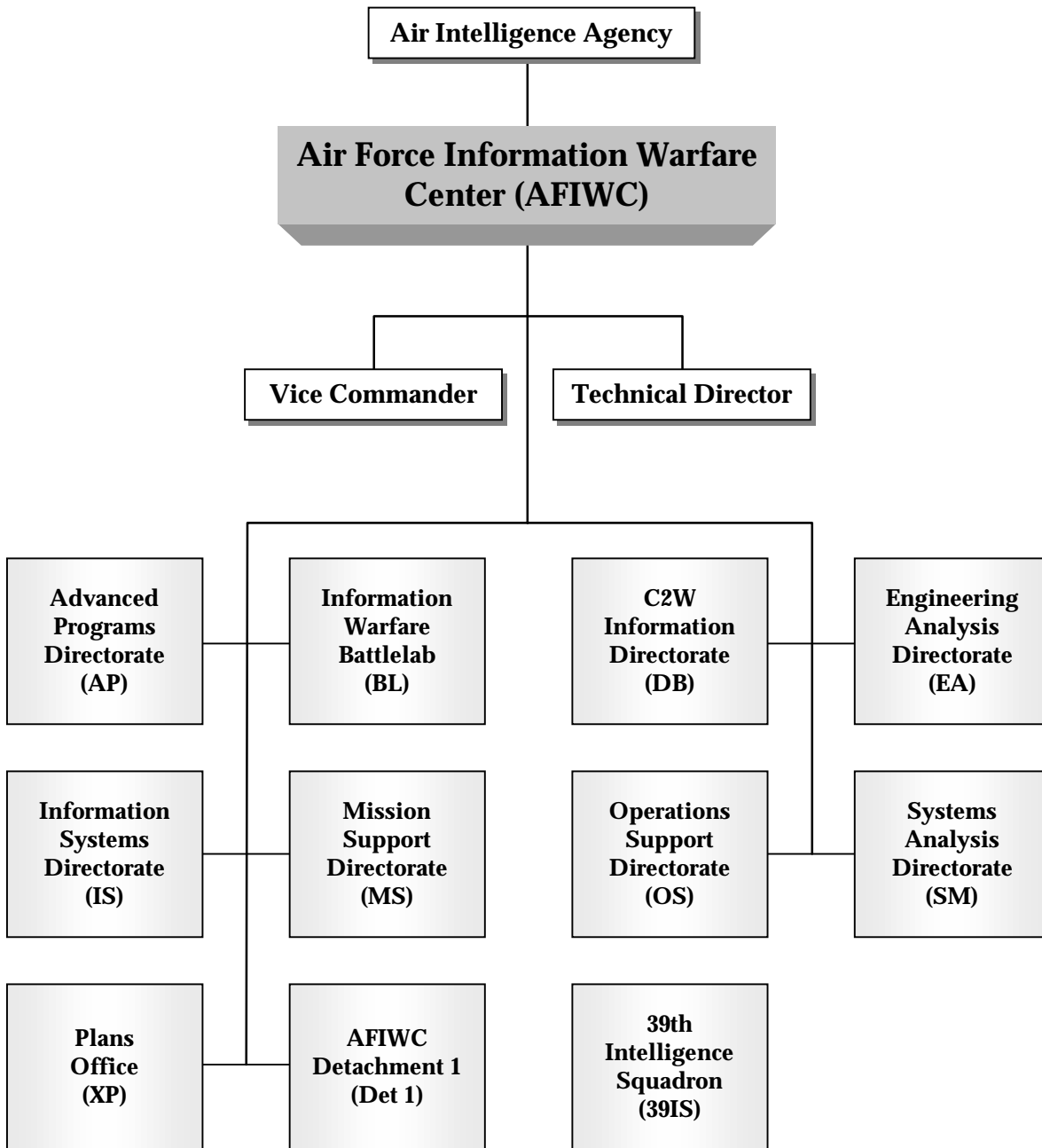
Due in part to the integrated, cross-cutting approach to IW within the Air Force, many line and staff organizations at various levels are actively involved integrating IW into Air Force doctrine, policy, plans, programs, and procedures. At the Air Staff, the Communications and Information, operations, intelligence, acquisition, and security police communities participate in the Information Protection Working Group and other forums. Line organizations, such as the Air Force Communications 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 assurance (IA) responsibilities and Wing Information Assurance Offices have been established in the local Communications Squadrons.

Activities:

- Published Air Force Policy Doctrine 10-20, 1 August 1998, Air Force Defensive Counterinformation Operations.
- Published Air Force Doctrine Document 2-5, Information Operations 5 August 1998.
- Information Warfare Battle lab established to identify and rapidly measure the worth of innovative concepts which advance the Air Force's core competencies. IW battle lab is under the Air Intelligence Agency, at Kelly AFB, Texas, Col James Watkins, DSN-969-3030.
- Establishing Network Operation Security Centers (NOSC) at the AF Major Commands. These groups have the ability to work for deployed forces. This group augments the embedded information security personnel of each organization.
- OSI personnel embedded at each organization to be able to perform information security functions and provide staff recommendations to the commander in matters concerning information security, such as intrusion and investigation alternatives.
- Started a program to install layered information security at all levels of the Air Force. Began with the installation of the Combat Information Transport System (CITS) and Base Information Protection (BIP) Equipment which was standard. The next phase will install a network management system.

- Developed Theater Deployable Communications (TDC) for units to have complimentary equipment forward to be able to communicate to the infrastructures at bases.
- Installed Automated Security Incident Measurement (ASIM) system at every Air Force installation.
- Counter Intelligence and Law Enforcement in Information Assurance and Information Operations embedded in the community. The law enforcement takes control of the initial intrusion investigation to be able to go to Commercial ISP. If at some point the intruder is identified as a “bad actor” then the counter intelligence element takes over.
- Air Force information “forensic lab” rolled into DOD lab as directed by ASD(C3I).
- Established Network Control Centers in communications units at all Air Force Bases
- Established Network Operations and Security Centers at seven Major Commands.
- Established Operationalizing and Professionalizing the Network (O/PTN) program; includes training and certification initiatives for all information systems users as well as skill level training and certification of network professionals.
- Published AFI 33-115, Volume 1, Network Management, providing the overarching direction and structure for Air Force efforts to operationalize and professionalize the network (O/PTN).
- Published AFI 33-202, Computer Security, providing directive requirements for the COMPUSEC component of the information assurance (IA) discipline as outlined in AFPD 33-2 and implementing the Air Force COM-PUSEC Program.
- Instituted a positive control process for computer vulnerability advisories which includes unit level acknowledgement of receiving the information, a schedule for implementing countermeasures, and a feedback mechanism to keep management tiers informed.
- Fielded Network Management System (NMS) capabilities and a Base Information Protection (BIP) tool suite at 105 Air Force installations.

This page intentionally left blank.



Organization: Air Force Information Warfare Center (AFIWC)

Senior Information Operations Official:

Col James C. Massaro, 210-977-2091

Information Operations Points of Contact:

Col Thomas C. Moe, Director, Operations Support Directorate, 202-977-2314

Senior Information Assurance Official:

Feliciano Rodriguez, Director, Engineering Analysis Directorate, 210-977-3141

Col Charles R. Hall, Director, Information Systems Directorate, 210-977-3420

Information Assurance Points of Contact:

Lt Col Kenneth W. Singleton, Chief, AFCERT, 210-977-3158

Ms. Hope C. McMahon, Chief, Infrastructure Management Division, 210-977-2411

On-Line Resources:

AFIWC Homepage: <http://www.afiwcaia.af.mil>

Missions and Functions:

AFIWC explores, applies, and migrates offensive and defensive information warfare (IW) capabilities for operations, acquisition, and testing. AFIWL provides advanced IW training for the Air Force.

The Advanced Programs Director (AP) leads the Center in the innovation, development, and employment of advanced C2W capabilities (Counter C2 and C2 Protect) using a multi-disciplined approach. The AP Directorate:

- Explores and advanced technologies, techniques, talents and tactics for C2W applications
- Provides the Center and its customers with multi-disciplined (scientific, technical, intelligence, and operations) developed solutions and products needed to support emerging warfare techniques
- Manages specialized C2W intelligence and counter-intelligence support.

The AP Directorate had four divisions: the Intelligence Warfare Battlelab is to advance the Air Force's core competencies by rapidly identifying innovative and superior ways to:

- Plan and employ IW capabilities,
- Organize, train, and equip IW forces, and
- Influence development of IW doctrine and tactics

in order to meet current and emerging Air Force missions for the advancement of air and space power.

The C2W Information Directorate (DB) develops and maintains Command and Control Warfare (C2W) databases and database applications for the AFIWC. The directorate is the focal point for database issues to include production, implementation, quality assurance, deployment, technical support, and training.

Using multi-disciplines US and rest-of-the-world data, DB develops, builds, extracts, and integrates C2W data into several different DOD-recognized data structures and/or architectures. Our C2W databases form the foundation upon which AFIWC builds its information mission. DB plays a critical role in AFIWC's execution of information operations – the acquisition, storage, transmission, and transformation of information.

The DB Directorate has five divisions: the C2 Networks Division (DBA); the Concepts and Requirements Division (DBC); the Engineering Information Division (DBE); the Integration and Standards Division (DBI); and the C2W Integrated Analysis Division (DBW).

The Engineering Analysis Directorate (EA) supports two significant Air Force initiatives-information and weapons systems development by providing technical guidance in the areas of computer security, communications security and emission security.

Specialized tools and capabilities of EA include:

- On-Line Survey (OLS), conducted within both EAA & EAS, is a project to measure the security posture of Air Force C4 systems, whereby survey operators attempt to penetrate targeted systems, and analyze data generated and create a report describing the security weaknesses found and the associated countermeasure
- The Computer Security Engineering Team (CSET), part of EAS, conducts assessments of off-the-shelf and government-developed computer security products for the Air Force as well as performing product security profiling, C4 security field assessments, ST&E of C4 systems and reviews of C&A plans for technical content.
- The Countermeasure Engineering Team (CMET), part of EAC, develops countermeasures to correct vulnerabilities in stand-alone and networked computer systems.

The EA Directorate has three divisions: the Assessments and Emergency Response Division (EAA); the Countermeasures Division (EAC); and the Engineering and Assessments Division (EAS).

The Information Systems Directorate (IS) provides a central focal point for IW technology and facilitates the application of new technology to support the USAF and AFIWC IW/C2W missions.

The IS Directorate:

- Maintains cognizance of all technology development and application efforts in the center
- Sponsors the IW technology review panel
- Facilitates cross-fertilization of technology across directorates to solve IW mission shortfalls
- Serves as Center focal point for space related applications and activities
- Investigates promising commercial and government technology efforts for application to the IW/C2W missions
- Support funded and unfunded Cooperative Research and Development Agreements (CRDAs) with industry to encourage refinement and development of promising technologies
- Host/sponsor advanced technology efforts for proof-of-concept demonstrations into Center.

The IS Directorate has three divisions: the Information Systems Applications Division (ISA), the Information Systems Concepts Division (ISC), and the Infrastructure Management Division (ISM).

The Mission Support Directorate (MS) oversees library, logistics security, facilities, and other staff services.

The MS Directorate has three divisions: the Logistics Division (MSL), the Mission Support Programs Division (MSP), and the Library Services Division (MSY).

The Operations Support Directorate (OS) trains, equips, and deploys personnel to provide intelligence and C2W services to the warfighter during contingencies, special operations, and exercises. It provides awareness and information on:

- Operations Security (OPSEC) and Education
- Command & Control Warfare (C2W)
- Imagery, C3/ELINT
- Electronic Combat (EC)
- Computer and Electronic Threat Assessments and Reports
- Signals Identification
- SERENE BYTE Exercise Planning
- Operationally Relevant Data
- Tactical Deception
- SIGINT Threat Analysis and Reporting
- Electronic Warfare Integrated Reprogramming (EWIR).

The OS Directorate has five divisions: the Intelligence Application and Production Division (OSA), the Information Warfare Support Division (OSD), the C2W Operations Division (OSJ), the Current Operations Division (OSO), and the Reprogramming Division (OSR).

The Systems Analysis Directorate (SM) is composed of more than 100 scientists and engineers whose mission is to provide quantitative analysis through modeling and simulation of offensive and defensive USAF Command and Control Warfare/Information Warfare (C2W/IW) systems capabilities and vulnerabilities. These analyses are used to support operations, test and evaluation, and acquisition. Under the new IW mission, SM will continue to produce offensive C2W/IW systems analyses (which includes electronic combat (EC)), and will also broaden its analysis capabilities of defensive C2W/IW systems.

SM provides:

- Analysis of C2W capabilities and vulnerabilities of friendly and hostile information, sensor, and weapons systems
- Evaluation of new and emerging technologies for potential application in supporting C2W electronic attack and protect
- Development and operation of engineering, platform, mission, and campaign (Level 1 to 4) C2W models for analysis of information, sensor, and weapon systems
- C2W modeling, simulations and analysis support of USAF wargames and exercises
- Support of acquisition requirements such as a Cost and Operational Effectiveness
- Analyses (COEAs), ORDs, MNS, and PMDs by providing C2W analysis of information, sensor, and weapon systems.

The SM Directorate has five divisions: the C2W Analysis Division (SMA), the Capability Analysis Division (SMC), the Advanced Combat Simulations Division (SMM), the Analysis Support Division (SMS), and the Vulnerability Analysis Division (SMV).

The AFIWC Plans Office (XP) develops, maintains, manages and provides oversight for the center's plans, programs, budget, manpower and quality.

By the Commander's direction, the Plans Office:

- Manages and maintains the center's mission, goals, and objectives
- Manages and maintains the center's plans
- Manages and maintains the center's requirements and initiatives
- Performs overall management and oversight of center programs
- Manages and maintains all actions dealing with center manpower and quality
- Reviews, coordinates and prepares responses for external directives and documents pertaining to the center's mission
- Reviews written agreements with other organizations
- Manages all center financial matters.

AFIWC Detachment 1 (Det 1) integrates Air Force IW concepts and technologies in response to the needs of the Air Force and the Information Operations Technology Center (IOTC).

Det 1 will:

- In conjunction with AFIWC, develop information operations (IO) tools and techniques and maintain them in a toolbox from which the Air Force may draw
- Facilitate development of IO technologies and techniques in accordance with appropriate Air Force element
- Organize and manage Air Force members working within the IOTC.

The 39th Intelligence Squadron (39IS) applies and migrates information operations (IO) knowledge and skills through specialized IO and initial qualification training (IQT) for Air Force information operators. The squadron provides IO training, exercise and testing support to the 53rd Wing (WG), Eglin AFB, and Command and Control Training and Innovation Center, Hurlburt Field, FL.

39IS training will focus on the following two areas:

- Actions necessary for defending and attacking information and information systems (Information Warfare/IW), including offensive counter information (OCI) and defensive counter information (DCI) disciplines
- Proficiency in the information functions and applications (Information-in-War/IIW) necessary for successful aerospace and information operations.

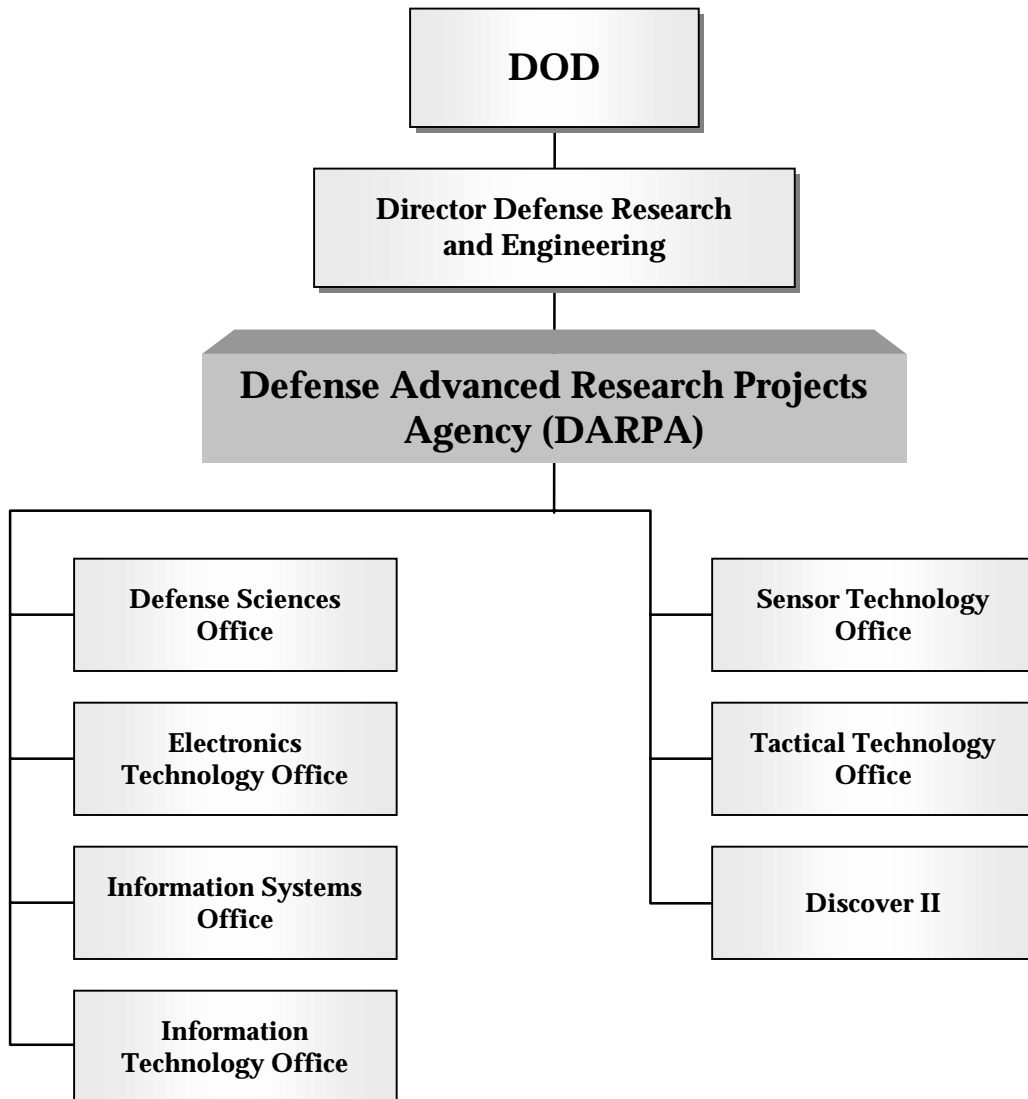
Activities:

- 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. 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 Automatic Security Incident Measuring System (ASIMS) 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. ASIMS analysts then measure the level of 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 ASIMS site as appropriate. The AFOSI may request technical assistance from the AFCERT to support their investigation. As of December 1998,

ASIMS is operational at 115 sites. Installation continues to cover all networked computer systems Air Force wide.

- 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. CDS is available on-line for 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 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.



Organization: Defense Advanced Research Projects Agency (DARPA)

Senior Information Operations Official:

Dr. F.L. Fernandez, DARPA Director

Information Assurance Points of Contact:

Mr. O'Sami Saydjari, Information Assurance Program Manager, 703-696-2231,
ssaydjari@darpa.mil

Dr. Gary Koob, Information Survivability Program Manager, 703-696-7463,
gkobb@darpa.mil

Critical Infrastructure Protection Points of Contact:

Mr. O. Sami Saydjari, Information Assurance Program Manager, 703-696-2231,
ssaydjari@darpa.mil

On-Line Resources:

DARPA Homepage: <http://www.darpa/mil>

Missions and Functions:

DARPA's primary responsibility is to help maintain the U. S. technological superiority and guard against unforeseen technological advances by potential adversaries.

Consequently, the DARPA mission is to develop imaginative, innovative, and often high risk research ideas offering a significant technological impact that will go well beyond the normal evolutionary developmental approaches; and, to pursue these ideas from the demonstration of technical feasibility through the development of prototype systems. and approaches.

Activities:

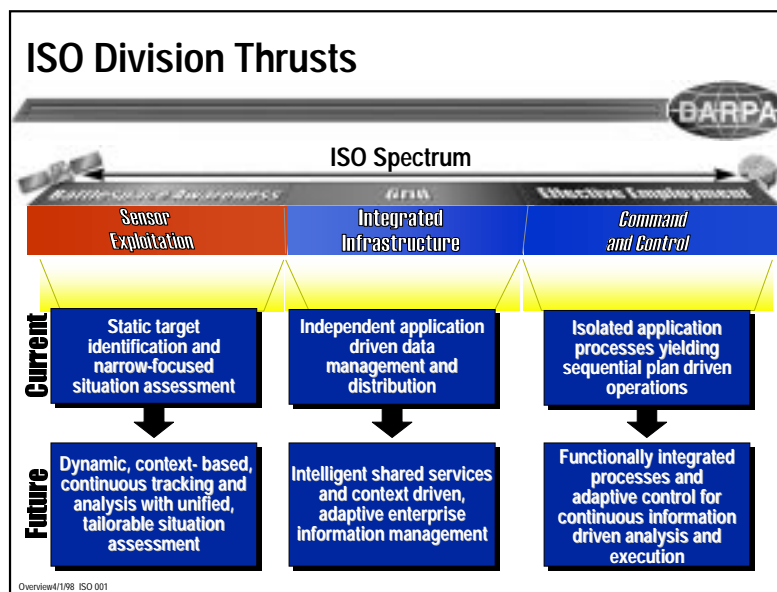
DARPA is an organization of about 210 personnel (approximately 130 of which are technical) directly managing a budget of about \$2 billion.

The DARPA Information Technology Office (ITO) advances the frontier of computing systems, information technology, and software to insure that DOD has the technologies needed for the future. The ITO is responsible for research into breakthrough information technologies for use in advanced defense applications. The office's mission is to provide the networking and computing hardware, software, systems and management technologies vital to ensuring DOD military superiority. The ITO is addressing information technology issues of strategic concern such as:

- Computing systems architectures
- Software technology
- Common interoperable services
- Scalable networking technologies
- System architecture
- Mobile computing and networking
- System management and distributed information technologies
- Security and survivability technologies
- Large-scale system design and integration technologies.

The Information Survivability Program creates technologies for use in building hardened information systems and networks that have strong barriers to attack, can detect malicious and suspicious activity, can isolate and repel such activity where possible, and can guarantee minimum essential continued operation of critical system functions in the face of concerted information attacks. These technologies will enable the construction of secure enclaves, and will allow distributed computing to span such enclaves, as is required in ISO's systems. These technologies will combine the strength needed for DOD, while retaining the cost savings resulting from use of COTS. Programs are in place to study the following areas: Survivability of Large-Scale Systems, High Confidence Networking, Wrappers and Composition, and High Confidence Computing.

The DARPA Information Systems Office (ISO) provides technologies and systems to allow the commander dominant battlefield awareness and superb force management.



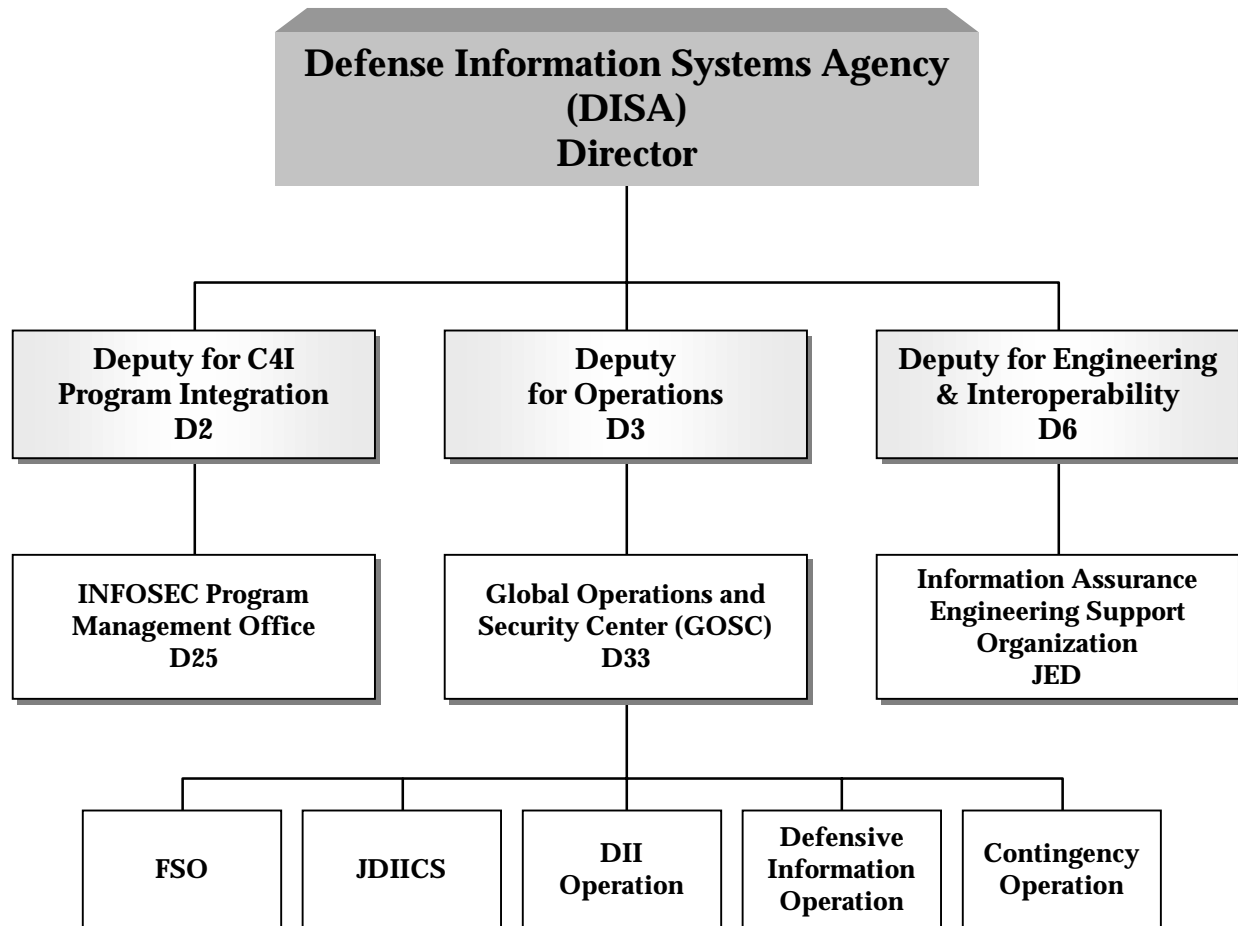
The DARPA Information Assurance Program will develop security and survivability solutions for the Next Generation Information Infrastructure (NGII) that will reduce vulnerability and allow increased interoperability and functionality.

Under DARPA sponsorship, technologies are now being developed in areas of Prevention, Detection and Response, and Security Management. Ultimately, these technologies will be integrated into a security architecture that, while integrating security and survivability concepts, techniques, and mechanisms, will also provide interfaces for future security upgrades.

The Information Assurance goals are to develop security and survivability solutions for the Next Generation Information Infrastructure (NGII) that will reduce vulnerability and allow increased interoperability and functionality. These include:

- Architecture and Integration - The IA Program will develop a security architecture for integration into the NGII Reference architecture, incorporating security and survivability concepts, techniques, and mechanisms. This security architecture will provide interfaces for future security upgrades, and create a security foundation for the Defense Information Infrastructure (DII).
- Prevent Attack Opportunity - Control Access Data that is integral to current and planned ISO-developed systems and that is openly stored and transmitted on public networks is available to any adversary and can allow inference of more highly sensitive information. Solutions to be integrated include encryption of message traffic, firewalls, and program and data authentication (e.g., within end systems and network routers). Other solutions include policy-controlled guards and release stations that remove the need for a man in the loop, strong user authentication, and protected execution domains to limit damage.
- Detect and Respond to Unprevented Attack - Because vulnerability cannot be eliminated, attack detection methods will be integrated. Through experimentation in real systems, we will reduce false alarm rates and enhance real-time detection capability. We will make these detectors self-protecting. Because damage can be done quickly (including the insertion of Trojan horses for use in future attacks), automated response is needed. We will build in automated and context-sensitive response capability, such as adding filters to firewalls and routers, selectively shutting down resources, rerouting traffic, and running only authenticated software. Emergency bypasses will be included and protected from abuse.
- Manage System Security - A security management infrastructure will be developed to support policy specification and security services such as global identification of users, and exchange and certification of cryptographic keys. The components of this infrastructure and the traffic among them will be protected.

DARPA recently conducted an initiative called Information Superiority Technology Integration (ISTI) 98. This initiative by the Information Assurance Program involved subjecting various technologies to a Red Team Attack. The purpose of the initiative was to gauge the effectiveness of IA strategies, architectures and technologies, and to gain an understanding of adversary methods and strategies to guide future IA research.



Organization: Defense Information Systems Agency (DISA)

Information Assurance Points of Contact:

Mr. J.P. Angelone, INFOSEC Program Manager, D25, 703-681-7936, angelonj@ncr.disa.mil
LTC Princess Boulware, USA, INFOSEC Deputy Program Manager, D25, 703-681-7932,
boulwarp@ncr.disa.mil

COL John Thomas, USA, Commander, GOSC, D33, 703-607-6680, thomasj@ncr.disa.mil
LTC Timothy Fong, USA, Director, Information Assurance Engineering Support
Organization, JED, 703-681-2211, fongt@ncr.disa.mil

Mr. John Hunter, Deputy Director, Information Assurance Engineering Support
Organization, 703-681-2219, hunterj@ncr.disa.mil

On-Line Resources:

<http://www.disa.mil>

Missions and Functions:

INFOSEC Program Management Office (IPMO) (D25)

The IPMO has the mission to manage the acquisition, implementation, and integration of INFOSEC products and services into the DISA pillar programs and other DOD systems and activities. Specific functions and objectives include:

- Provide INFOSEC Technical Support/Products to DISA pillar programs and CINCs, Services and Agencies
- Provide INFOSEC Plans, Policy and Project Management in support of DISA pillar programs
- Provide INFOSEC Education, Training and Awareness Products to CINCs, Services and Agencies.

The IPMO supports the Director, DISA, in his role as the Manager of the Defense Information Infrastructure, to ensure the DII is adequately protected. The approach to doing so is embodied in the following objectives:

- Operate and Maintain a Secure DII
- Secure the Applications
- Secure the Hosts and Enclaves
- Protect the Networks.

Specific activities to accomplish these objectives are outlined below.

Global Operations and Security Center (GOSC) (D25)

The GOSC mission is to integrate and provide support for current military operations, - contingency operations, network operations, and Information Warfare (IW) events to develop a global DII SA for the warfighter.

The key GOSC functions derived from this mission statement include the following:

- Has oversight responsibility for the entire DII
- Monitors status of DII applications, networks, systems, DIO concerns
- Provides management control, technical direction of DII
- Provides DII policy, standards, guidance for systems and network management
- Interfaces with organizational and individual users of the DII.

In support of this mission, the subordinate elements of the GOSC perform the following key functions:

- Field Security Operations (FSO)
 - Conduct Security Readiness Reviews (SRR)
 - Conduct Scheduled Vulnerability and Assistance Program (VAP)
 - Certification of Assigned Systems
 - Develop Operational and Technical Guidance
 - Deploy Security Management Tools
- Joint DII Control Systems (JDIICS)
 - Plan and Manage GOSC Support Environment
 - Implement a Global View of Critical C/S/A Systems and Networks
- DII Operations
 - Detect, Assess, and Restore (Network and System Anomalies)
 - Authorized Outage Control
 - Manage Non-Defense Information Systems Network (DISN) High Interest Networks
 - Manage Defense Satellite Communications System (DSCS)
 - Status Reporting.
- Defensive Information Operations
 - Detect and Assess Information Assurance (IA) Anomalies And Restore DII Services
 - IA Vulnerability Alerting
 - DIO Reporting
 - Virus Detection and Eradication
 - Conduct Unscheduled VAAP Surveys
 - Defense Intrusion Analysis & Monitoring Desk (DIAMOND) Analysis of Security Anomalies
 - DIAMOND Sensor Management and Control
 - DIAMOND Determine Operational Impact of DII (Network, System and Security) Anomalies.

- Contingency Operations
 - C/S/A Exercise, Crisis, and Contingency Support
 - Super High Frequency/High Frequency (SHF/HF) Gateway Management.

Information Assurance Engineering Support Organization (IAESO)

The mission of the IAESO is to organize, train, and equip the organization in order to provide technically qualified engineers, administrative, contracting, acquisition, budget, and logistical support personnel to the Information Assurance Chief Executive Engineer (IA CEE) and Chief Engineer (CE). The IAESO serves as DISA's IA focal point for the provision of engineering services in support of IA requirements. These engineering services are provided for legacy information systems and new C4I programs supporting the Warrior and the DISA core programs (DII COE, DISN, GCCS, GCSS, DMS).

The IAESO fulfills its mission responsibilities through the provision of information system security engineering support in the form of system designs, technical advice, assistance, information, and guidance to DOD during the entire information systems life cycle.

Specifically, engineering support is provided for the:

- Development and implementation of an IA architecture in accordance with the Defense-In-Depth strategy
- Provision of IA engineering services to DISA pillar programs, and CINCs/Agencies/Services
- Development of DOD PKI engineered solutions and support the development of PKI enabled applications
- Provision of multiple security level interoperability capabilities
- Development and evolution of an IA Lab used to identify, develop, evaluate, and implement IA technologies and products
- Provision of an information assurance situation awareness view to the common operational picture (COP) by instrumenting the DII with protect, detect, react/recovery, and reporting tools.

Activities:

The DISA IA strategy includes the following:

- *Technical Capabilities.* The DISA technical implementation approach to protecting the DII is to implement a defense in depth. This layered security is intended to make it very difficult to penetrate the DII and also deal effectively with penetrations that occur. Protection measures will be based on a balance between the cost of securing the information and the value of the information if it is stolen, modified, destroyed, or delayed. DISA must focus on providing cost effective fixes to critical vulnerabilities in the near term while implementing the objective defense in depth.

- *Operations.* Operational capabilities must support technical measures. Operational policy and procedures, including enhanced situational awareness and system and network management, are critical to an effective defense in depth.
- *Policy.* Common security standards, policies, and architectures provide the framework within which capabilities and resources can be leveraged.
- *Personnel.* People are the most crucial aspect of IA. Adequate protection can only be attained and maintained through the active involvement of trained and aware users, terminal area security officers, proactive security professionals, and knowledgeable system owners and operators. The challenge is to provide the right amount and type of training to all the people who use military information systems.

During Fiscal Years 1996, 1997 and 1998, the Director, DISA took several actions to address his responsibility to protect the DII. The Director established INFOSEC as a central program within DISA – one of five pillars that are the central focus of DISA day-to-day operations and long term planning.

Operate and Maintain a Secure DII

- *Defensive Information Operations (DIO).* DIO focuses on support to the operational community. During FY98 funding was maintained for the Software Engineering Institute (SEI) Carnegie-Mellon Computer Emergency Response Team/Coordination Center (CERT®/CC) which continues to provide valuable support to DOD and the larger Internet community. During Solar Sunrise, a series of intrusions in February 1998, a CERT®/CC representative worked on-site with DISA Automated System Security Incident Support Team (ASSIST) personnel. Reserve Component personnel have also been integrated into ASSIST operations and were particularly helpful during Solar Sunrise response activities. Scheduled and unscheduled Vulnerability Analysis and Assistance Program (VAAP) assessments continued throughout the year in support of DISA and other DOD customers. In order to shorten the gap of time between when a computer or network vulnerability is discovered and when a fix is put in place, DISA developed the IAVA and the Vulnerability Compliance and Tracking System (VCTS). Through IAVA, DISA is able to automatically disseminate vulnerability alerts to the DOD personnel who are responsible for *locking down* systems and networks. The VCTS provides a means to document that vulnerabilities are addressed on all computers in the shortest possible time. This greatly improves the old way of doing business, whereby hackers could exploit vulnerabilities for six months to two years before a fix was applied. While VCTS use currently is limited to DISA users, plans are to offer the system for use to the entire DOD community. Another significant accomplishment was the standing up of Regional Computer Emergency Response Teams (RCERTs) in the DISA Regional Operations and Security Centers (ROSCs). The RCERTs will provide direct support to DMCs, Defense Agencies and CINCs. The CERT in Columbus will support the DISA WESTHEM DMCs and the Defense Agencies.
- *Certification and Connection Approval.* In coordination with the C/S/As, DISA developed a standardized, success oriented Certification and Accreditation (C&A) Process for all

DOD systems. The Process was signed out as a DOD Instruction on 30 December 1997. DISA has supported the implementation of the new Defense Information Technical Security Certification and Accreditation Process (DITSCAP) by publishing various guides and handbooks, as well as establishing an on-line Information Assurance Support Environment (IASE). The IASE is a one-stop shop for the DOD IA and INFOSEC professionals to acquire information pertaining to the various security disciplines and for information sharing. In support of information sharing, the IASE houses and links to security policy and guidance including Executive Orders, National Security Directives, Office of Management and Budget Circulars, and Service directives/instructions. In addition, the IASE is linked to various DOD entities including the Department of Energy Computer Incident Advisory Capability, the Trusted Products Evaluations Program, Center for Information Technology, and the National Institute of Health (NIH) Security World Wide Web sites. In 1998, the IASE was expanded to include a classified web site on the Secret Internet Protocol Router Network (SIPRNET) in addition to the unclassified IASE web site on the Unclassified-but-Sensitive Internet Protocol Router Network (NIPRNET) that was established in 1997. The SIPRNET IASE web site is a mirror site of the unclassified site with the exception of the sensitivity of the data. Areas of interest were expanded on both of the IASE sites to include various security-related areas such as Public Key Infrastructure (PKI), Traditional Security (TRADESEC), IA Tools, the DOD Antivirus Software and the IAVA system. Existing security related areas consist of the DITSCAP, Education, Training and Awareness (ETA), Secret and Below Interoperability (SABI), Connection Approval Process (CAP), ITSC, and IA Policy and Guidance. Chat Rooms were also established for these security areas. The IASE has implemented an IASE Information Desk that processes IA and INFOSEC requests via web request tickets, e-mail, phone, or faxes for both the unclassified and classified IASE environments. In addition to the IASE web site accesses for 1998 which include over 439,906 accesses to the unclassified IASE web site, and over 93,787 accesses to the classified IASE web site, the Information Desk has responded to over 700 requests. The IASE implemented a Solutions Database. The DOD IA and INFOSEC professionals can benefit by obtaining solutions to requests previously submitted by other IA and INFOSEC professionals.

SIPRNET Connection Approval Program activities continue while work continues on coordinating a NIPRNET CAP.

- *DII IA Education, Training, and Awareness.* The IMPAIR IA/INFOSEC ETA initiatives address DOD-wide requirements including: computer based training (CBI) development, courseware development, the DOD Awareness Program, and training provided to DOD personnel in the DISA INFOSEC Training Facility (IF). The accompanying chart indicates the numbers of products developed and distributed, as well as the number of students attending courses in the IF. During FY98, the IMPAIR placed increased emphasis on training-the-trainer courses. The IMPAIR was a key driver in developing and coordinating the DOD Certification and Licensing Program for users and system administrators. DISA products and training courses fulfill some of the certification requirements.

An Air University research report [*Future War: How vulnerable is our Information Based Infrastructure? What are the Best High Payback, Moderate Cost Corrective Actions, LtCol R.*

Cabell, 1998] cites the ETA program as “one of DISA’s best success stories.” Customers incorporating IAPMO products into their security programs include: Treasury Department, Department of Energy, State Department, U.S. Special Operations Command, U.S. Military District of Washington, Naval War College, and U.S. Air Force 68th Intelligence Squadron.

- *DII Security Architecture, Standards and Engineering.* DISA continues to provide technical IA engineering support and services to the DISA Pillar Programs and customers. Significant progress was made in the engineering necessary in preparing to integrate PKI as a DII service. Though emphasis is on implementing a pilot program for Defense Travel Region (DTR) 6, Joint Interoperability Engineering Organization (JIEO) engineers are working to ensure that it can provide general-purpose services to a broad range of programs. During FY98, security engineering and architecture work continued on the DII Common Operating Environment (COE), which provides the software support infrastructure for GCCS and Global Combat Support System (GCSS), key tools for the warfighting CINCs. A major focus of the effort was on identifying and patching security vulnerabilities in the COE.
- *DOD IA Software Licenses.* In FY97, DISA awarded a new five-year DOD-wide enterprise licensing agreement for anti-virus (AV) software to two software vendors. Exact cost savings are difficult to estimate; however, the current cost-per-seat is approximately \$0.50. The software can be downloaded by authorized users from a protected DISA web site. Limited help desk support is also provided. DISA has been procuring enterprise AV software for DOD personnel since 1995. At the end of FY98, there were an estimated 1.5 million users. DISA also negotiated a DOD enterprise license for Netscape during FY98.
- *Joint Warrior Interoperability Demonstration (JWID) Technical Assistance and Operational Planning.* JWID is an annual Joint Staff (JS) sponsored demonstration of emerging Command, Control, Communications, Computers and Intelligence (C4I) technologies and joint interoperability solutions, impartially presented to the CINCs and Military Services in an operational environment. Warfighters are given the opportunity to experiment with new and evolving capabilities, assess their value and recommend them for implementation, where appropriate. The IAPMO is responsible for conducting vulnerability analysis of the information technology infrastructure, demonstrations, and preparing required security documentation, as well as serving as security consultant for all JWID participants. During JWID 98, the IAPMO supported a Coalition Vulnerability Assessment Team (CVAT) in the United Kingdom, as well as a United States vulnerability assessment team and risk analysis.

Protect the Networks

- *DISN INFOSEC.* DISN is DOD's consolidated worldwide enterprise-level telecommunications infrastructure that provides end-to-end information transfer for supporting military operations. Significant effort and resources have been dedicated to hardening the DISN infrastructure. Efforts include research, engineering equipment acquisition and installation needed to maintain the security of the DISN Internet Protocol Router (IPR) networks, the NIPRNET and the SIPRNET. The KIV-7(HS) operates at the T1 rate and below and costs approximately \$3,632. KIV-7 (HS) are used for most customer access lines and many backbone trunks. 1000 are being bought in FY98. The KG-95-2 is an encryption device, operating at the T3 rate and below, used in securing portions of the ATM backbone networks. In FY98, 20 units were purchased at \$15,831 each.
- *DIO Situational Awareness Instrumentation.* DISA is developing software and software environments to improve DII detection and response. This includes Malicious Code Detection and Eradication (MCDES) software, Vulnerability Assessment Software (VAS), including data mining and real-time DII mapping capabilities. MCDES is designed for real-time detection and eradication of malicious code (viruses, Trojan Horse software, logic bombs, sniffers, etc.). VAS will map networks, identify legitimate/illegitimate hardware, software, system connectivity, essential information on each node, anomalies, vulnerabilities, and countermeasures and provide continuous reporting. It will also analyze open-source information for indications of attacks on the DII, vulnerabilities of DII components, etc. The situational awareness tool, the Automated Infrastructure Management System (AIMS) will provide Information Operations tracking and display capabilities, risk management databases, and an instrumentation display facility. Initial versions of these tools have been made available to C/S/As. Emphasis has been placed upon use of commercial off-the-shelf (COTS) products and interoperability. The objective architecture is an integrated Defense IA Command and Control System (DIACCS) to provide global IA situational awareness for DISA and the warfighter.

Secure the Hosts and Enclaves

- *Defense Megacenter Security.* The enterprise information processing elements for the DII are the Defense Megacenters (DMC). The DMCs provide information processing services in support of the DOD warfighter and functional communities on a fee-for-service basis. The nucleus of DMC security is the Security Readiness Review (SRR) process. Validated by the GAO, the SRR process provides for periodic comprehensive assessments, documented deficiencies and monitored compliance. DISA conducts on-site and remote SRRs on DOD's computer systems, facilities and networks. This process identifies, documents and corrects security vulnerabilities in DISA's and their customers' operating facilities. A database is used to track all activity and generate management reports as required. The data is used to document site security posture for C&A purposes and is also referenced by the DOD Inspector General (IG) and GAO during information system audits. The management feedback available through this process has accelerated the closure of vulnerabilities by focusing attention on the

problems. The process also provides the accreditors with the continuous ability to monitor risk, therefore greatly easing the maintenance of system and facility accreditation. Future development includes the ability to receive data from multiple tool sets and offering the benefits of this process to a wider customer base.

DISA is standardizing the security management environment by focusing on intrusion prevention and intrusion detection. DISA has installed technical security enhancements at DMCs, including firewalls, network intrusion detectors (NID), secure web servers and robust identification and authentication (I&A) services. To jump-start this endeavor, DISA selected, deployed and provided training on automated COTS security management and intrusion detection tools. These tools utilize policies that are based on DISA's Security Technical Implementation Guides (STIGs). DMC staff members utilize these automated tools to perform their security functions in a more efficient and standard manner.

DISA also provides intensive technical security training to improve mission performance of DOD INFOSEC and IA professionals. During FY98, DISA conducted more than 28 formal classes that addressed six basic IA functional categories and another distinct group of courses that supported many IA application tool sets. However, the rapid turnover of trained security personnel, technology advancements, systems migrations, and organizational realignments make an aggressive training program vital to the continued security posture of the DII.

Processes and tools that have proven successful in the DMC environment are often tailored to meet requirements of other DISA elements and customers; e.g., ROSCs and CINCs. The assessment portion of the SRR process was used as a model for the CINC DIO Reviews. Security tools have been fielded and training provided at ROSC and CINC locations.

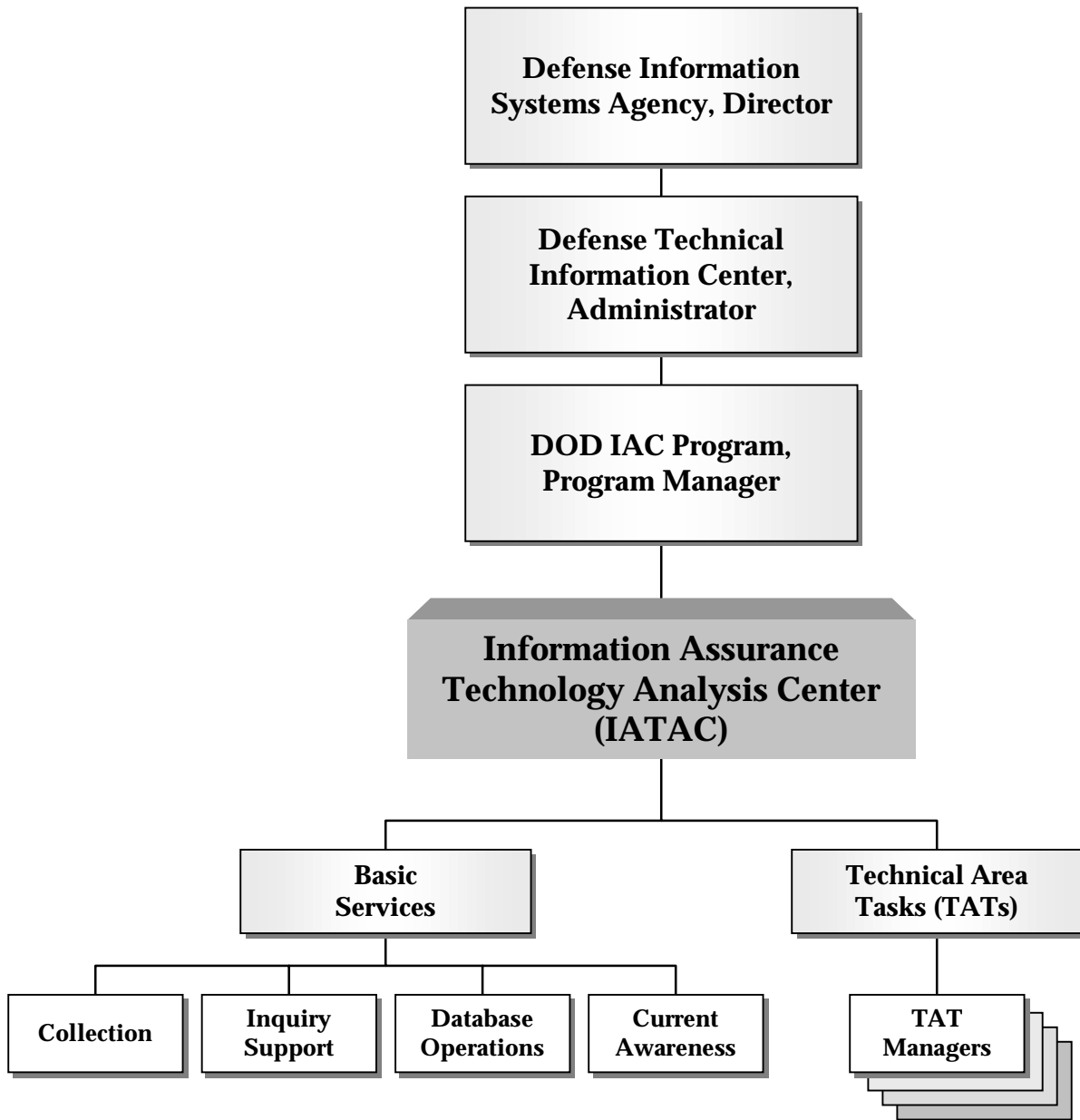
- *CINC DIO Reviews.* Annual CINC DIO Reviews are conducted to assist the Combatant Commands and the Components in evaluating their information assurance postures, identifying needed improvements, and recommending and assisting corrective actions. The reviews involve the CINC staffs and include both traditional security reviews, as well as technical reviews. A key purpose is to provide near term fixes/support. The traditional security reviews focus on the operational, organizational, and functional aspects of defensive information operations. Near term support includes installation of security management and intrusion detection tools, training on the tools and formal training for network and system administrators and others. The review team also assists the CINC staffs in developing DIO and IA strategies, CONOPS, policies and exercise programs.

Secure the Applications

- *Public Key Infrastructure.* The Deputy Secretary of Defense (DEPSECDEF) directed the establishment of a DOD PKI to provide a trustworthy foundation upon which to build cryptography-enabled services. This foundation is necessary for both the revolution in business affairs proposed by the Defense Reform Initiative (DRI) and the revolution in military affairs offered by Joint Vision 2010. The objective is to build an infrastructure

providing basic services that the C/S/A can build on to meet their unique requirements. Using an evolutionary approach based upon open system standards, DISA and NSA, in coordination with the C/S/As, are implementing a pilot medium assurance project for the DTR 6. Ultimately, DOD PKI will provide for multiple security levels (MSL). Much progress was made during FY98, including establishing a Help Desk at the DMC Chambersburg, developing Registration Authority (RA), Local Registration Authority (LRA) and end user guides, standard operating procedures, and training, and PKI program management and policy documents. The accompanying diagram depicts current accomplishments.

- *Defense Message System INFOSEC.* DMS is the messaging component of the DII providing multi-media messaging and directory services. It is flexible and COTS based. During FY98, the DMS PMO shipped a total of 134 Certificate Authority Workstations (CAWs) to designated Service and Agency locations. A total of 130 CAWs were installed to support DMS Sensitive-but-Unclassified (SBU) requirements; at 29 of these locations, an additional removable hard drive was installed to support DMS Secret requirements. DMS PMO has directed the contractor to upgrade the CAW platforms to 160 MG RAM to support the additional memory that will be required to support CAW Version 4.2.1 (scheduled for release in the 3QFY99). The DMS PMO plans to purchase an additional 50 CAWs in FY99 to support DMS top secret (TS) requirements. Additional requirements for FY99 include but are not limited to the following: CAW 4.2.X training for ISSO/SA/CA (two classes - 12 persons per class, total 24), CAW Installations, 500 4.2.X Registrar upgrades, Help Desk Support (GTE & Motorola), Memory upgrades 32 MG -> 160 MG. During FY98, the DMS PMO supported Security Test and Evaluation (ST&E) testing of the High Assurance Guard (HAG) Version 2.2. This was a joint test performed with NSA, D24, D25, and JITC. The DMS PMO requirements for FY99 include but are not limited to the following: purchase of six SCC HAGs to support Prototype testing the DMS LABs/LMFS and beta deployment and HAG 2.2 SW upgrade costs. The accompanying chart depicts current accomplishments.
- *Multilevel Security/Secret and Below Interoperability.* Accomplishments in MLS/SABI range from program management to installation and engineering of MLS/SABI implementations. A long-standing warfighter operational requirement, the MLS/SABI Program has met with great success, providing near-term engineering and installation support to the CINCs, while establishing a SABI Process to ensure the security and minimize the risk associated with these low-to-high connections. Engineering work continues to develop robust MLS capability and to provide for managed connectivity with Coalition systems.



Organization: Information Assurance Technology Analysis Center (IATAC)

J. M. McConnell, 703-289-5588

Information Assurance Points of Contact:

Robert P. Thompson, Director, IATAC, 703-289-5455
Donald J. Vincent, Information Analysis Centers, 703-289-5153
Donald G. Busson, Information Assurance, 703-289-5260
Natalie M. Givans, Information Assurance, 703-289-5406
Michael G. Otten, Information Assurance, 703-289-5427
Richard J. Wilhelm, Critical Infrastructure Protection, 703-289-5060
Mark J. Gerencser, Information Warfare, 410-684-6534

On-Line Resources:

IATAC Home Page: <http://www.iatac.dtic.mil>
IATAC E-Mail: iatac@dtic.mil

Missions and Functions:

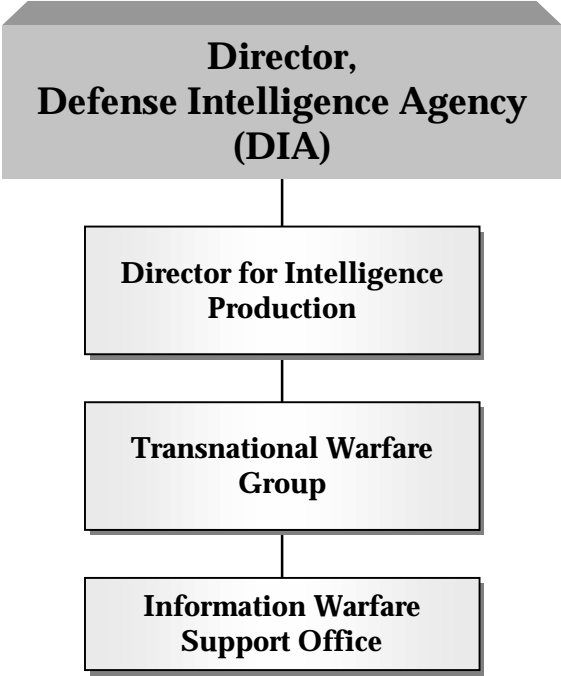
The Information Assurance Technology Analysis Center (IATAC) is one of thirteen DOD-sponsored Information Analysis Centers (IACs), IATAC is managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA). IATAC provides the Department of Defense (DOD) with emerging scientific and technical information in support of Defensive Information Operations. IATAC's mission is to provide a DOD central point of access for Scientific and Technical Information (STI) on Information Assurance emerging technologies. These technologies include system vulnerabilities, research and development, models, and analysis to support the effective defense against Information Warfare attacks. IATAC focuses on all defensive activities related to the use of information, information-based processes and information systems. IATAC operates at the classified and unclassified levels, with home page operations available via SIPRNET and JWICS access.

Activities:

- IATAC basic services include the collection, analysis and dissemination of Information Assurance scientific and technical information. IATAC's Information Assurance Library includes the below listed categories.
 - Biometrics
 - C4I
 - Computer Network Attacks
 - Critical Infrastructure Protection
 - Encryption
 - Firewalls
 - Hackers

- Information Assurance
- Information Operations
- Information Warfare
- Intrusion Detection
- Red Teaming
- Vulnerability Analysis
- Virus/Anti-Virus.
- IATAC analyzes the STI information to respond to user inquiries. The technical complexity of inquiries vary from basic requests for products to more complex requests such as how to develop secure code for home pages. DOD inquiries that require 8 hours or less of technical support to complete are provided at no cost to the DOD originator.
- IATAC maintains an Information Assurance Tools database that contains information on intrusion detection, vulnerability analysis, firewalls, and anti-virus tools. Additional IA-related databases include Bibliographic, Critical Infrastructure Protection, and Subject Matter Expert.
- IATAC hosts technical workshops and courses to promote greater awareness of critical IA technologies. IATAC conducts a workshop on Penetration Testing that includes an introduction to penetration testing, approaches to testing, building a penetration testing capability, the development of testing scenarios, and performing the penetration tests.
- IATAC's technical area task program supports five pillars of information assurance: authentication, access control, confidentiality, integrity, and non-repudiation. IATAC supports tasks in the following information assurance areas: certification and accreditation, vulnerability assessments, security test and evaluation, red teaming, public key infrastructure, program protection planning, and security policies.
- An overview of IATAC products (i.e. reports and current awareness material) is provided below:
 - *Information Assurance Digest* (disseminated in association with The Joint Staff (J6K)). The Information Assurance Digest is a monthly news summary of IA articles. IATAC identifies articles for inclusion in the digest, coordinates re-print requests with publishers, and compiles the digest for distribution. The Information Assurance Digest is produced on a monthly basis.
 - *Information Assurance Newsletter*. The Information Assurance Newsletter supports the DOD IA current awareness initiatives. The Newsletter provides a forum through which to share organizational IA initiatives with the broader IA Community. IATAC solicits articles from various sources and levels: OSD/Joint Staff, CINC, Service, Systems Command, Government R&D, Coalition, Academia, and Vendors. The Information Assurance Newsletter is produced on a quarterly basis.
 - *Technical Report on Modeling and Simulation Activities in Support of Information Assurance*. This technical report describes models, simulations and tools used by DOD organizations chartered with the IA mission. Data collection efforts focused on the current definitions of Information Operations and Information Warfare.
 - *IA Tools Report on Intrusion Detection*. This IA Tools Report provides an index of intrusion detection tool descriptions contained in the IATAC IA Tools database. Research for this report identified 43 intrusion detection tools currently employed and available.

- *IA Tools Report on Vulnerability Analysis.* This IA Tools Report provides an index of vulnerability analysis tool descriptions contained in the IATAC IA Tools database. Research for this report identified 35 intrusion detection tools currently employed and available.
- *IA Tools Report on Firewalls.* This IA Tools Report provides an index of firewall tool descriptions contained in the IATAC IA Tools database. Research for this report identified 46 intrusion detection tools currently employed and available. Report provides a basic overview of each tool to include system requirements, availability, description, and contact information.
- *State-of-the-Art Report on Malicious Code Detection.* This state-of-the-art report provides a taxonomy for malicious software, an overview of commercial products and vendors, a description of DOD initiatives, as well as future trends.



Organization: Defense Intelligence Agency (DIA)

Senior Information Operations Official:

Arthur Zuehlke, Chief, Transnational Warfare Group, Directorate for Intelligence Production, 202-231-3488

Information Operations Points of Contact:

Dr. John Yurechko, Defense Intelligence Officer (DIO) for Information Operations, 202-231-3554

Michael Lamb, Chief, Information Warfare Support Office, 202-231-3554

Senior Critical Infrastructure Protection Official:

Dr. John Yurechko, Chief Infrastructure Assurance Officer, 202-231-3554

On-Line Resources:

DIA Homepage: <http://www.dia.mil>

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.
- Serve as the focal point for DOD Information Operation Indications and Warning.
- 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.

Activities:

- DIA has established an Information Warfare Support Office with a staffing level of 85 people.
- DIA is currently leading key intelligence efforts:
 - With the advent of the information age and the threat posed by information operations, the U.S. intelligence community has adopted a new approach to fulfilling its strategic and tactical indications and warning responsibilities. Conventional indications and warning mechanisms, procedures, and protocols do not suffice for information operations. 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 Joint Information Warfare Threat Analysis Working Group, to exchange and discuss relevant threat information.

This page intentionally left blank.

**National Security Agency
(NSA)**

Organization: National Security Agency (NSA)

Senior Information Operations Official:

Lawrence Castro, 410-854-7087

On-Line Resources:

NSA Homepage: <http://www.nsa.gov:8080>

Missions and Functions:

The National Security Agency's (NSA) Information Systems Security Organization (ISSO) re-organized its Defensive Information Operations (DIO) efforts effective February 1, 1999. A new organization, called X Group, combined a number of elements involved in defensive information operations that were previously located throughout the ISSO.

The mission of X Group is to provide DIO analytic, reporting, and operations expertise and capabilities to information assurance (IA) planners and decision makers throughout the Department of Defense (DOD), and to other users, operators, and owners of national security and critical infrastructure systems.

The X Group portion of the ISSO Strategic Plan outlines the following six objectives:

- Disseminate near-real-time intrusion alerts, advisories and threat reports to enable customers to take appropriate action to defend their information systems.
- Provide operational and exercise support to enhance customers' operational readiness and measure the results.
- Apply technologies and tools to optimize the analysis of DIO-relevant data.
- Develop and demonstrate methods and techniques to support intrusion response and attack sensing and warning operations.
- Leverage internal and external partnerships to optimize the defense of customers' information systems.
- Increase emphasis on, and manpower investment in, DIO and transfer expertise to customers.

To meet these objectives, X Group:

- Provides unique, tailored, and time-critical DIO support, including management oversight of the National Security Operation Center's Information Protection Cell/Senior Information Protection Officer (IPC/SIPO).
- Serves as a focal point for DOD exercises requiring DIO support.
- Maintains analytic, reporting, and data connectivity to the various intelligence communities to facilitate acquisition, exchange, and dissemination of all-source intelligence material within NSA and the intelligence community.

- Provides the analysis, reporting, planning, and coordination of interdependent DIO disciplines and activities across NSA.
- Performs and provides, either directly or through teaming, analysis and reporting of all-source information, including trend analysis reporting, inputs to customers' risk management decisions, and development and review of customer requirements.
- Serves as the NSA focal point for DIO awareness and training and matters relevant to critical infrastructure initiatives.
- Conducts INFOSEC assessments or, in some cases, trains other organizations to perform their own INFOSEC assessments, by analyzing the threat to each system, identifying the vulnerabilities of each system, and recommending countermeasures.
- Provides internal NSA guidance and direction for IA tool and technology development.
- Provides Operations Security (OPSEC) support, training, and consulting services to NSA/CSS and U.S. Government departments and agencies, and other U.S. Government-sponsored entities as needed.
- Monitors U.S. Government telecommunications/information systems in support of department, agency, military service, JCS, CINC, unified command, and NSA requirements.
- Establishes and sustains a red team exercise capability.
- Conducts system vulnerability assessments for DOD and civil national security customers.

The INFOSEC Monitoring and Analysis/Joint COMSEC Monitoring Activity (JCMA) conducts COMSEC and INFOSEC monitoring of U.S. Government national security-related telecommunications systems and assesses the vulnerability of these systems to intercept and exploitation. JCMA supports:

- The CINC, JTFs, DOD agencies and some civil agencies (e.g., the Department of Commerce, Customs, and the Coast Guard) with friendly force COMSEC monitoring. Their focus is on COMSEC practices and procedures and on discovering and reporting system vulnerabilities.
- Deployed forces during exercises and real-world operations. Deployed JCMA teams provide friendly force COMSEC monitoring to discover and correct vulnerabilities as a proactive force protection measure. These teams identify, in real time, the compromise of mission-sensitive information and alert commands and provide recommendation for future operations.

The Office of Operations Readiness and Assessments provides critical infrastructure protection support, red teaming operations security (OPSEC) services and vulnerability assessments to DOD customers (including the CINCs, Joint Staff, JWFC, JC2WC, DIA, DISA, DSWA, the Service IW Centers, JTF-CND, and SPAWAR). The Office also operates the Interagency OPSEC Support Staff (IOSS), providing OPSEC services to all U.S. Government departments and agencies having a national security mission as directed by Presidential directive. The Office conducts information security readiness assessments of overall information security readiness through the use of red teams and vulnerability

assessments; provides risk mitigation support; and disseminates threat and vulnerability information.

The Office of Network Defense Operations provides tailored, time-critical, all-source analysis and reporting on matters addressing the threat, warning, detection and response to intrusions into national security and critical infrastructure networks. These efforts come together in the National Security Incident Response Center (NSIRC) which is called for by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) in its Directive No. 503. The NSIRC facilitates/coordinates responses to security incidents and vulnerabilities threatening national security systems; supplements DOD and other departmental activities with timely support during incidents; and develops and disseminates appropriate reports. The Office:

- Operates the Information Protect Cell (IPC) as the twenty-four hour a day, seven days a week analysis, reporting and response center for the NSIRC.
- Publishes time-sensitive analyses such as alerts and advisories, including a weekly summary of all intrusions.
- Provides analysis of network intrusions and exploitations including in-depth technical analysis.
- Provides broad, long term, all-source analysis of threats to U.S. Government communications and information systems.

Activities:

For activities, contact the Point of Contact or visit the on-line resource.

This page intentionally left blank.



Executive Branch

This page intentionally left blank.



Organization: National Economic Council (NEC)

Senior Information Operations Official:

Gene Sperling, Assistant to the President for Economic Policy
Sally Katzen, Deputy Assistant to the President for Economic Policy

Information Assurance Points of Contact:

Tom Kalil, Special Assistant to the President for Economic Policy, 202-456-5366,
kalil_t@a1.eop.gov

Critical Infrastructure Protection Points of Contact:

Tom Kalil, Special Assistant to the President for Economic Policy, 202-456-5366,
kalil_t@a1.eop.gov

On-Line Resources:

NEC Homepage: <http://www.whitehouse.gov/WH/EOP/nec/html/index.html>

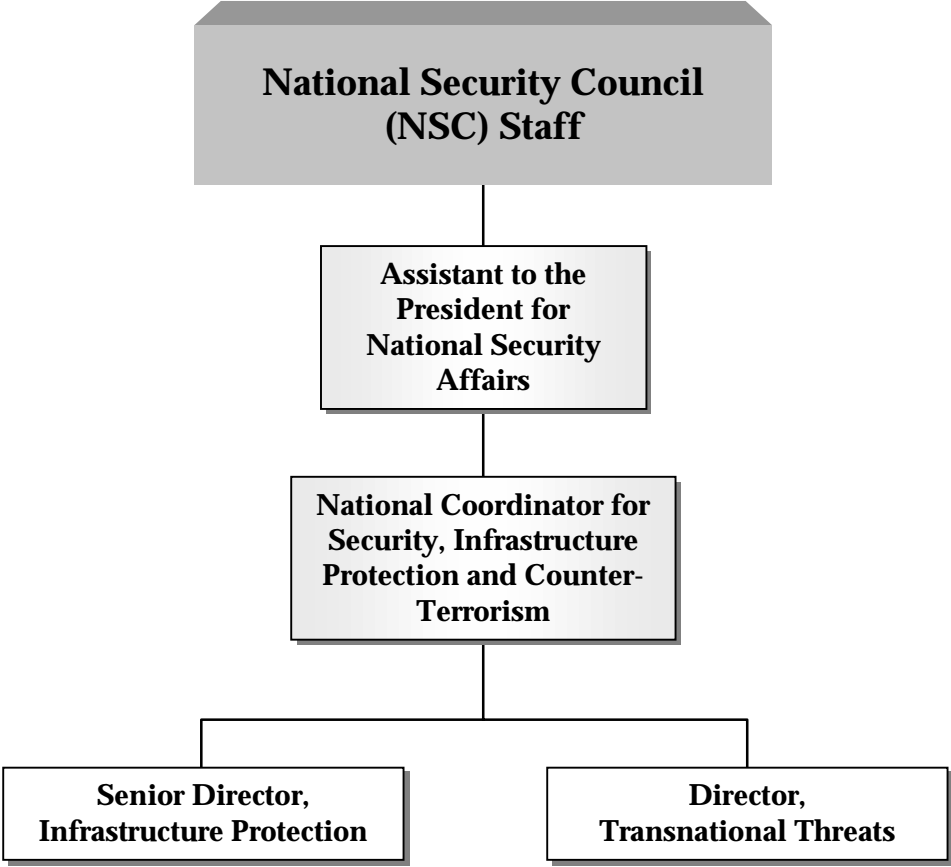
Missions and Functions:

The NEC was created by Executive Order on January 25, 1993. The principal functions of the Council are:

- To coordinate the economic policy-making process with respect to domestic and international economic issues
- To coordinate economic policy advice to the President
- To ensure that economic policy decisions and programs are consistent with the President's stated goals, and to ensure that those goals are being effectively pursued
- To monitor implementation of the President's economic policy agenda.

Activities:

- Sally Katzen, Deputy Assistant to the President for Economic Policy has been designated a member of the Critical Infrastructure Coordination Group (CICG).
- Tom Kalil, Special Assistant to the President for Economic Policy has been designated the co-chair of the CICG Working Group on ISACs (Information Sharing and Analysis Centers).



Organization: National Security Council (NSC) Staff

Senior Information Operations Official:

Richard A. Clarke, National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, NSC, 202-456-9351

Information Assurance Points of Contact:

Philip C. Bobbitt, Senior Director for Infrastructure Protection, NSC Staff, 202-456-9351

Mary McCarthy, Senior Director for Intelligence, NSC Staff, 202-456-9341

Mark C. Montgomery, Director for Transnational Threats, NSC Staff, 202-456-9361,
mark_c._montgomery@nsc.eop.gov

Critical Infrastructure Protection Points of Contact:

Philip C. Bobbitt, Senior Director for Infrastructure Protection, NSC Staff, 202-456-9351

Mark C. Montgomery, Director for Transnational Threats, NSC Staff, 202-456-9361,
mark_c._montgomery@nsc.eop.gov

On-Line Resources:

NSC Homepage: <http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html>

Missions and Functions:

Members of the National Security Council 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.

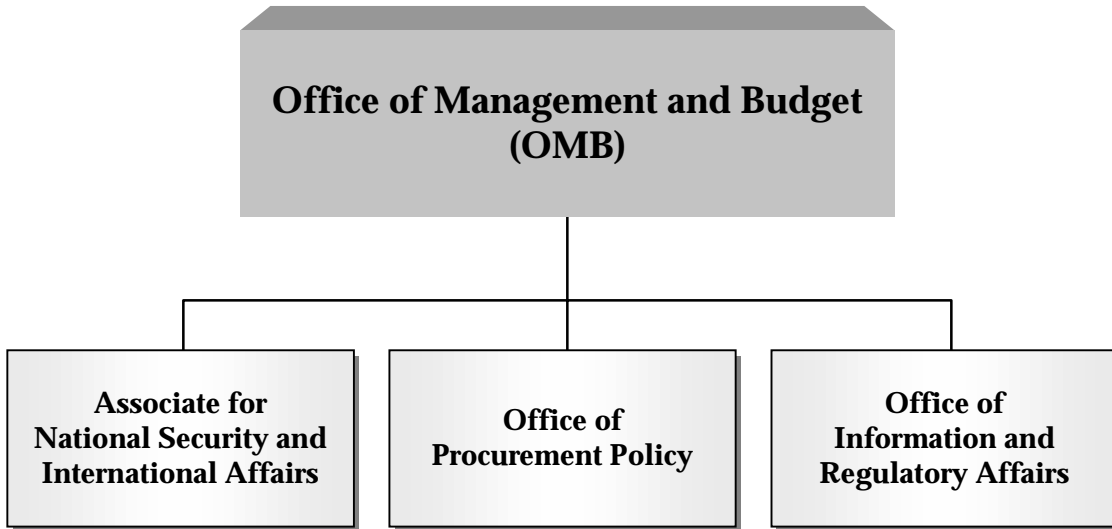
The Secretary of the Treasury, the U.S. Trade Representative, the Chief of Staff to the President, and the Assistants to the President for National Security Affairs and Economic Policy are invited to all meetings of the Council.

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.

Activities:

The NSC is coordinating the implementation of Presidential Decision Directive 63, “Critical Infrastructure Protection”. These efforts include:

- Development of the National Information System Defense Plan.
- Monitoring of federal agency critical infrastructure protection plans.
- Fostering of a public-private sector partnership on information assurance.



Organization: Office of Management and Budget (OMB)

Senior Information Operations Official:

Don Arbuckle, Acting Administrator, Office of Information and Regulatory Affairs,
202-395-4852

Information Assurance Points of Contact:

Glenn Schlarman, Senior Policy Analyst, Information Policy and Technology Branch,
202-395-3785, schlaman_g@a1.eop.gov

Critical Infrastructure Protection Points of Contact:

Glenn Schlarman, Senior Policy Analyst, Information Policy and Technology Branch,
202-395-3785, schlaman_g@a1.eop.gov

On-Line Resources:

OMB Homepage: <http://www.whitehouse.gov/WH/EOP/omb>

Missions and Functions:

- The Office of Management and Budget evaluates, formulates, and coordinates budget and management policies and objectives 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 on 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. The security principles and policies of Appendix III are fully compatible with the requirements of PDD-63, "Critical Infrastructure Protection." National security information and systems as well as national security emergency preparedness activities are subject to additional regulations under appropriate directives and executive orders. OMB works closely with the CIO Council and the council's Security Committee to implement and share best security practices and leverage scarce agency resources.
- OMB Circular No. A-130, Management of Federal Information Resources, is issued pursuant to OMB's authorities under the Clinger-Cohen Act (formerly known as the

Information Management Reform Act of 1996), Paperwork Reduction Act, (44 U.S.C., Chapter 35), the Computer Security Act of 1987, 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

Activities:

- 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 the willing participation of from the public private sector. OMB is additionally concerned that privacy and civil liberties are appropriately considered in the equation and that new regulation of industry is avoided.
- 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 controls. 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: agency investments in information technology, intellectual property rights, software protection, privacy, freedom of information, and security. National Performance Review implementation underway through Government Information Technology Services Board (GITSB) primarily concerning key recovery demonstration projects.

This page intentionally left blank.

**Office of
Science and Technology Policy
(OSTP)**

**Assistant to the President
for
Science and Technology**

**Associate Director for
National Security and
International Affairs**

Organization: Office of Science and Technology Policy (OSTP)

Senior Information Operations Official:

Vacant, Associate Director for National Security and International Affairs

Information Assurance Points of Contact:

Dr. Steven Rinaldi, Office of Science and Technology Policy, 202-456-6057,
rinaldi@ostp.eop.gov

Critical Infrastructure Protection Points of Contact:

Dr. Steven Rinaldi, Office of Science and Technology Policy, 202-456-6057,
rinaldi@ostp.eop.gov

On-Line Resources:

OSTP Homepage: http://www.whitehouse.gov/WH/EOP/OSTP/html/OSTP_home.html

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 the United States continues to maintain global leadership in science, mathematics and engineering research; and that science continues to provide support for the successful resolution of important problems in the areas of health, agriculture, the economy, energy, social well-being, education, and national security. The Division focuses on maintaining a Federal research program that is based on excellence and strongly coupled to education.

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:

- Sustaining U.S. technological leadership through partnerships to promote the development of innovative technologies
- R&D and policy initiatives for advanced computing and communications technologies
- Advancing technologies for education and training
- The U.S. space and aeronautics program, including the space station.

Environment Division

The Associate Director for Environment leads the White House efforts to:

- A sound scientific and technical underpinning for environmental policies
- An interagency R&D strategy for environment and natural resource issues.

Priority policy areas include global climate change, ozone depletion, loss of biological diversity, desertification, deforestation, pesticides and toxic substances, urban and regional air quality, environmental technologies, water quality, hazardous and solid waste, natural hazards, and marine pollution. The division also has responsibility for promoting risk analysis and environmental education programs, and supporting the development of regional ecosystem approaches to environmental protection.

National Security and International Affairs Division

The Associate Director for National Security and International Affairs leads the White House effort to strategically promote the contribution of science and technology to national security, global stability, and economic prosperity. Division activities address science and technology policies in national security, the commerce-security nexus, and international engagement to contribute to the quality and productivity of the U.S. science and technology

enterprise and foreign policy goals. National security science and technology policy priorities include nuclear materials security, nuclear arms reduction, nonproliferation of weapons of mass destruction, critical infrastructure protection, and counterterrorism. Priorities in the commerce-security nexus include international technology transfer, export controls, information security, and dual-use technology policies. Science and technology priorities to strengthen U.S. goals and capabilities through international engagement include science capacity building, science and technology for economic growth and competitiveness, sustainable development and science and technology to address global threats.

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 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 (NCS), 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)

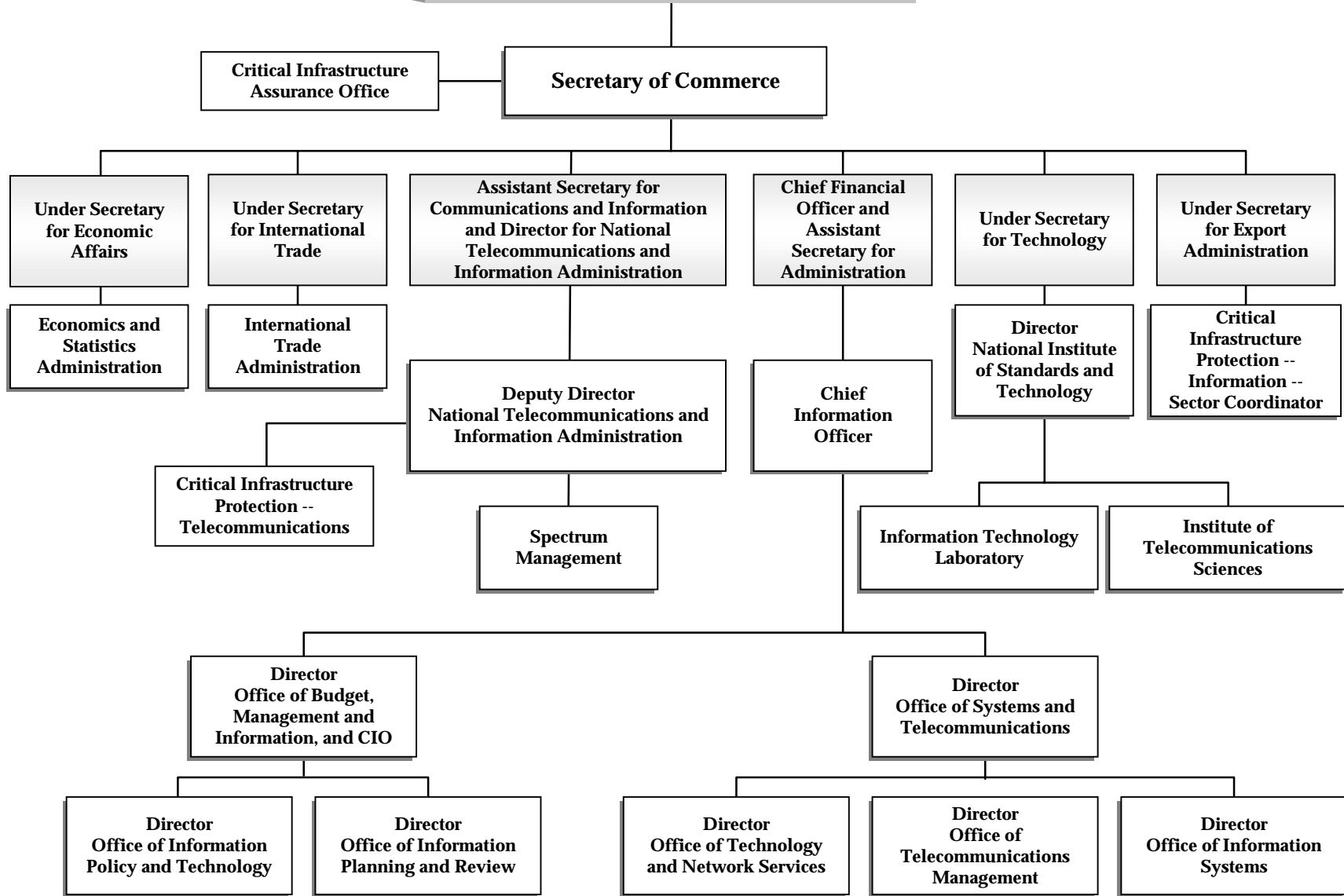
- Responsibilities under the Federal Response Plan. The Robert T. Stafford Disaster Relief and Emergency Assistance Act provides the authority to the Federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property. 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 critical infrastructures, information networks, computers and communications systems, and emergency telecommunications services. OSTP also maintains professional relationships with the broader national scientific and technical community.
- Critical Infrastructure Protection. As designated in PDD-63, OSTP is responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council.

Activities:

- Critical Infrastructure Protection: Working closely with the National Science and Technology Council, OSTP coordinates, recommends, and monitors Federal research and development for critical infrastructure protection. OSTP ensures that the Federal R&D agenda for critical infrastructure protection is coordinated with and leverages other related Federal R&D programs, such as high performance computing initiatives and weapons of mass destruction protection programs. Recognizing the essential roles that the private sector and academia play in critical infrastructure protection R&D, OSTP fully supports and encourages the development of an R&D partnership among the government, private sector, and academia.

This page intentionally left blank.

**Department of Commerce
(DoC)**



Organization: Department of Commerce (DoC)

Senior Information Assurance Official:

D. Holmes, Director of Security, Roger Baker, Chief Information Officer, 202-482-4371 or 202-482-4797

Information Assurance Points of Contact:

G. Imber, Director Office of Technical Support and Network Services, 202-482-2096

Senior Critical Infrastructure Protection Official:

Jeffrey Hunker, Chief, Critical Infrastructure Assurance Office, 202-482-6055
Roger Baker, Chief Information Officer, 202-482-4797

Critical Infrastructure Protection Points of Contact:

I. Pikus, Sector Coordinator, Information, 202-482-1116
S. Kinney, Sector Coordinator, Telecommunications, 202-482-1830
D. Holmes, Director of Security, 202-482-4371

On-Line Resources:

DoC Homepage: <http://www.doc.gov>

Missions and Functions:

The Department of Commerce encourages, serves, and promotes the Nation's trade policy for international trade, economic growth, and technological advancement. DoC offers assistance and information to increase America's competitiveness in the world economy; administers programs to promote fair 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 (BXA) 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 prohibited countries, and for various foreign policy objectives. BXA 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 (ITA) 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 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 (NOAA) 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. NOAA's 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 Atmosphere Research. NOAA's corp is staffed as the uniform service with naval officers who command NOAA ships and aircraft.

The National Telecommunications and Information Administration (NTIA) responsibilities include frequency management and are described in a separate organizational summary.

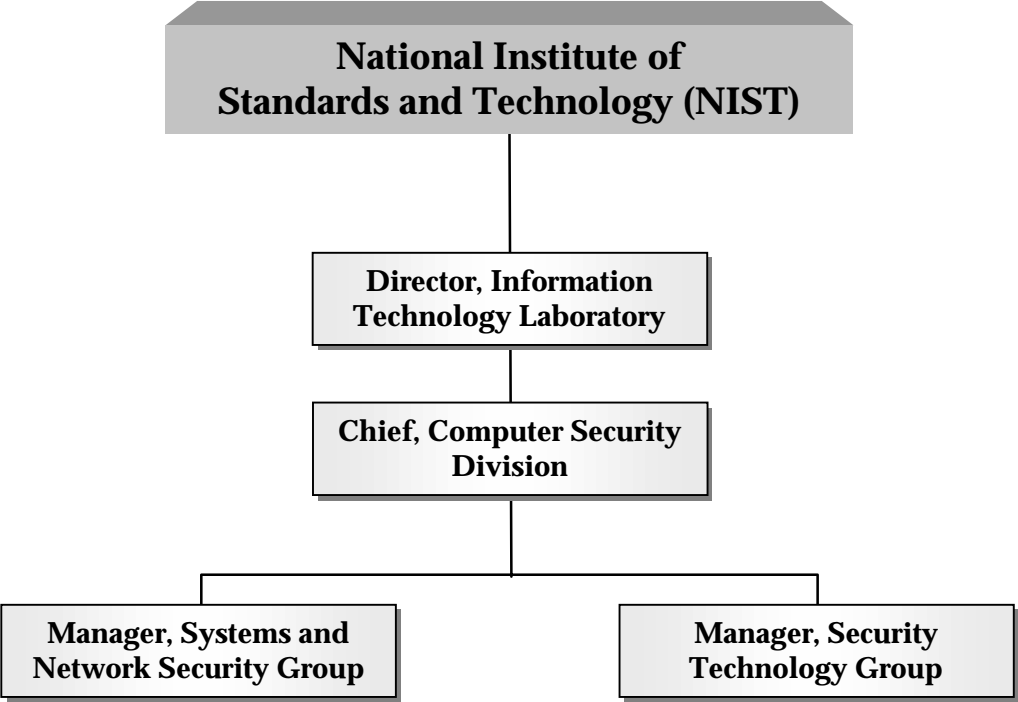
The Technology Administration (TA) is responsible for working with U.S. industry in addressing competitiveness issues. TA discharges this role through the Office of Technology Policy by advocating coherent policies for maximizing the impact of technology on economic growth, through the National Institute 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 Economics 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 Census and the Bureau of Economic Analysis. The Bureau of the Census collects, tabulates and publishes a wide variety of statistical data about the people and the economy of the Nation. The goal of the Bureau of Economic Analysis provides 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.

Activities:

- Within the Department of Commerce all 13 elements have a Chief Information Officer (CIO). They have their own internal CIO Council.
- CIO maintains INFOSEC responsibility.
- Working with DOD an upgrade of Defense Message System (DMS) because commerce uses Autodin quite frequently.
- Working on encryption algorithm for protection of Next Generation Internet (NGI).
- Established a comprehensive web page with extensive links.
- Works with DOD for transfer of technology for Defense Science Board (DSB) and National Institute and Technology for outside organizations.
- Efforts continue in the Department's Y2K efforts to ensure systems that support the nation remain operational.
- The Census Bureau has developed a plan for conducting Census 2000 incorporating many new features. The Census 2000 plan redesigns the census process in bold and fundamental ways. The schedule began back in late 1996 and continues until completion. April 1, 2000 is Census day.



Organization: National Institute of Standards and Technology (NIST), U.S. Department of Commerce

Senior Information Operations Official:

Paul Domich, Acting Deputy Director, Information Technology Laboratory, 301-975-2144
Dan Benigni, Chief Information Officer, NIST, 301-975-3279

Information Operations Points of Contact:

Paul Domich, Acting Deputy Director, Information Technology Laboratory, 301-975-2144
Dan Benigni, Chief Information Officer, NIST, 301-975-3279

Senior Information Assurance Official:

Shukri Wakid, Director, Information Technology Laboratory, 301-975-2904

Information Assurance Points of Contact:

Miles Smid, Acting Chief, Computer Security Division, 301-975-2934
Edward Roback, Acting Deputy, Computer Security Division, 301-975-3696
Tim Grance, Manager, Systems and Network Security Group, 301-975-4242
Donna Dodson, Acting Manager, Security Technology Group, 301-975-2921

Senior Critical Infrastructure Protection Official:

Paul Domich, Acting Deputy Director, Information Technology Laboratory, 301-975-2144

Critical Infrastructure Protection Points of Contact:

Miles Smid, Acting Chief, Computer Security Division, 301-975-2934

On-Line Resources:

NIST Homepage: <http://www.nist.gov>

NIST Security Activities: <http://csrc.nist.gov>

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. NIST carries out this mission through four major programs, each one addressing different components of the technology pipeline. The four major programs are:

- The Measurement and Standards Laboratories which works at all stages of the pipeline advancing basic science and pioneering new measurement methods to the development of standard test methods, materials, and data to ensure the quality of commercial products.
- The Advanced Technology Program helps fill the gaps that often exist between basic research advances and commercialization by providing cost-shared funding to industry for development of high risk, “enabling” technologies with broad commercial potential.
- The Manufacturing Extension Partnership uses a nationwide network of centers to help smaller manufacturers adopt technologies and business practices that can improve their competitiveness in the global marketplace.
- The Baldrige National Quality Program provides information to companies of all sizes on how to continuously improve their products, services, and processes through effective business and quality management.

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 Government Affairs of security issues. These responsibilities are carried out by the Information Technology Laboratory (ITL).

Within the Infrastructure Technology Laboratory, the Computer Security Division provides guidance and technical assistance to government and industry in the protection of unclassified automated information systems. With the growth of electronic commerce and increase use of distributed systems linked by networks, the need to ensure the security of data and the privacy of information becomes critical.

Activities:

The Computer Security Division is working the following projects:

- Advanced Encryption Standard – Purpose is to develop an encryption algorithm capable of protecting sensitive information well into the next century and serve as the successor to the current Data Encryption Standard (DES).
- Attack and Incident Mitigation – Attack scripts are widely available on the Internet that allow automatic penetration of hosts. NIST is responding to this threat by developing a tool that identifies published attacks that meet user defined characteristics. The tool can be used by law enforcement to identify attacks that could have compromised a penetrated host or by system administrators wishing to perform penetration testing of their site. In addition, NIST is aggregating statistics on the types of attacks that are published on the Internet and measuring the frequency of these attacks. The statistics

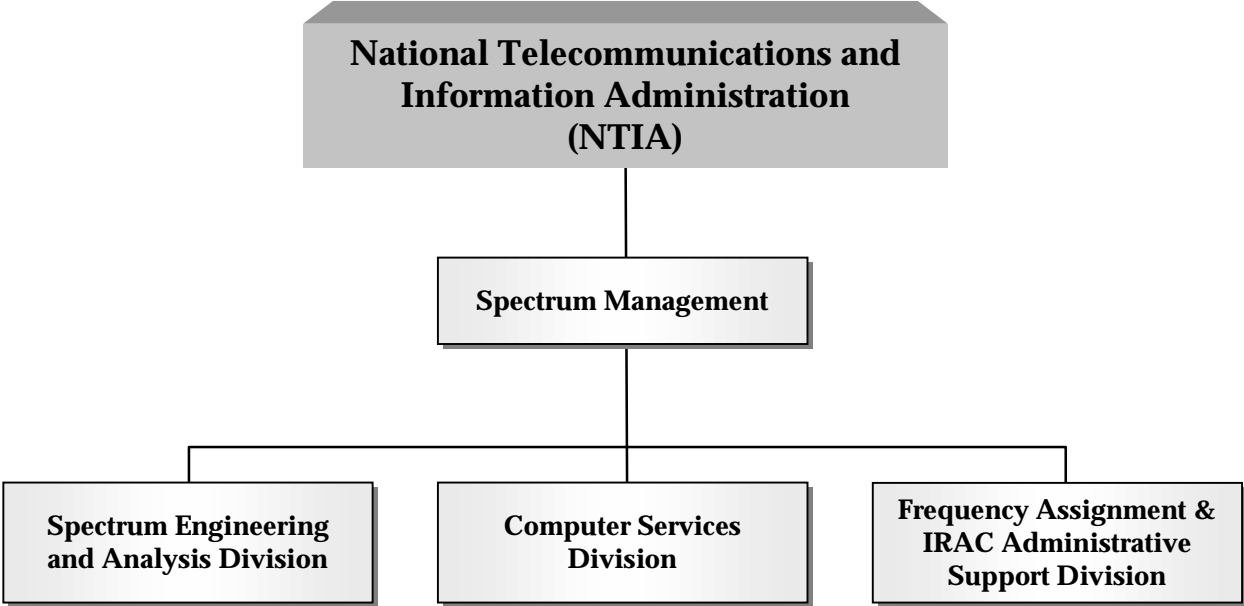
can assist policy makers to better understand the threat posted by the attacks and the attack frequency measurements can be used to create public advisories warning of new trends in attack usage.

- Computer Security Resource Clearinghouse (CSRC) – The objective is to provide a comprehensive reference of information technology security information and resources. The CSRC is a web site developed to provide access to crisis response information as well as information on security-related threats, vulnerabilities, and solutions. Additionally, the CSRC strives to be a general index to computer security information on a broad variety of subjects including general risks, privacy, legal issues, assurance, policy, planning and training.
- Critical Infrastructure Protection – As one of the lead Department of Commerce information technology components, NIST serves as a technical resource on the Administration’s Infrastructure Protection Initiative.
- Encryption Key Recovery – NIST participates as a federal liaison and serves as Executive Secretary for the “Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure.” NIST will be the principal recipient of the Committee’s recommendations to turn the recommendations into a Federal Information Processing Standard.
- Government Information Technology Services (GITS) Information Technology Security Training – The pilot project is designed to establish a single focal point for the development of IT security training for use throughout the federal government. The project will focus executive and senior management attention on the critical need to provide appropriate IT security training to their staff. The objectives of the project are:
 - To provide the need for IT security training throughout the government
 - To coordinate the dissemination of existing laws, policies procedures, and training materials
 - To assist in development of a reporting of IT security training resources appropriate for use by federal agencies.
- Internet Protocol Security (IPSec) – This NIST project focuses on emerging Internet protocols that provide increased security services at the Internet level; these services will be used to secure the infrastructure of the Internet (routing, DNS, etc.) and to protect application-level Internet communications. NIST developed a reference implementation of the IPsec Key Negotiation and Management Protocol, IKE (Internet Key Exchange). NIST’s Web-based IPsec Interoperability Tester, IPsec-WIT, is in constant use, serves as a yardstick for IPsec performance, and has helped in the development and debugging of numerous industry IPsec implementations. See <http://csrc.ncsl.nist.gov/ipsec/> and <http://ipsec-wit.antd.nist.gov/>.
- Mobile Agent Security – NIST is conducting joint research with industry in the area of mobile agent security and also working with international standards bodies to develop specifications for secure and interoperable agent frameworks. A Network Management and Security Testing prototype tool has been developed. Research is also being conducted in new threats and countermeasures against agent-based network attacks.
- National Information Assurance Partnership (NIAP) – NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP develops tools, test methods, test and validation procedures used

by developers and testing laboratories to assess and improve information technology security products and systems. Some of NIAPs key projects are developing:

- An internationally recognized Common Criteria (CC) Evaluation and Validation Scheme
 - Protection profiles and security targets in concert with the public and private sectors
 - Tests for firewalls, telecommunication switches, and other application areas
 - Automated tools for generating CC-based Protection Profiles and Security Targets
 - Collaborating with industry to establish industry-lead forums in community sectors (such as healthcare, telecommunications, and financial) for specifying and testing IT security requirements (see <http://niap.nist.gov> for more information).
- **Public Key Infrastructure** – This project works on further standardizing public key cryptography and ensuring security by establishing a network of Certificate Authorities, or a public key infrastructure. CSD Chairs the Federal PKI Technical Working Group. NIST establishes and maintains the Digital Signature Standard (DSS), a Federal Information Processing Standard. NIST also developed the Minimum Interoperability Specification of PKI Components (MISPC) and an associated reference implementation in collaboration with CRADA members.
 - **Role Based Access Control (RBAC)** – RBAC is an evolution from Discretionary Access Control (DAC) and Mandatory Access Control and is a method of managing authorization data for large networks. NIST independently developed the original RBAC design and formal specification. This NIST publication was the first formal description of role based access control, and has been used as a basis for other formal models of RBAC by a variety of researchers. As a result of RBAC research, both small and large technology firms have been able to implement advanced authorization management features while reducing time-to-market for new products (see <http://nissa.ncsl.nist.gov/rbac>).
 - **Next-Generation Internet** – NIST researchers are working to remove barriers to the next generation of reliable and secure internetworking technologies; interoperability among next-generation internetworking products; and measurement techniques and performance characterizations for network services that integrate voice, video, and data. Research projects include investigating changes to the Internet architecture that will support guaranteed bandwidth and quality of services for real-time applications, such as audio, video, and synchronized data. This project focuses on the scalability of the proposed enhancements, interoperability issues, and methods and metrics to characterize the digital data streams. More information is available on <http://snad.ncsl.nist.gov/itg/itg.html>.

This page intentionally left blank.



Organization: National Telecommunications Information Administration (NTIA)

Senior Information Assurance Official:

Larry Irving, Administrator, 201-482-1551

Information Assurance Points of Contact:

Bill Hatch, Chief, Office of Spectrum Management, 202-482-1850

Bill Gamble, Office of Spectrum Management,

Senior Critical Infrastructure Protection Official:

Irwin M. Pikus, Director, Communications and Information Infrastructure Assurance Program, 202-482-1116

Critical Infrastructure Protection Points of Contact:

Mary Wallach, CIIAP, 202-482-1116

On-Line Resources:

NTIA Homepage: <http://www.ntia.doc.gov>

OSM Homepage: <http://www.ntia.doc.gov/osmhome/osmhome.html>

Missions and Functions:

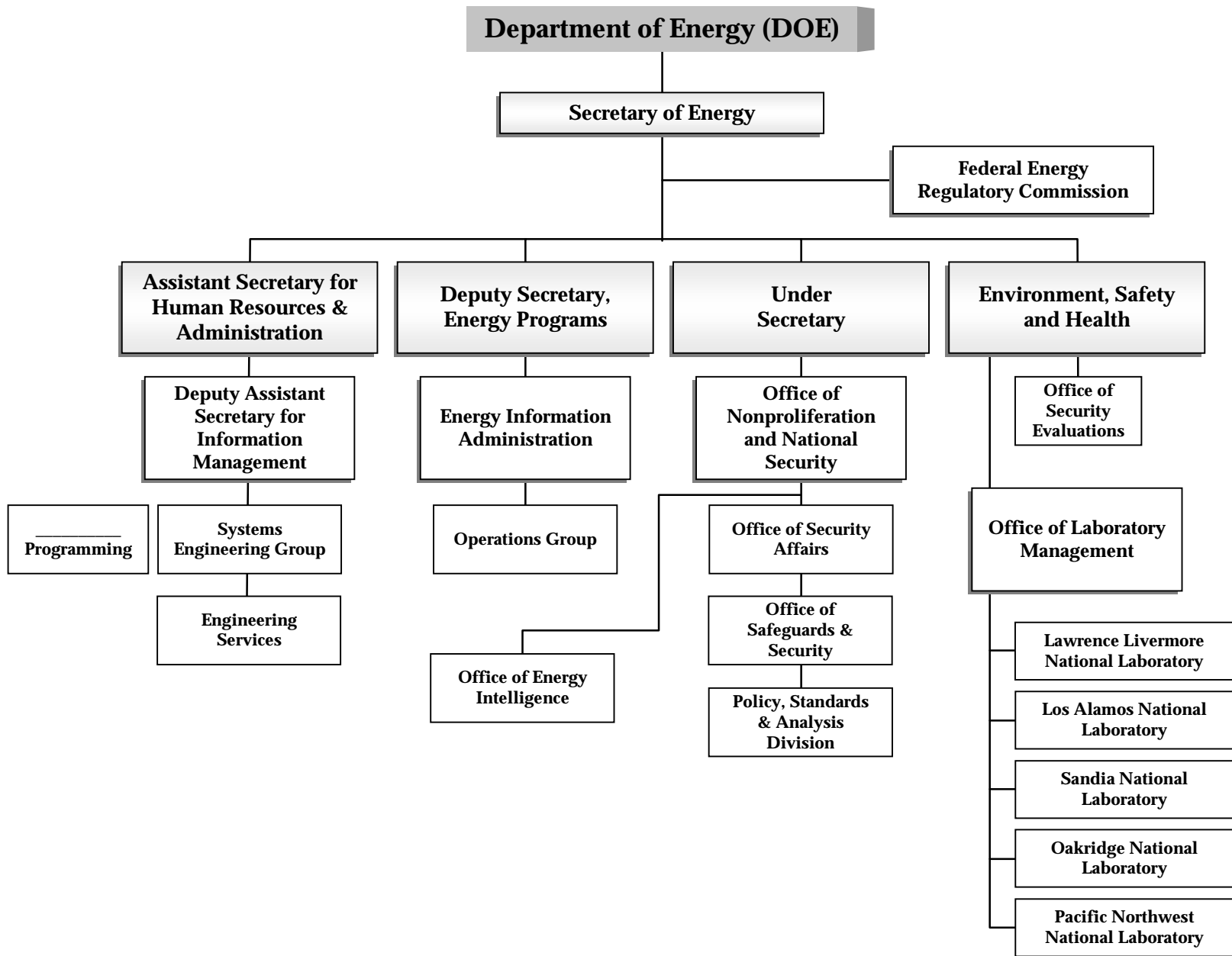
The National Telecommunications and Information Administration responsibilities are:

- 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
- To strengthen the capabilities of existing public broadcasting stations to provide telecommunications services.

Activities:

- 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.
- The Office of Spectrum Management (OSM) is responsible for managing the Federal Government's use of the radio frequency spectrum. To achieve this, OSM receives assistance and advice from the Interdepartment Radio Advisory Committee (IRAC). OSM carries out this responsibility by:
 - Establishing and issuing policy regarding allocations and regulations governing the Federal spectrum use
 - Developing plans for the peacetime and wartime use of the spectrum
 - Preparing for, participating in, and implementing the results of international radio conferences
 - Assigning frequencies
 - Maintaining spectrum use databases
 - Reviewing Federal agencies' new telecommunications systems and certifying that spectrum will be available
 - Providing the technical engineering expertise needed to perform specific spectrum resources assessments and automated computer capabilities needed to carry out these investigations
 - Participating in all aspects of the Federal Government's communications related emergency readiness activities
 - Participating in Federal Government telecommunications and automated information systems security activities.
- The Communications and Information Infrastructure Assurance Program (CIAP) carries out the responsibilities of sector lead agency assigned to the Department by the President's directive on critical infrastructure protection. It is the primary liaison between the government and the communications and information sector on all infrastructure assurance matters.

This page intentionally left blank.



Organization: Department of Energy (DOE)

Senior Information Assurance Official:

Joseph Mahaley, Director, Office of Security Affairs, 202-586-6591

John M. Gilligan, Chief Information Officer, 202-586-0166

Susan Frey, C10, Executive Officer, 202-586-8682

Information Assurance Points of Contact:

Larry Wilcher, Program Manager, Information Assurance Program, 301-903-5217

David Berkay, Office of Architecture, Standards and Security

Senior Critical Infrastructure Protection Official:

Dr. Ernest Moniz, Undersecretary of Energy, 202-586-5500

Critical Infrastructure Protection Points of Contact:

Dr. Paula Scalingi, Director, Office of Critical Infrastructure Protection

Marshall Combs, Critical Infrastructure Assurance Officer, Office of Safeguards and Security, 301-903-3652

On-Line Resources:

DOE Homepage: <http://www.doe.gov>

Computer Incident Advisory Capability: <http://www.ciac.org/ciac/>

Mission 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 program.

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 Non Proliferation and National Security includes the Department of Energy Office of Critical Infrastructure Protection and the Office of Safeguards and Security.

The role of the Office of Critical Infrastructure Protection (OCIP) is to plan, facilitate and monitor the implementation of infrastructure protection activities within the Department. OCIP is the focal point for coordination and integration of Department-wide infrastructure

protection activities. These activities comprise three major missions: protect the Department's infrastructure, facilitate the protection of the National Energy infrastructure (the electric power grid, and the oil and gas transmission, storage and distribution systems), and conduct research and development on infrastructure protection technologies for all infrastructures.

Responsibilities of the Office of Safeguards and Security include oversight of protection of classified cyber-based assets and interdependencies through the Classified Information Systems Security Program in coordination with the CIO and program offices.

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.

Their responsibilities fall under three main categories: (1) National Security, (2) Science and Methodology, and (3) Environmental Quality. The Department of Energy has important national security responsibilities. The Department maintains the safety, security and reliability of the U.S. nuclear stockpile, without underground nuclear testing.

The Department of Energy laboratories help support American leadership in science and technology. These scientists and engineers are conducting breakthrough research in energy sciences and technology, high energy physics, superconducting materials, accelerator

technologies, material sciences and environmental sciences. Finally, the Department is working to assure clean, affordable, and dependable supplies of energy for the nation.

CIO Vision. Information management leadership will obtain senior management support for utilizing information technology in enhancing mission accomplishment. Corporate systems will provide the core information for supporting our business processes. Information technology capital planning and investments will build a strong infrastructure for meeting our business needs. Information management will provide computing tools to meet customer expectations and to increase Federal and contractor employee productivity.

Information management provides advice and other assistance to the head of the agency and other senior management personnel to ensure that information technology is acquired and information resources are managed in a manner that implements the policies and procedures of legislation. Information management provides for greater coordination and shared vision, to effectively manage information and to provide for corporate systems that add value to the businesses of the Department.

Information management promotes effective agency operations by encouraging performance-based management and where appropriate, facilitate the restructure of mission related processes before making significant information technology (IT) investments to improve the performance and cost-effectiveness of the Department's information management activities.

The CIO organization includes:

- *Office of Information, Records, and Resource Management.* Ensures that the Department's recorded information is managed in an economical, effective, and efficient manner throughout its life cycle in support of mission accomplishment and accountability. This encompasses the creation, maintenance, use, disposition, donation, and preservation of records, regardless of media.
- *Office of Planning, Policy, and Mission Analysis.* Provides advice and other assistance to the head of the agency and other senior management personnel to ensure that information technology and resources are planned for, acquired and managed in a manner that implements the policies and procedures of legislation, including the Paperwork Reduction Act, the ITMRA, and the priorities established by the head of the agency. Provides for greater coordination and shared vision, i.e., corporate perspective, among the Department's information activities and champion Departmental initiatives to effectively manage information and to provide for corporate systems that add value to the businesses of the Department.
- *Office of Architecture, Standards, and Information Security.* Develops and maintains, in conjunction with the Program Offices, information architecture and standards for information management initiatives in the Department of Energy. Ensures effective and efficient management of the Department's information architecture and information management infrastructure to improve responsiveness to the information needs of our customers and stakeholders. In accordance with the ITMRA, conducts analyses using the General Accounting Office approved Strategic Information Management (SIM)

process to ensure a corporate focus for Information Technology investments. Advocates Department-wide policy concerning information standards which will enhance information sharing, reliability and effectiveness throughout the Government and private sector. Assures that all Departmental IM systems adhere to Departmental quality standards. Participates on international standards committees, improving the Department's ability to support universal access to information and enhancing the management of information and its dissemination to the public and Federal community to meet intra- and inter-departmental business requirements. In collaboration with the Department's information stakeholders, works to improve the Department's access to information thus enhancing its ability to meet mission and business requirements. Guides the Software Management Program, providing a methodology for software engineering, project management, and quality assurance in all aspects of and throughout the software lifecycle. Coordinates with technology assessment teams from across the Department to facilitate the publication of results of assessments conducted and promotes implementation and deployment of new Information Technology (IT) tools to improve the effectiveness of information management. Manages the Department of Energy radio communications and frequency management program. Manages the Department-wide COMSEC, TEMPEST, PDS, and Unclassified Computer Security programs and provides assistance and guidance in these areas to all DOE entities.

- *Office of Operations, Engineering, and Customer Service.* Provides advice and technical infrastructure support to the CIO and other senior Departmental officials to ensure delivery of vital IM and IT services. Serves as the Headquarters Chief Information Officer in the facilitation and collaboration necessary to ensure quality services. Provides for IM and IT administrative information systems and business reengineering. Provides IM/IT operations planning, management, and operational support for computer systems, telecommunications systems, and Local and Wide Area Networks required to sustain the Department-Wide IM systems. Manages and operates the nationwide, secure, record communications network. Manages and operates the Network Management Information Center to provide technical control, circuit management, and transmission system support. Provides telephone, voice mail, and telephone operator services for Headquarters personnel located at various sites throughout the metropolitan Washington, DC, area. Supplies nationwide cellular communications, nationwide pagers, facsimile systems, and hand-held portable telephones. Provides secure voice telephones, secure data devices, and secure televideo conferencing systems and services. Provides unclassified televideo systems, operations, maintenance, and services to Headquarters. Provides desktop computer systems installation, enhancements, software implementation, applications and IT training, technical assistance, and help desk services for all Headquarters customers in support of their distributed information management requirements. Provides direct support to the Office of the Secretary on all automated data processing and telecommunications systems and video services. Provides foreign travel support to the Office of the Secretary on all automated data processing and telecommunications systems and video services. Provides foreign travel support to the Office of the Secretary, as required. Manages and facilitates the IM business lines included within the Working Capital Fund.

Activities:

- Information security responsibilities are split in DOE. Office of IRM is responsible for unclassified information (to include connections to Internet), the Office of Nonproliferation and National Security is responsible for classified information. Office of Energy Intelligence.
- The Assistant Secretary for Environment, Safety, and Health operates an Office of Security Evaluations.
- DOE's ESNet is the primary backbone of the Internet.
- The 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.
- DOE owns the National Laboratory facilities and products of research. The laboratories are operated by independent entities, such as the University of California.
- Within the DOE, there exists the following information and information management.
 - DOE IM Council
 - Interagency CIO Council
 - Capital Planning and IT Investment Committee
 - Callaboration Group
 - Committee on Computing, Information, and Communications R&D (CCIC)
 - Computing, Information, and Communications R&D (CIC R&D) Subcommittee
 - Corporate IM Guidance Group
 - Executive Committee for Information Management (ECIM).
- The DOE has established an unclassified computer security program web page to educate users on computer security.
- The objective of the ECIM is to serve as the senior management group for departmental initiatives to employ information to increase mission effectiveness and program accomplishment. The committee provides a senior management focus to ensure the objectives are reached in a cost-effective manner from a corporate standpoint, so as to minimize the development of duplicative and overlapping information systems. The Committee's specific responsibilities include:
 - Promoting the focus of managers on the value of information and the need to manage it properly from a corporate standpoint.
 - Promoting the development of a cost-effective Department-wide information infrastructure that supports effective proactive management of the Department.
 - Ensuring that the required resources are available.
 - Overseeing the implementation of policy decisions and cross-cutting activities.
 - Directing Department-wide efforts to establish measurable information management goals, including reliable and relevant measurements of performance.
 - Providing corporate leadership to the Department's Information Management council.

- Developing an automated tool to help select, control, and evaluate major IT investments. The tool is called Information Technology Investment Portfolio System. When complete it will fully implement the selection monitoring and evaluation phases of the capital planning process.

This page intentionally left blank.

**Lawrence Livermore National
Laboratory
(LLNL)**

Organization: Lawrence Livermore National Laboratory (LLNL)

Information Operations Points of Contact:

J. Smart, Program Manager, Information Operations, Warfare and Assurance (IOWA) Initiative, 925-423-0733, smart1@llnl.gov

Senior Information Assurance Official:

David Grubb, Computer Security Manager, Computer Security Organization (CSO), 925-423-4745, gubbl@llnl.gov

Information Assurance Points of Contact:

Mike Pruitt, Acting Computer Security Site Manager, 925-422-3350, puit2@llnl.gov
Bill Robson, Computer Protection Program Manager, 925-423-7261, robson@llnl.gov
Doug L. Mansur, Program Manager, Computer Security Technology Center (CSTC), 925-422-0896, mansur@llnl.gov
Sandy Sparks, Project Leader, Computer Incident Advisory Capability (CIAC), 925-422-6856, ssparks@llnl.gov

On-Line Resources:

Computer Incident Advisory Capability: <http://ciac.llnl.gov>
Computer Security Technology Center: <http://ciac.llnl.gov/cstc/CSTCHome.html>

Missions and Functions:

The Computer Security Organization (CSO) ensures compliance with DOE orders relating to computer network and telecommunications security; coordinates training, education and awareness of computer security issues; coordinates and represents the Lab in negotiations between LLNL and other government agencies on issues of computer and communications security; provides assistance and advice on technical issues relating to computer security; and provides a response team to assist in threat analysis, incident response, and computer security forensics.

The Computer Security Technology Center (CSTC) is an element of the Computation Organization at the LLNL and 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).

Activities:

- Development is underway for a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources. This system will use large numbers of small sensors across a large network environment to track and detect unauthorized or suspicious activity. Immediate response to the threat will be possible to permit actions to limit or deny the actions of the attacker.
- Other information assurance activities emphasize network security topics, with particular specialization in the areas of vulnerability analyses and security profiling, network intrusion detection, security architecture, education, and tools for security management.

This page intentionally left blank.

**Los Alamos National Laboratory
(LANL)**

Organization: Los Alamos National Laboratory (LANL)

Senior Information Operations Official:

Terry Hawkins, 505-665-1259, hthawkins@lanl.gov

Information Operations Points of Contact:

Keith Lindsay, 505-665-4335, klindsay@lanl.gov

Senior Information Assurance Official:

Chad Olinger, 505-665-8564, colinger@lanl.gov

Information Assurance Points of Contact:

Keith Lindsay, 505-665-4335, klindsay@lanl.gov

Senior Critical Infrastructure Protection Official:

Don Cobb, 505-667-1437, dcobb@lanl.gov

Critical Infrastructure Protection Points of Contact:

Keith Lindsay, Cyber, 505-665-4335, klindsay@lanl.gov
Wayne Hardie, Modeling & Simulation, 505-667-2142, hardie@lanl.gov

On-Line Resources:

LANL Homepage: <http://www.lanl.gov>

Missions and Functions:

The following is a top-level list of the missions of Los Alamos National Lab. Work in Information Operations falls under the Nonproliferation/Counterproliferation mission area.

- Stockpile Stewardship ensures that the U.S. has safe, secure, and reliable nuclear weapons.
- Stockpile Management provides capabilities ranging from dismantling to remanufacturing of the enduring stockpile.
- Nuclear Materials Management ensures the availability and safe disposition of plutonium, highly enriched uranium, and tritium.

- Nonproliferation and Counterproliferation help to deter, detect, and respond to the proliferation of weapons of mass destruction.
- Environmental Stewardship provides for the remediation and reduction of wastes from the nuclear weapons complex.

Activities:

In support of the Lab's core missions, there are many ongoing activities that have a related IO focus. These are not exactly presented here. However, a general sense of the sorts of activities and their underlying motivations is provided.

The Laboratory develops and provides a full spectrum of capabilities for responding to threats to domestic and international security and critical infrastructure, including, when necessary, methods for mitigating and neutralizing these threats. These capabilities are available to senior policy-makers, not only in DOE but also in DOD, the Intelligence Community, and national and local law enforcement agencies. Under the International Technology Program, LANL provides technical support in the development of innovative options for mitigating new security threats, including those associated with the worldwide proliferation of advanced conventional and cyber weapons. LANL provides:

- Advanced computational and analysis capabilities that enable rapid assessment of options for responding to evolving threats, including the capability to model the consequences of those response actions. Advanced computing is defined at the teraflop performance level.
- A range of credible, high-confidence methods for locating, characterizing, and disabling nuclear, biological, and chemical weapons, including those of unknown design.
- Technologies that battlefield commanders, military special forces teams, and law enforcement agencies can use in place of lethal force.
- Real-time access to Laboratory resources and capabilities to support on-site reaction teams.
- Creative technical solutions to "intractable" national security problems using the full range of expertise and competencies that exists at the Laboratory.
- Access to appropriate Laboratory technical capabilities to counter criminal activities and terrorism.

This page intentionally left blank.

**Oak Ridge National Laboratory
(ORNL)**

Organization: Oak Ridge National Laboratory (ORNL)

Senior Information Operations Official:

George A. Dailey, 423-574-9543, gad@ornl.gov

Information Operations Points of Contact:

George A. Dailey, 423-574-9543, gad@ornl.gov

Senior Information Assurance Official:

George A. Dailey, 423-574-9543, gad@ornl.gov

Information Assurance Points of Contact:

Sharon Jacobsen, Deputy Director, Data Systems Research and Development Program,
423-574-0900, sej@ornl.gov

Senior Critical Infrastructure Protection Official:

George A. Dailey, 423-574-9543, gad@ornl.gov

Critical Infrastructure Protection Points of Contact:

George A. Dailey, 423-574-9543, gad@ornl.gov

On-Line Resources:

LMES Homepage: <http://www.ornl.gov/y12>

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. Since that time, CIST has grown to an organization of multi-agency sponsorship. It provides support at the national level for a variety of federal agencies, as well as for the Department of Energy (DOE) and Lockheed Martin Energy Systems, Inc. (LMES). 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 sector as well as the unclassified sensitive sector.

A combined staff of information security professionals with a host of state-of-the-art technology resources focus on the protection of classified and unclassified systems for processing information up to and including Top Secret. The experience gained from a

variety of information management applications that include major accounting and financial transactions, command and control, law enforcement, medical, nuclear material tracking and many other diverse areas of government concern is available to all CIST activities. Established security expertise includes, access control and authentication, contingency planning, electronic signature, risk assessment, communications, system development, security reviews, security testing, standards, procedures, encryption, security training development and review. Some activities in support of the Department of Energy (DOE) include: 1) Baseline Skills Evaluation and Certification; 2) Multilevel Secure (MLS) Network Design; 3) Specifications for a Multilevel Secure (MLS) Document Management Center; and 4) Technology Assessment of the Security Aspects of Database Management Systems. Other federal agency projects, such as the Department of Defense Marine Forces Pacific Defense Information Infrastructure (DII) Sensitive Local Area Network (LAN) Integration, U.S. Coast Guard Vulnerability Analysis, National Institute of Standards and Technology (NIST) Key Escrow, and providing technical support to the Department of State for various domestic and international initiatives throughout the world are just a few examples of past and present projects supported by CIST.

CIST is unique in its wide range of technical talent and facilities which offer a high degree of physical security. It serves as the single DOE testbed for testing and installation of the National Security Agency (NSA) security products and as the developer and instructor for DOE wide information security training and certification by conducting courses through the DOE Central Training Academy as adjunct instructors. In an advisory role, technical assistance in information assurance policies and strategies are provided to numerous agencies including DOE, DOD, NIST, and a variety of national and international working groups, such as the President's Commission on Information Infrastructure Protection (PCCIP), Communications and Information Assurance and Banking and Financial Information Surety. This experience and technical expertise is demonstrated through previous and current project activities, as well as appropriate analytical tools in a single, secure location which are utilized to provide accurate comprehensive evaluations and analyses in an expedient, cost-effective, and unbiased manner. Areas of expertise include: in-depth knowledge of various hardware, software, and telecommunications systems, testing methodologies and equipment, formal independent verification and validation techniques, product functional and penetration testing techniques, security monitoring techniques, and risk assessments methodologies. The Center for Information Security (CIST) has extensive knowledge and understanding of national computer security criteria, and the ability to interpret that criteria and apply it to specific hardware/software platforms that are used by or will be used by government agencies.

Activities:

For activities, contact the Point of Contact or visit the on-line resource.

This page intentionally left blank.

**Pacific Northwest National
Laboratory
(PNNL)**

Organization: Pacific Northwest National Laboratory (PNNL)

Senior Information Operations Official:

Michael Kluse, Associate Laboratory Director, National Security Division, 509-376-0299

Information Operations Points of Contact:

D.R. Miles, Staff Scientist and Executive Advisor to the Department of Energy, Office of Safeguards and Security for Information Assurance, 509-372-4515, dr.miles@pnl.gov

Senior Information Assurance Official:

Michael Kluse, Associate Laboratory Director, National Security Division, 509-376-0299

Information Assurance Points of Contact:

D.R. Miles, Staff Scientist and Executive Advisor to the Department of Energy, Office of Safeguards and Security for Information Assurance, 509-372-4515, dr.miles@pnl.gov

Senior Critical Infrastructure Protection Official:

Michael Kluse, Associate Laboratory Director, National Security Division, 509-376-0299

Critical Infrastructure Protection Points of Contact:

D.R. Miles, Staff Scientist and Executive Advisor to the Department of Energy, Office of Safeguards and Security for Information Assurance, 509-372-4515, dr.miles@pnl.gov

On-Line Resources:

PNNL Homepage: <http://www.pnl.gov>

DOE IAOP Homepage: <http://w3.pnl.gov:2080/iaop>

Missions and Functions:

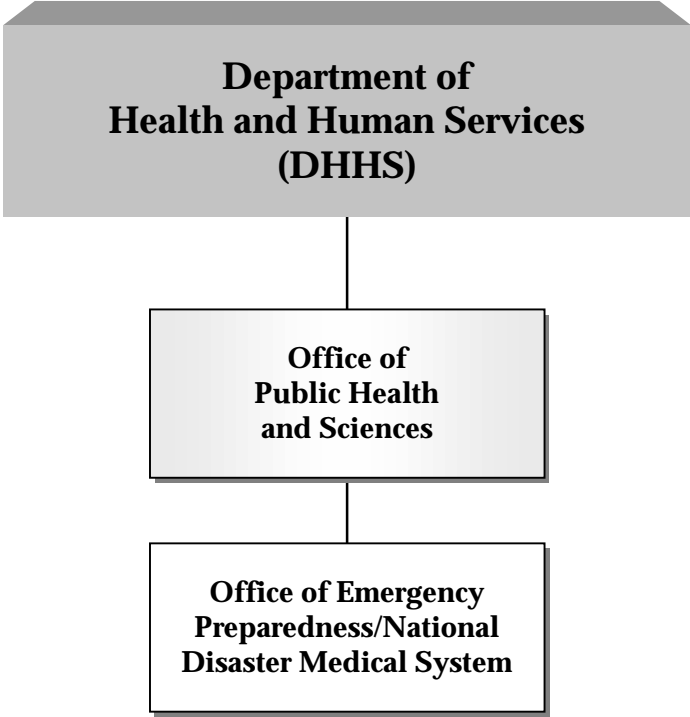
The Department of Energy's (DOE's) Office of Safeguards and Security (NN-50) established the Information Assurance Outreach Program (IAOP) to provide the nation's energy industries with access to skills and expertise developed for the protection of information assets. This effort is consistent with the findings and recommendations of the President's Commission on Critical Infrastructure Protection and assists DOE with the discharge of its responsibilities mandated by Presidential Decision Directive 63. D.R. Miles at the Pacific Northwest National Laboratory (PNNL) serves as the Information Assurance Outreach Program's Executive Agent.

The IAOP has an ongoing effort to develop cooperative agreements with organizations active in the electric industry as well as other elements of the Federal sector that have Information Assurance (IA) responsibilities. In the first year, the IAOP has conducted or has pending IA Assessments for a number of organizations responsible for providing electric power. Additionally, various assistance include providing technical assistance with establishing programs to enhance information assurance, providing specialized training, and monitoring the performance of DOE developed IA tools provided to these organizations. The IAOP is working cooperatively with the private and public sector to enhance information assurance in all dimensions.

Activities:

- The DOE IAOP performs Information Assurance Assessments of the nation's critical infrastructures to identify vulnerabilities and weaknesses. The IAOP is also engaged in raising public awareness regarding cyber threats and vulnerabilities in order to address the "cyber threat" to the national information infrastructure and the competitiveness of corporate America. The DOE IAOP also supports forums to discuss measures to protect the nation's electric, gas and oil, and telecommunications.

This page intentionally left blank.



Organization: Department of Health and Human Services (DHHS)

Information Assurance Points of Contact:

Bob Gignilliat, Senior Information Systems Security Officer, 202-690-7228,
rgignill@os.dhhs.gov

Critical Infrastructure Protection Points of Contact:

Bob Gignilliat, Senior Information Systems Security Officer, 202-690-7228,
rgignill@os.dhhs.gov

On-Line Resources:

DHHS Homepage: <http://www.hhs.gov>

Missions and Functions:

- Presidential Decision Directives (PDD) #62 and #63 mandate DHHS to participate in a federal response program specifically aimed at preparing for and responding to terrorist incidents. Specifically, PDD-63 appoints DHHS as the lead agency for sector liaison for protection of the health services infrastructure. This includes public health services and prevention, surveillance, laboratory services and personal health services.
- The U.S. Department of Health and Human Services, Office of Emergency Preparedness, (HHS/OEP) coordinates the Department's efforts to provide assistance to supplement State and Local resources in response to public health and medical care needs following a disaster or event. This could include natural disasters, technological disasters or acts of terrorism.
- The U.S. Department of Health and Human Services is the primary agency under Emergency Support Function #8 of the Federal Response Plan to coordinate the Federal health and medical services to areas affected by disasters.

Activities:

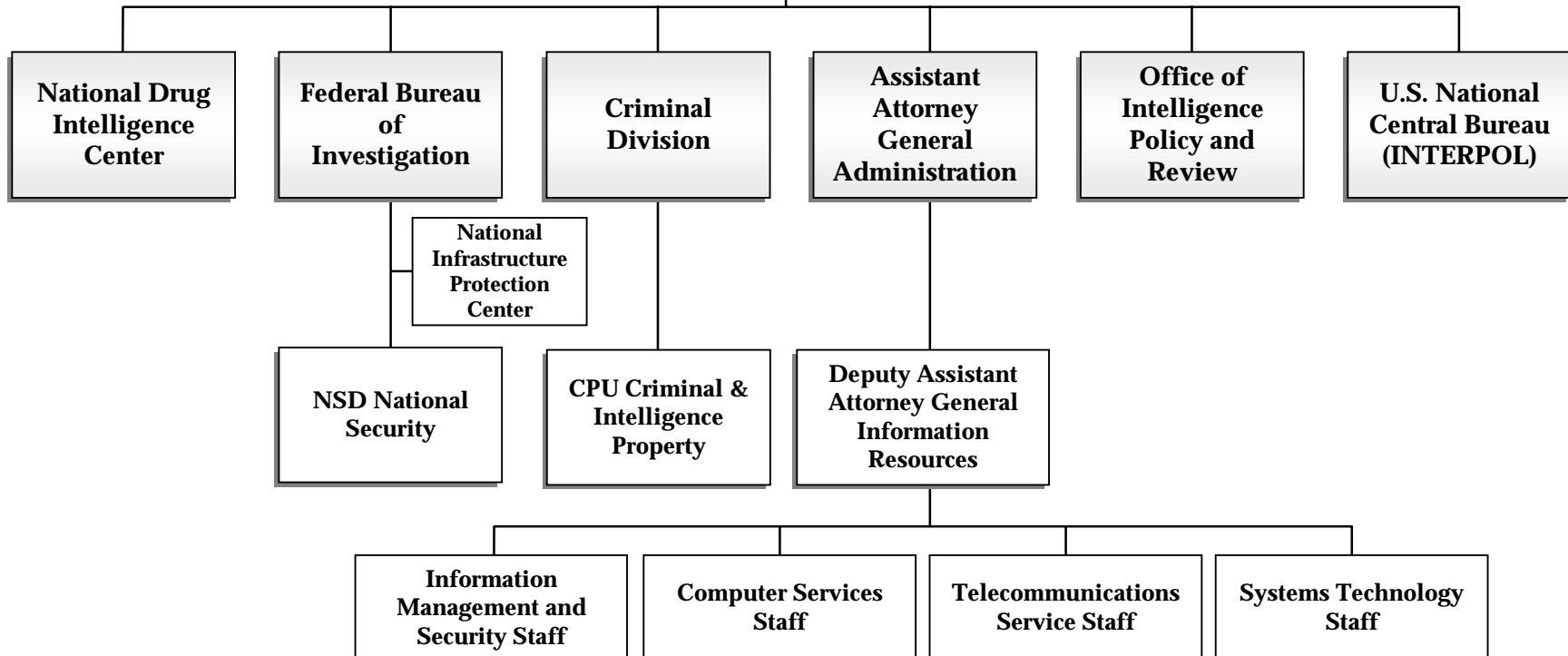
- The National Disaster Medical System (NDMS) is a Federally coordinated system that augments the Nation's emergency medical response capability. The overall purpose of the NDMS is to establish a single integrated National medical response capability for assisting State and local authorities in dealing with the medical and health effects of major peacetime disasters and providing support to the military and Veterans Health Administration medical systems in caring for casualties evacuated back to the U.S. from overseas armed conflicts.

- The HHS National Strategic Counterterrorism Plan is:
 - Create local resources - rapid response time required [27 - MMST's]
 - Develop Partnerships to:
 - » Improve local health and medical system capability to respond effectively
 - » Improve Federal health and medical capability to rapidly augment State/Local response - enhance response plans with FBI & FEMA
 - Develop 3 National NBC response teams [NMRT]
 - Enhance national surveillance system, laboratory support, and technical assistance
 - Identify critical research and development needs
 - Enhance communications infrastructure.

This page intentionally left blank.

**Department of Justice
(DoJ)**

Attorney General



Organization: Department of Justice (DoJ)

Senior Information Assurance Official:

Stephen R. Colgate, Assistant Attorney General for Administration, 202-514-3101

Information Assurance Points of Contact:

Linda Burek, Acting Deputy Assistant Attorney General for Information Resources Management (IRM), 202-514-0507

Mary Ellen Condon, Director, Information Management Security Staff (IMSS), IRM, 202-514-4292

Scott Charney, Chief, Computer Crime and Intellectual Property Section, Criminal Division, 202-514-1026

Robert Bryant, Assistant Director, National Security Division, FBI

Neil J. Gallagher, Deputy Assistant Director, Criminal Investigative Division, FBI

Senior Critical Infrastructure Protection Official:

Stephen R. Colgate, Assistant Attorney General for Administration, 202-514-3101

Critical Infrastructure Protection Points of Contact:

Mary Ellen Condon, Director, Information Management Security Staff (IMSS), IRM, 202-514-4292

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/comperim.htm>

Drug Enforcement Agency: <http://www.usdoj.gov/dea/deahome.htm>

Missions and Functions:

- The Department of Justice serves as counsel for 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 their 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 is 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 also 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.

Activities:

- The Department has formed a Computer Security Officers Task Force consisting of the representatives with computer security responsibility from each of the Department's 34 components. Each component Computer Systems Program Manager is responsible for overseeing the activities of Computer Systems Security Officers designated for each

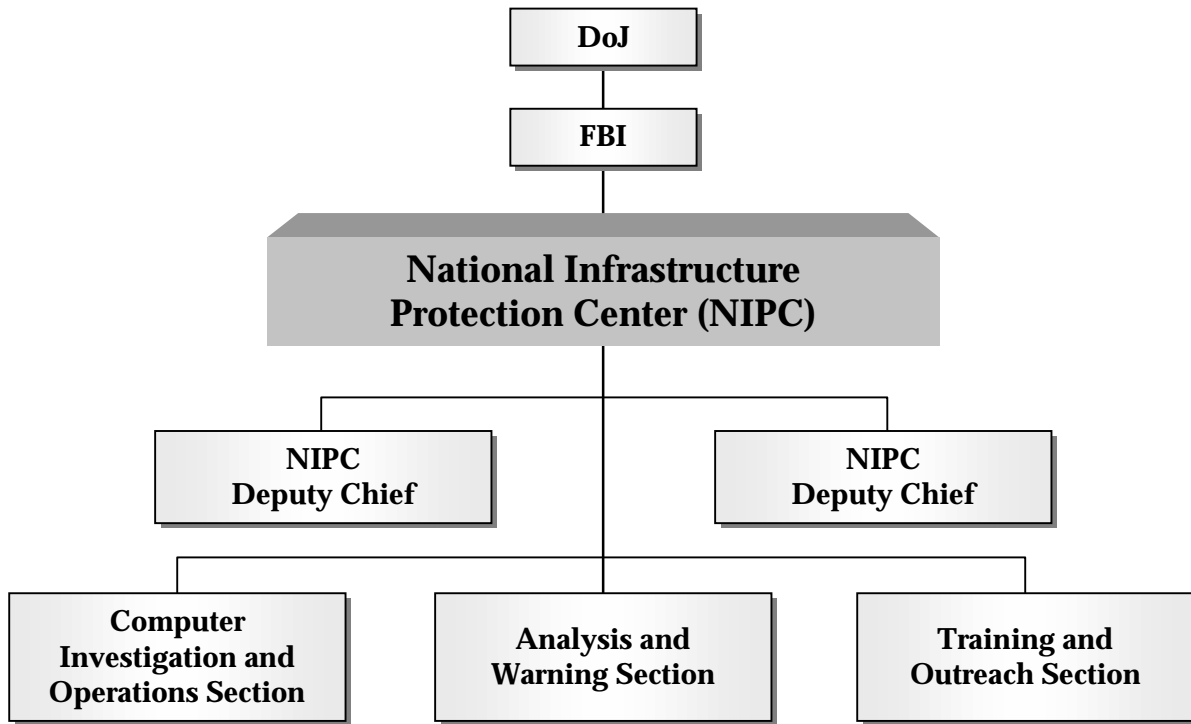
system. These systems security officers are full-time or part-time security specialists, depending on the size and sensitivity of the system and its information.

- 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.
- 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.
- 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 that 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 were 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.

This page intentionally left blank.



Organization: National Infrastructure Protection Center (NIPC)

Senior Critical Infrastructure Protection Official:

Miek Vatis, Chief, NPC, 202-324-0308

Critical Infrastructure Protection Points of Contact:

Ron Dick, TAOS, 202-324-6302

Hal Hendershoti, CIOS, 202-324-6303

Gary Kosciusko, AWS, 202-324-0340

Paula Wendell, TAOS, 202-324-6303

Missions and Functions:

The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and “cyber,” that threaten or target our critical infrastructures.

The NIPC’s job is not simply to investigate and respond to attack after they occur, but to learn about them beforehand and prevent them.

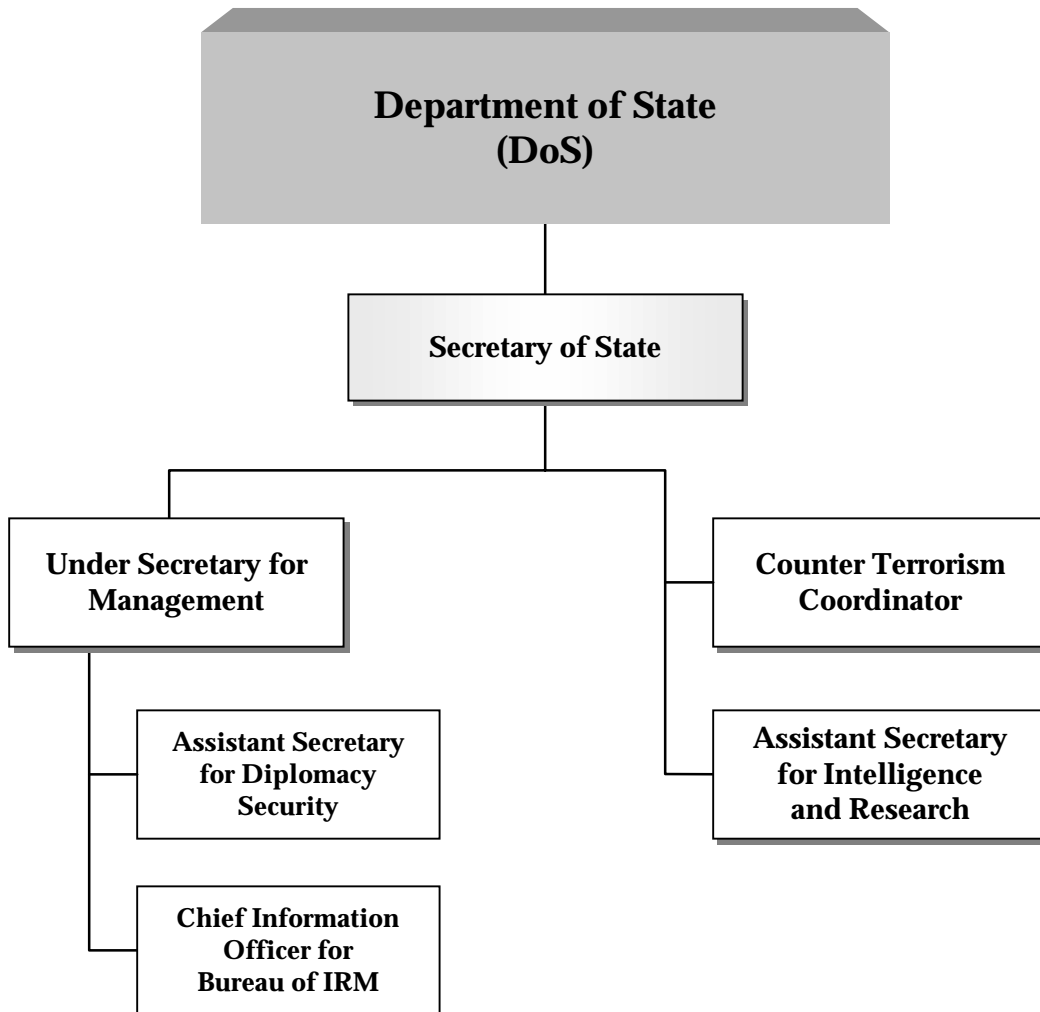
- *Training, Administration, and Outreach Section (TAOS)*. The Training, Administration, and Outreach Section (TAOS) coordinates the training and continuing education of cyber investigators in the FBI Field Offices, in other federal agencies, and in state and local law enforcement; and of personnel in the public and private sector involved in infrastructure protection. It also will direct our extensive outreach efforts to FBI Field Offices, other government agencies, industry, and academia, which are necessary to encourage the sharing of information about foreign and domestic threats, vulnerabilities, and technological developments. In addition, the TAOS provides the administrative support that underlies and is necessary to all of the other activities of the Center.
- *Analysis and Warning Section (AWS)*. The Analysis and Warning Section (AWS) provides comprehensive assessments and analyses of foreign and domestic threats, exploited vulnerabilities, and exploitation techniques concerning physical and cyber risks to the critical infrastructures of the United States. The AWS provides direct analytical support for computer investigations, and serves as the information clearinghouse for research and analysis and unlawful acts on the nation’s infrastructures. It is charged with obtaining relevant real time information from all sources – law enforcement investigations, intelligence sources, open sources, and voluntarily provided industry data – analyzing it, and disseminating its analyses to relevant consumers in the government and private sectors. The AWS is the hub for public-private sector information sharing and analytical work. It also provides a Watch –and-Warning function to help alert other government agencies and private sector companies to impending or ongoing attacks.

- *Computer Investigations and Operations Section (CIOS)*. The Computer Investigations and Operations Section (CIOS) is responsible for coordinating and supporting computer intrusion investigations conducted by the 56 FBI Field Offices, providing and coordinating technological support to investigations involving computers and information technologies, and for managing a Cyber Emergency Support Team, which will help respond to a cyber attack on critical infrastructures. In addition, CIOS provides coordinates the provisions of investigative and technological support to cyber investigators from other federal, state or local government agencies.

Activities:

- Started the InfraGard program to establish a mechanism for two-way information sharing about intrusion incidents and system vulnerabilities and provides channel for the NIPC to disseminate analytical threat products to the private sector. The program has the following objectives:
 - Provide members a forum for education and training on infrastructure vulnerabilities and protection measures
 - Provide members prompt, value-added threat advisories, alerts and warning
 - Ensure the protection of computer intrusion/threat data shared among InfraGard members, FBI field offices, and the NIPC through compliance with proprietary, legal, and security requirements
 - Increase the quantity and quality of infrastructure intrusion/threat reports provided to local FBI field offices and the NIPC
 - Increase interaction and information sharing among IntraGard members, their associated local field offices and the NIPC on infrastructure threats, vulnerabilities, and interdependencies.
- The program provides four capabilities: (1) members participate in local chapter activities; (2) have access to an Alert Network to voluntarily report actual or attempted illegal intrusions, disruptions and vulnerabilities of information systems; (3) can access a secure InfraGard Website with recent information about infrastructure protection; and (4) can call the Help Desk at NIPC to ask questions about the program.
- Publishes Cyber Notes every two weeks. The purpose is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

This page intentionally left blank.



Organization: Department of State (DoS)

Senior Information Operations Official:

David G. Carpenter, Assistant Secretary for Diplomatic Security, 202-647-6290

Information Assurance Points of Contact:

Fernando Burbano, Chief Information Officer, 202-647-2226

On-Line Resources:

DoS Homepage: <http://www.state.gov>

Missions and Functions:

The Department of State advises the President in the formulation and execution of foreign policy. The Department of State's primary objective in the conduct of foreign relations is to promote the long-range security and well being of the United States. The Department determines and analyzes the facts relating to American overseas interests, makes recommendations on policy and future action, and takes the necessary steps to carry out established policy. In so doing, the Department engages in continuous consultations with the American public, the Congress, other U.S. departments and agencies, and foreign governments; negotiates treaties and agreements with foreign nations; speaks for the United States in the United Nations and in more than 50 major international organizations in which the United States participates; and represents the United States at more than 800 international conferences annually.

The Secretary of State is the principal foreign policy adviser to the President, is responsible for the overall direction, coordination, and supervision of U.S. foreign relations and for the interdepartmental activities of the U.S. Government abroad. The Secretary is the first-ranking member of the Cabinet, is a member of the National Security Council, and is in charge of the operations of the Department, including the Foreign Service. The Office of the Secretary includes the offices of the Deputy Secretary, Under Secretaries, Assistant Secretaries, Counselor, Legal Adviser, and Inspector General.

The Bureau of Diplomatic Security, established under the Omnibus Diplomatic Security and Antiterrorism Act of 1986, as amended (22 U.S.C. 4803 et seq.), provides a secure environment for conducting American diplomacy and promoting American interests worldwide. Overseas, the Bureau develops and maintains effective security programs for every U.S. Embassy and consulate abroad; protects U.S. diplomatic personnel and missions from physical and electronic attack as well as technical espionage; and advises U.S. Ambassadors on all security matters.

In the United States, the Bureau investigates passport and visa fraud, conducts personnel security investigations, and issues security clearances. It protects the Secretary of State, the

U.S. Ambassador to the United Nations, and many cabinet-level foreign dignitaries and other foreign officials who visit the United States. The Bureau also assists foreign embassies and consulates in the United States in the protection of their diplomats and facilities, and arranges for training in the United States for foreign civilian police who then return to their own countries better able to fight terrorism.

The Bureau of Intelligence and Research coordinates programs of intelligence, analysis, and research for the Department and produces current intelligence analyses essential to foreign policy determination and execution. Through its Office of Research, the Bureau maintains liaison with cultural and educational institutions and oversees contract research and organizes conferences on foreign affairs subjects of high interest to policymakers.

Diplomacy is an instrument of power, essential for maintaining effective international relationships. It is a principal means through which the United States defends its interests, responds to crises, and achieves its international goals. The Department of State is the lead institution for the conduct of American diplomacy, a mission based on the role of the Secretary of State as the President's principal foreign policy adviser.

To carry out U.S. foreign policy at home and abroad, the Department of State:

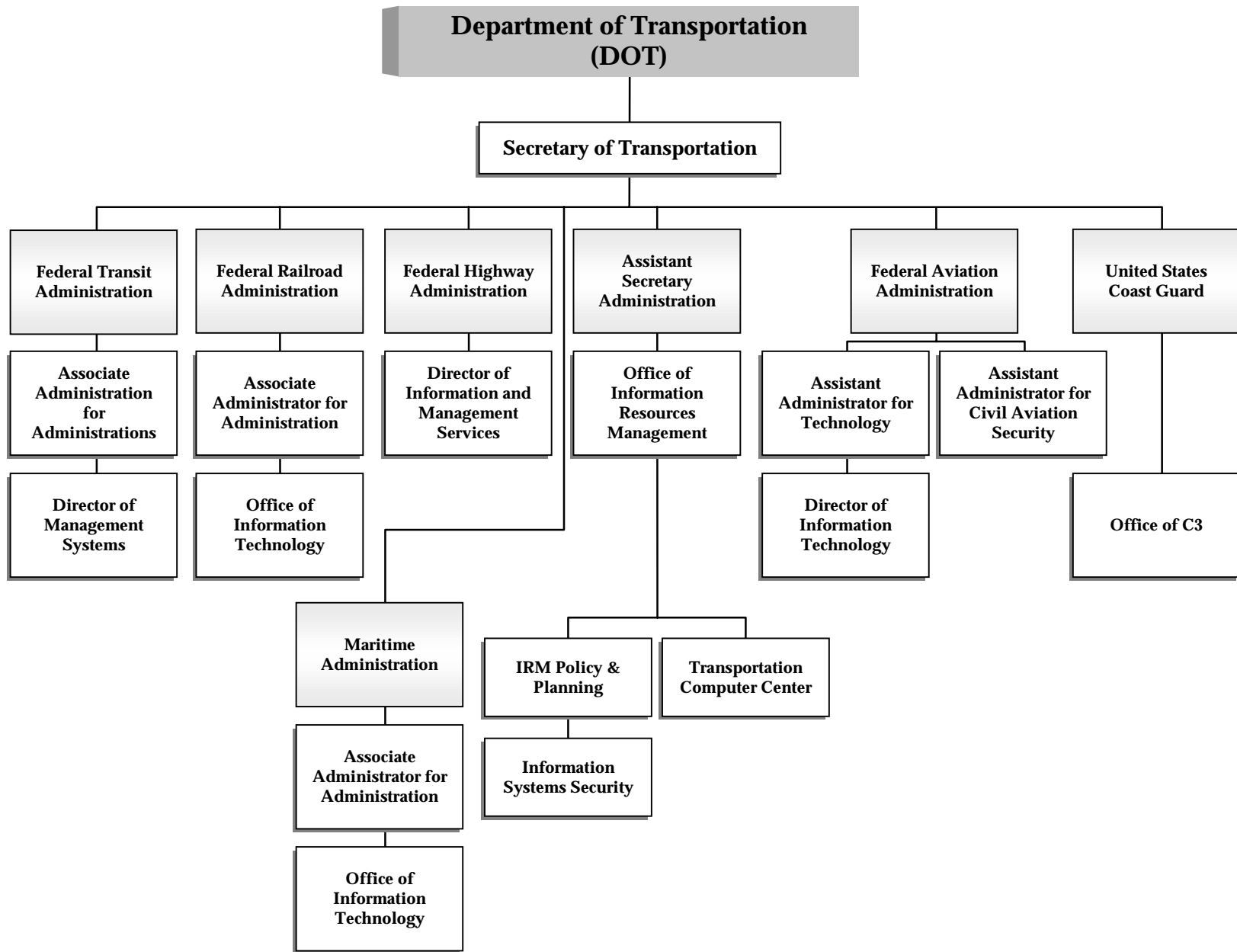
- Exercises policy leadership, broad interagency coordination, and management of resource allocation for the conduct of foreign relations.
- Leads representation of the United States overseas and advocates U.S. policies for foreign government and international organizations.
- Coordinates, and provides support for, the international activities of U.S. agencies, official visits, and other diplomatic missions.
- Conducts negotiations, concludes agreements, and supports U.S. participation in international negotiations of all types.
- Coordinates and manages the U.S. Government response to international crises of all types.
- Carries out public affairs and public diplomacy.
- Reports on and analyzes international issues of importance to the U.S. Government.
- Assists U.S. business.
- Protects and assists American citizens living or traveling abroad.
- Adjudicates immigrant and nonimmigrant visas to enhance U.S. border security.
- Manages those international affairs programs and operations for which the Department has statutory responsibility.
- Guarantees the Diplomatic Readiness of the U.S. Government.

The above mission statement guides Department employees in conducting foreign affairs programs and activities. Department employees are also guided by a set of values, as individuals and as an institution. The work of these individuals has an impact on U.S. citizens, both domestic and abroad. Expertise in languages, understanding of foreign cultures, and management of complex issues and programs gained through international experience are essential elements of this work. The Department exercises discipline in

implementing policy, regardless of personal preferences, and its personnel are willing and able to serve worldwide as needed. Divergent views are expressed when necessary to strengthen the formulation and execution of foreign policy. The conduct of foreign relations is viewed as a long-term career commitment, rather than just a job. The Department workforce, a blend of Civil and Foreign Service employees and Foreign Service Nationals overseas, reflects the diversity of the United States.

Activities:

- 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 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.



Organization: Department of Transportation (DOT)

Senior Information Assurance Official:

Kim Taylor, Acting Chief Information Officer, 202-493-0678

Information Assurance Points of Contact:

Dale Hamilton, Resource Management, 202-366-9715

Critical Infrastructure Protection Points of Contact:

Thomas Falvey, Associate Director, 202-366-2716

On-Line Resources:

DOT Homepage: <http://www.dot.gov>

FAA: <http://www.faa.gov>

FAA Technical Center: <http://www.tc.faa.gov>

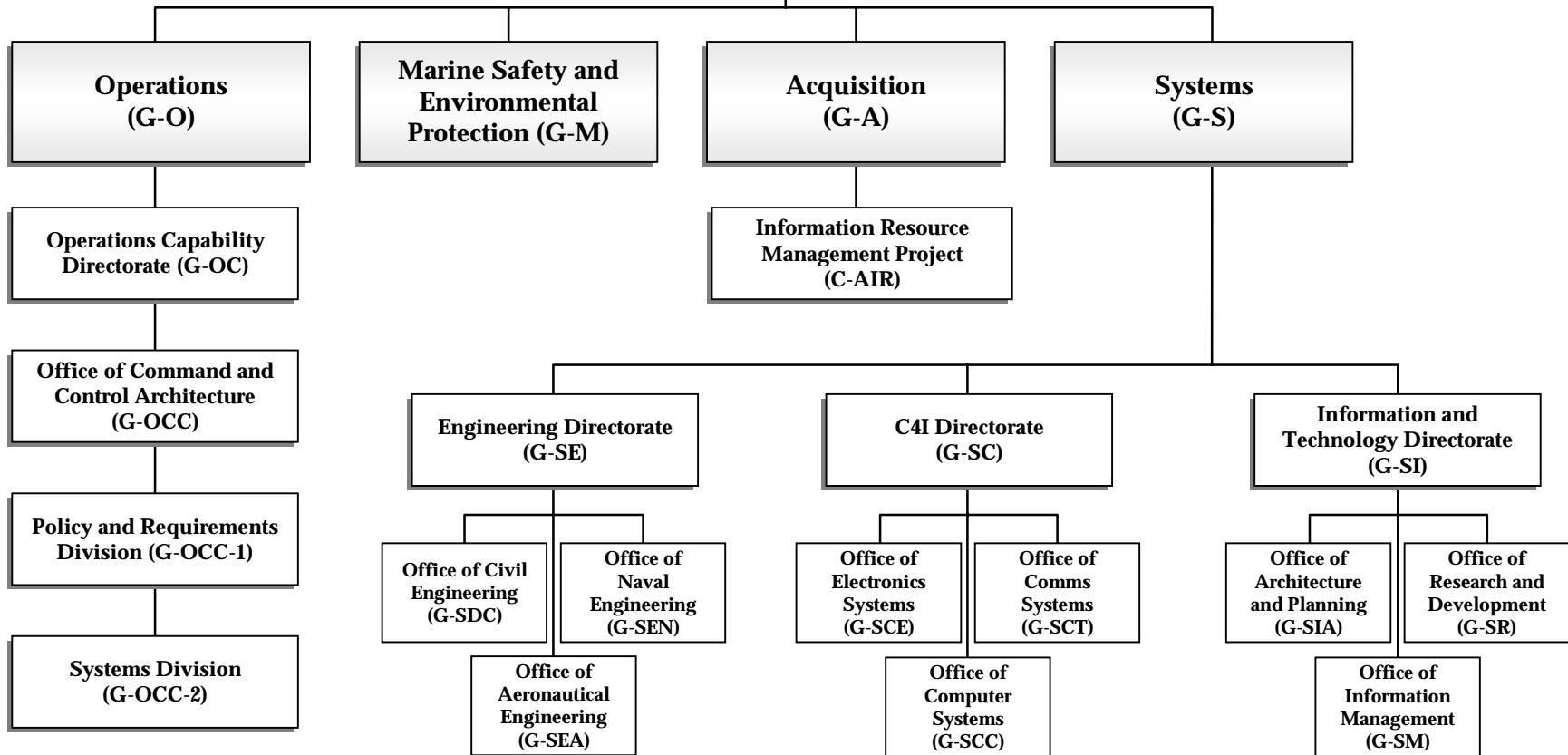
Missions and Functions:

The Office of Information Resource Management formulates, prescribes, and assures compliance with telecommunications and automated data processing policy to include information systems security policy.

Activities:

- Critical Infrastructure Assurance Officer is the assistant Secretary for Administration.
- Chief Information Officer is Kim Taylor.
- In January 1998, DOT produced a 5-year Information Technology plan. It describes the direction of information technology in DOT for Office of the Secretary of Transportation and each Operating Administration. The plan concentrates on five areas: (1) productivity enhancement, (2) customer communications, (3) Information Infrastructure, (4) Information Technology Security, and (5) Year 2000 and Innovations and Partnerships.
- Security of the DOT Information Systems rests with the Transportation Administrative Service Center.
- Identified the major information systems with DOT and based on PDD 63 requirement, will determine which ones are critical. The identification of critical systems also has to do with assisting in resolving the Year 2000 issue. Prioritizing systems for Y2K review assists both projects.
- Year 2000 responsibility is with each Operating Administration. A web site has been established for each OA to share information, disseminate government wide policies and provide links to other useful sites.

**United States Coast Guard
(USCG)**



Organization: United States Coast Guard (USCG)

Senior Information Operations Official:

RADM George Naccara, Director, Information and Technology Directorate (G-SI)

Information Operations Points of Contact:

Brian King, Chief Architecture and Planning, 202-267-1370

Senior Information Assurance Official:

RADM George Naccara, Director, Information and Technology Directorate (G-SI)

Information Assurance Points of Contact:

Capt Fred Squires, C4 Directorate, Systems, 202-267-2860

Capt Bill Bannister, Office of Command and Control Architecture, Operations, 202-267-6956

CDR Joe Rodriguez, Office of Command and Control Architecture, Operations,
202-267-1446

Capt Rick Hartman, Office of Communications Systems, C4 Directorate, Systems,
202-267-6856

CDR Kurt Guth, Office of Communications Systems, C4 Directorate, Systems, 202-267-1269

Senior Critical Infrastructure Protection Official:

RADM George Naccara, Director, Information and Technology Directorate (G-SI)

Critical Infrastructure Protection Points of Contact:

Harris McGarrah, Office of Information Management, 202-267-1324

On-Line Resources:

USCG Homepage: <http://www.uscg.mil>

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. When declared by Congress, 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.

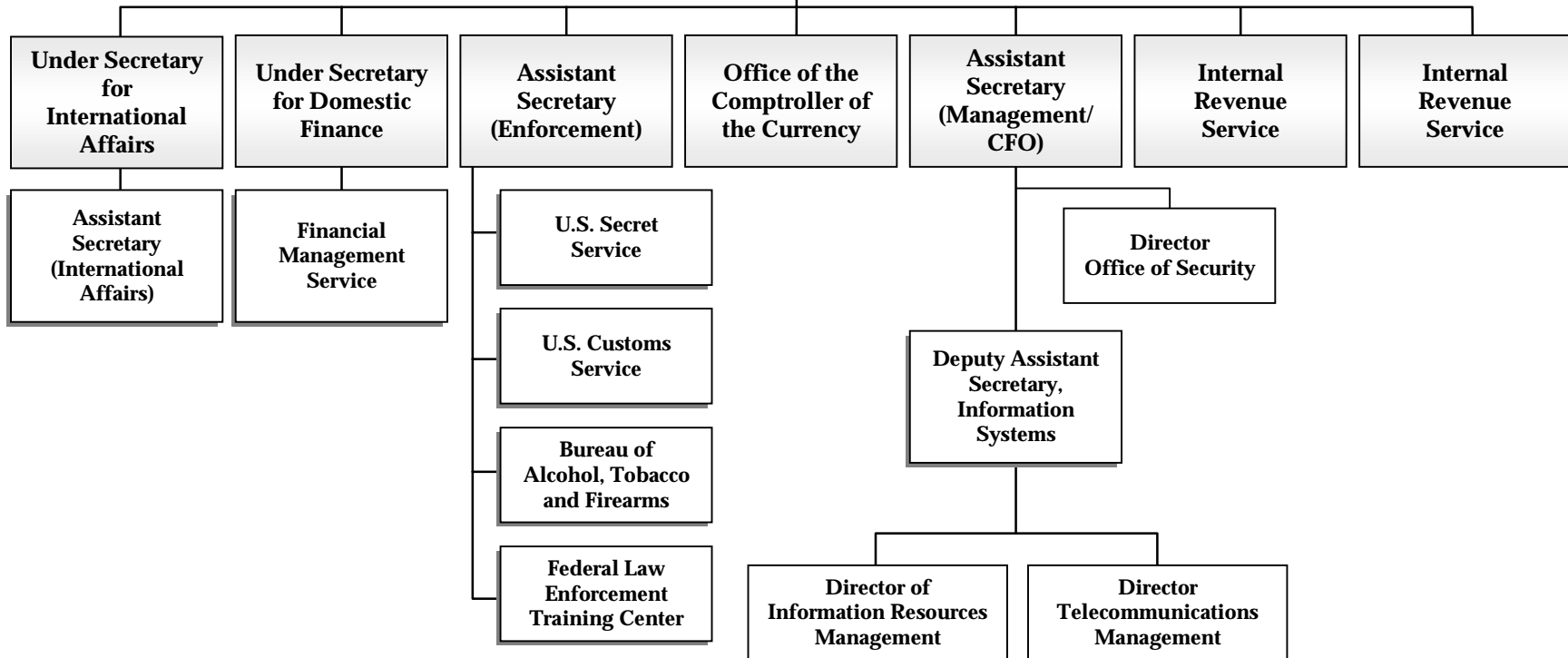
Activities:

- With respect to IW, the biggest issue for the Coast Guard is interoperability. Standard operations for the Coast Guard 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 interest but not in the same sense as DOD. The Coast Guard has not 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 are not as identifiable with DOD.
- Another key issue which distinguished 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
(Treas)**

Secretary of the Treasury



Organization: Department of the Treasury (Treas)

Senior Information Operations Official:

James Flyzik, CIO, 202-622-1200
Tom Wiesner, Director CSM, 202-622-1592

Information Operations Points of Contact:

Edd Barnes, 202-622-6501, edd.barnes@cio.treas.gov

Senior Information Assurance Official:

James Flyzik, 202-622-1200

Information Assurance Points of Contact:

Michelle Moldenhauer, Director, Office of Information Systems Security, Office of Deputy
Assistant Secretary for Information Systems/CIO, 202-622-1110
James Flyzik, Deputy Assistant Secretary for Information Systems, 622-1200
J. Sullivan, Director, Office of IT Policy and Management, 622-1599
T. Wiesner, Director, Office of Telecommunications Management, 622-1592

Senior Critical Infrastructure Protection Official:

Ted Carter 202-622-2400

Critical Infrastructure Protection Points of Contact:

IT Issues; Jim Flyzik 202-622-1200;
IT Issues; Don Hagerling; 202-622-2780

On-Line Resources:

DoTreas Homepage: <http://www.ustreas.gov>

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.

Activities:

- 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.
- The Department, with input from departmental security experts, writes very broad policy for internal implementation. Baseline policy requirements, standards, and procedures are included in the Department's security manual.
- The Department maintains an extensive communications and data network, the Treasury Communications System, which relies 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.
- 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 Information Technology Security Policy Forum coordinates information security issues. 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 and the Financial Management Service participate in developing banking standards.
- Wireless architecture and security issues are being addressed by the newly created wireless organization of the Department in the CIO office.
- 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.



Independent Establishment

This page intentionally left blank.

**Central Intelligence Agency
(CIA)**

Organization: Central Intelligence Agency (CIA)

Senior Information Operations Official:

George J. Tenet, Director of Central Intelligence

Information Operations Points of Contact:

Chief, Critical Technologies Group, Office of Transnational Issues, 703-874-0394

Chief, Information Warfare Team, (CTG, OTI), 703-874-0405

Critical Infrastructure Protection Points of Contact:

DCI/CIO, 703-482-5213

On-Line Resources:

CIA Homepage: <http://www.odci.gov/cia/ciahome.html>

Missions and Functions:

Information Warfare Team provides foreign intelligence support to the US government on information warfare (IW).

The Office of Transnational Issues provides analysis on weapons, advanced critical technologies, economics, and societal conflicts that affect US national security. The Critical Technologies Group is tasked with identifying cutting-edge technologies (materials, lasers, stealth, information technologies) and their impact on military and civil programs. Our analysis is provided to the White House, Congress, and Cabinet-level departments.

Activities:

We have surveyed foreign IW threat information for selected state and non-state actors, and are studying the information more in-depth.

**Environmental Protection Agency
(EPA)**

**Office of
Solid Waste
and
Emergency Response**

Organization: Environmental Protection Agency (EPA)

Information Assurance Points of Contact:

Ken Stroech, 202-260-3434, stroech.ken@epamail.epa.gov

Critical Infrastructure Protection Points of Contact:

Ken Stroech, 202-260-3434, stroech.ken@epamail.epa.gov

On-Line Resources:

EPA Homepage: <http://www.epa.gov/swercepp/cntr-ter.html>

Missions and Functions:

- Under existing authorities, such as the National Oil and Hazardous Substances Pollution Contingency Plan (NCP), CERCLA and Clean Water Act, as amended; EPA is required to prepare for and respond to any release or threat of release of oil, hazardous substances, pollutants, or contaminants into the environment that may present an imminent and substantial threat to public health or welfare and the environment.
- Presidential Decision Directives (PDD) #39, #62, and #63 mandate EPA to participate in a federal response program specifically aimed at preparing for and responding to terrorist incidents. Specifically, PDD-63 appoints EPA as the lead agency for sector liaison for protection of the water supply infrastructure.
- In addition, EPA participates in the Domestic Preparedness Program, established under the Defense Against Weapons of Mass Destruction Act (Title XIV of Public Law 104-201), known as the Nunn-Lugar-Domenici Act.

Activities:

Program Development

CT Program development at EPA Headquarters (including the ERT and the NEIC) included:

- Producing a CT Program Strategy for EPA that includes a mission statement and both short- and long-term goals. EPA also identified key tasks to address these goals and developed a CT Workplan for FY98 that assigned each task to a participating EPA Office and point person.
- Establishing the Counter-Terrorism Program Coordination Team (CTPCT) to lead EPA in defining its CT Program and to serve as the primary focal point for the effective utilization of the Agency's assets and resources.
- Focusing on State Emergency Response Commissions (SERCs) and Local Emergency Planning Committees (LEPCs) in developing and providing guidance materials and other assistance to state and local planners/responders.

- Assessing the need for additional ERT and Regional chemical and biological equipment including developing Interim CT Equipment Guidance to the Regions outlining the types of equipment necessary for CT preparedness and response.

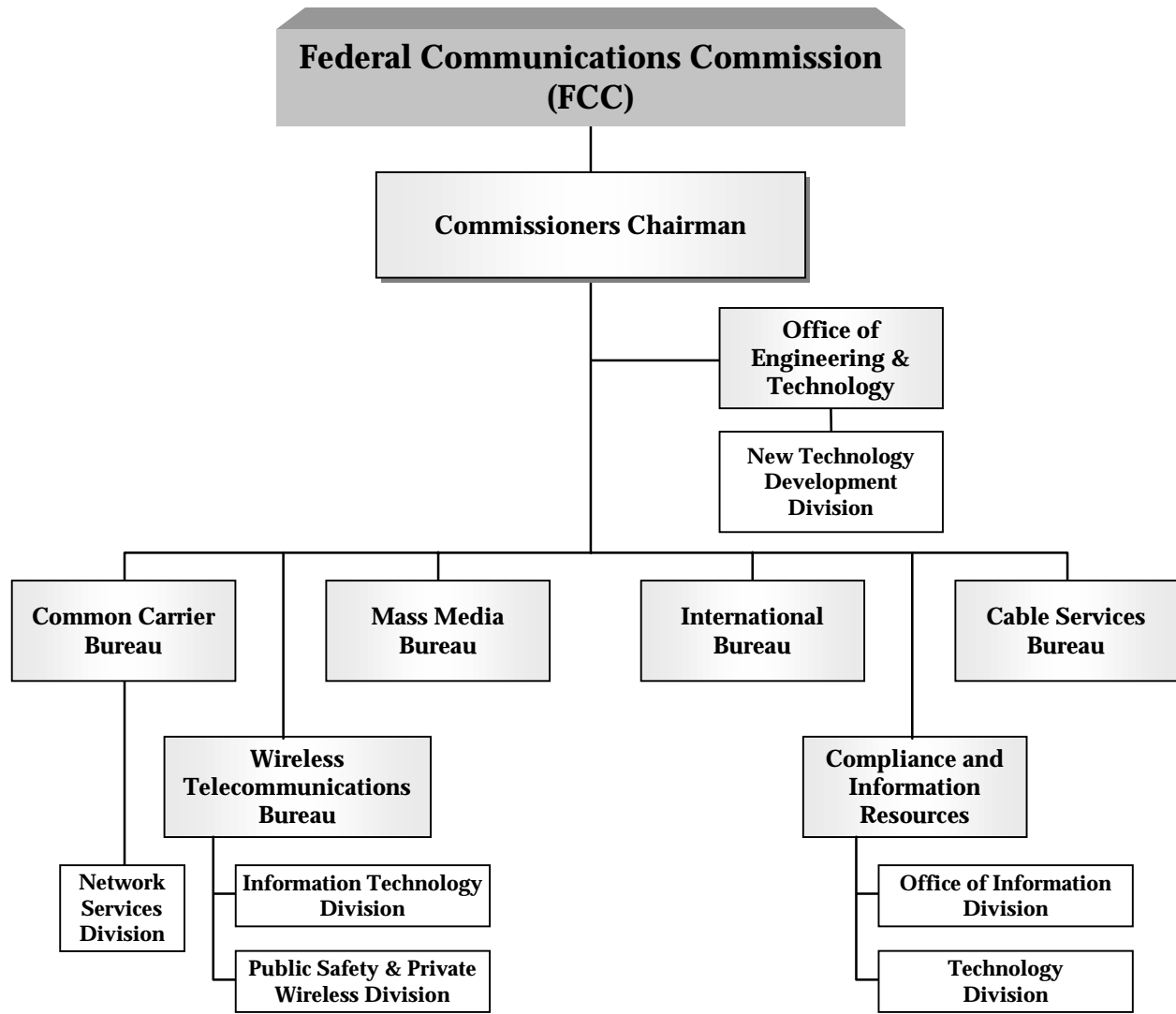
Interagency and Intra-Agency Coordination

- EPA participated in numerous interagency CT groups. The Agency's accomplishments include:
 - Concept of Operations Plan (CONPLAN): Developing, with the Federal Bureau of Investigation (FBI) and the Federal Emergency Management Agency (FEMA), a more detailed and refined CONPLAN to improve federal coordination with state and local sectors during the crisis and consequences management phases of a WMD response.
 - Bio Decon Plan: Developing the interim Bio Decon Plan to address the decontamination of areas affected by a release of a biological agent. The Bio Decon Plan emphasizes the National Response System/NCP approach, focusing on the decontamination of the environment.
 - Department of Justice's (DOJ) Five-Year Interdepartmental Counter-Terrorism and Technology Crime Plan: Developing the draft DOJ Five-Year Plan. EPA participated on three of the subgroups of the Core Agency Group responsible for the creation of a plan to serve as the baseline strategy for coordinating national policy and operational capabilities for combating terrorism in the U.S.
- EPA engaged in the following interagency coordination activities outside of formally established workgroups:
 - Provided an EPA Liaison to FBI Headquarters.
 - Worked with the U.S. Coast Guard (USCG) to address and define its role in terrorist incident response under Emergency Support Function (ESF) #10 of the FRP.
 - Responded to a request from the House Subcommittee on National Security, International Affairs and Criminal Justice to compile and submit information on the Agency's terrorism-related programs and activities for FY95 and FY99.
- Provided numerous briefings to both internal and external audiences to ensure that parties understood EPA's role and responsibilities under the NCP, FRP, and FRERP and the implications for CT activities.
- Developed a publicly accessible CT Website to disseminate information about EPA's roles and responsibilities in terrorist incident response.

Training and Education

EPA's participation in CT training and exercise was targeted to federal, state, and local responders. EPA developed its own training and exercises and also participated in exercises sponsored by other government entities. EPA's long-term goal is to fully incorporate CT technical training into the Agency's overall preparedness and response training program. EPA activities included:

- Continued to play a major role in developing Domestic Preparedness Program under Nunn-Lugar-Domenici (NLD). EPA assisted in redesigning the city visit process and participated in several of the initial visits, with a focus on transitioning more responsibility to the Regional offices.
- Participated, primarily through the ERT, in developing six training courses provided by the Chemical and Biological Defense Command (CBDCOM), now the Soldiers Biological and Chemical Command [SBCCOM]).
- Helped develop and participated in the following exercises: Keystone I and II, Exercise Gauged Strength, ITRAP VIII, and Phoenix '98.



Organization: Federal Communications Commission (FCC)

Senior Information Assurance Official:

Michael Powell, Defense Commissioner, 202-418-2200

Information Assurance Points of Contact:

Arlan Van Doorn, Deputy Chief, Compliance and Information Bureau, Representative to the NCS Committee of Principals, 202-418-1105

Roy Kolly, Compliance and Information Bureau, Representative to the NCS Council of Representatives, 202-418-1191

Herber Neumann, Common Carrier Bureau, Representative to the NCS National Coordinating Center for Telecommunications, 202-418-2341

On-Line Resources:

FCC Homepage: <http://www.fcc.gov>

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, lightguide 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, the Network Reliability Council, was chartered in 1992 to investigate reliability of the public switched network after the occurrence of several major service outages. The Council has been rechartered three times since-in 1994, 1996, and 1998. In 1996, the title was changed to the present Network Reliability and Interoperability Council (NRIC). An organizational summary of the NRIC can be found under Advisory Committees in this appendix. The Council is composed of CEO-level representatives of about 35 carriers, equipment manufacturers, state regulators, and large and small consumers. The telecommunications industry has used the NRIC as an effective vehicle for cooperation in improving network reliability and resiliency.

The report of the Council's study on network reliability performance 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 wither 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

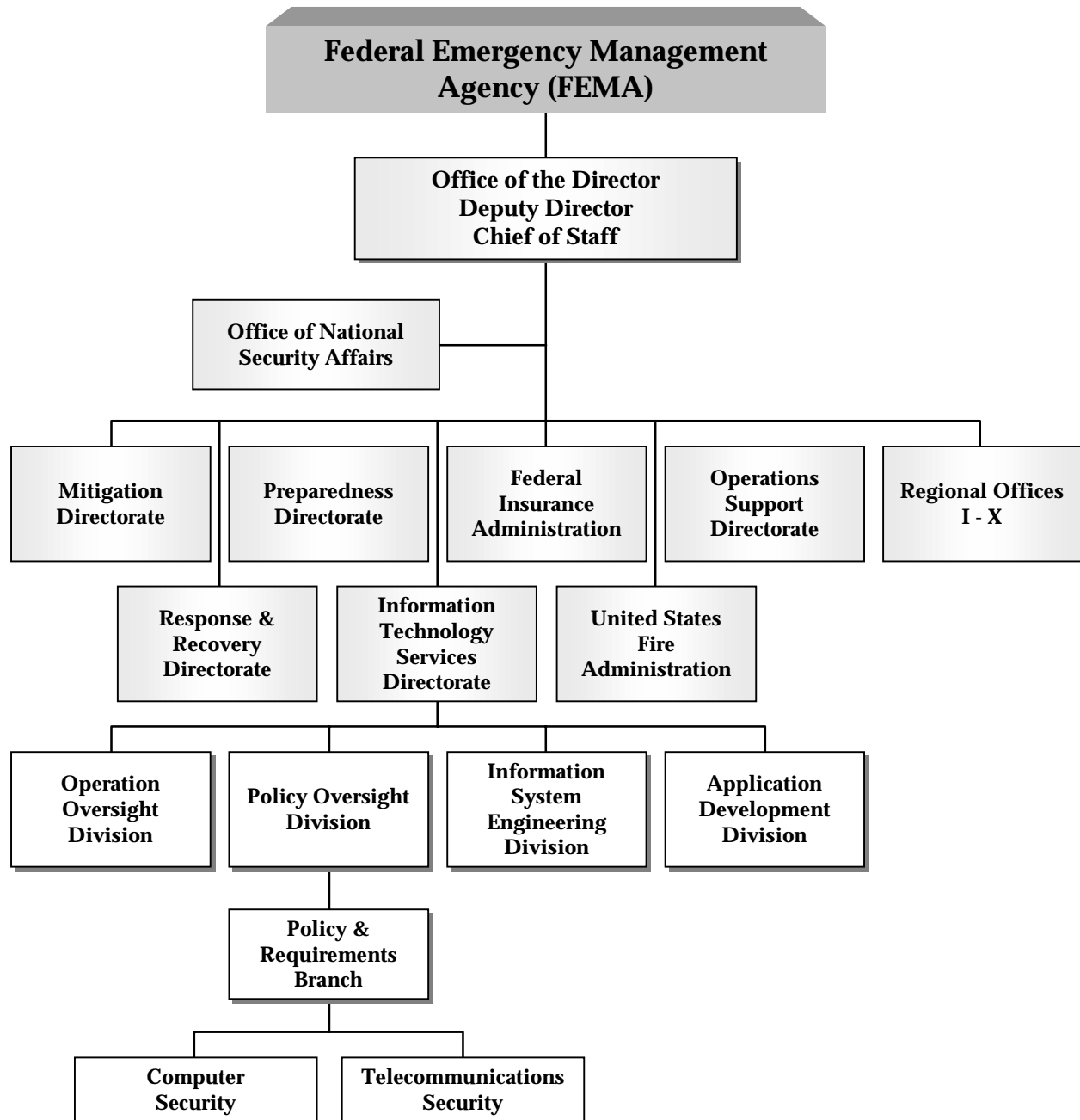
power plant, or an emergency 911 tandem switch. Outages involving nuclear power plants, government facilities and military facilities are reported through the NCS National Coordinating Center (NCC). The initial report is made to the DISA Network Management Operations Center which contacts NCC staff members. 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.

In 1996, the NRIC's charter was revised to include advising the FCC on how Section 256 of the Telecommunications Act-Coordination for Interconnectivity-should be implemented. 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. The purposes of Section 256 of the Telecommunications Act were to promote nondiscriminatory accessibility to telecommunications networks and to ensure the ability of users to "seamlessly and transparently transmit and receive information between and across telecommunications networks." Among its conclusions, the Third Council stated that the reliability of the nation's wireline telecommunications network remained the same as shown in earlier studies, the single greatest risk to those networks was damage to transmission facilities, while the most effective way of dealing with those risks was the enactment of effective one-call legislation.

The FCC, working with the National Weather Services and the Federal Emergency Management Agency, designed the Emergency Alert System (EAS), which replaced the Emergency Broadcast System (EBS) in January, 1997. The EBS was designed to provide the President with a means of addressing the American people in the event of national emergency giving him access to broadcast stations, cable systems and participating satellite programmers to transmit a message to the public. It has never been used for this purpose, but, since 1963, the system has been made available to transmit state and local emergency information. The EAS uses a digital system architecture to permit emergency information to be sent and received quickly and automatically and ensures redundancy by requiring at least two sources of emergency information. It is also designed to be less intrusive so that when emergency information is seen or heard it will be taken seriously rather than being dismissed as "only a test."

Activities:

- A 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.



Organization: Federal Emergency Management Agency (FEMA)

Senior Information Operations Official:

G. Clay Hollister, Executive Associate Director, Information Technology Services
Directorate (ITSD), 202-646-3006

Information Assurance Points of Contact:

Dennis B. Green, Chief, Policy and Requirements Branch, Policy Oversight Division, ITSD,
202-646-3470, dennis.green@fema.gov

Critical Infrastructure Points of Contact:

Dennis B. Green, Chief, Policy and Requirements Branch, Policy Oversight Division, ITSD,
202-646-3470

On-Line Resources:

FEMA Homepage: <http://www.fema.gov>

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 supports State and local emergency management programs by funding emergency planning, training emergency managers and local officials, conducting large-scale tests and sponsoring programs that teach the public how to prepare for disasters. 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.

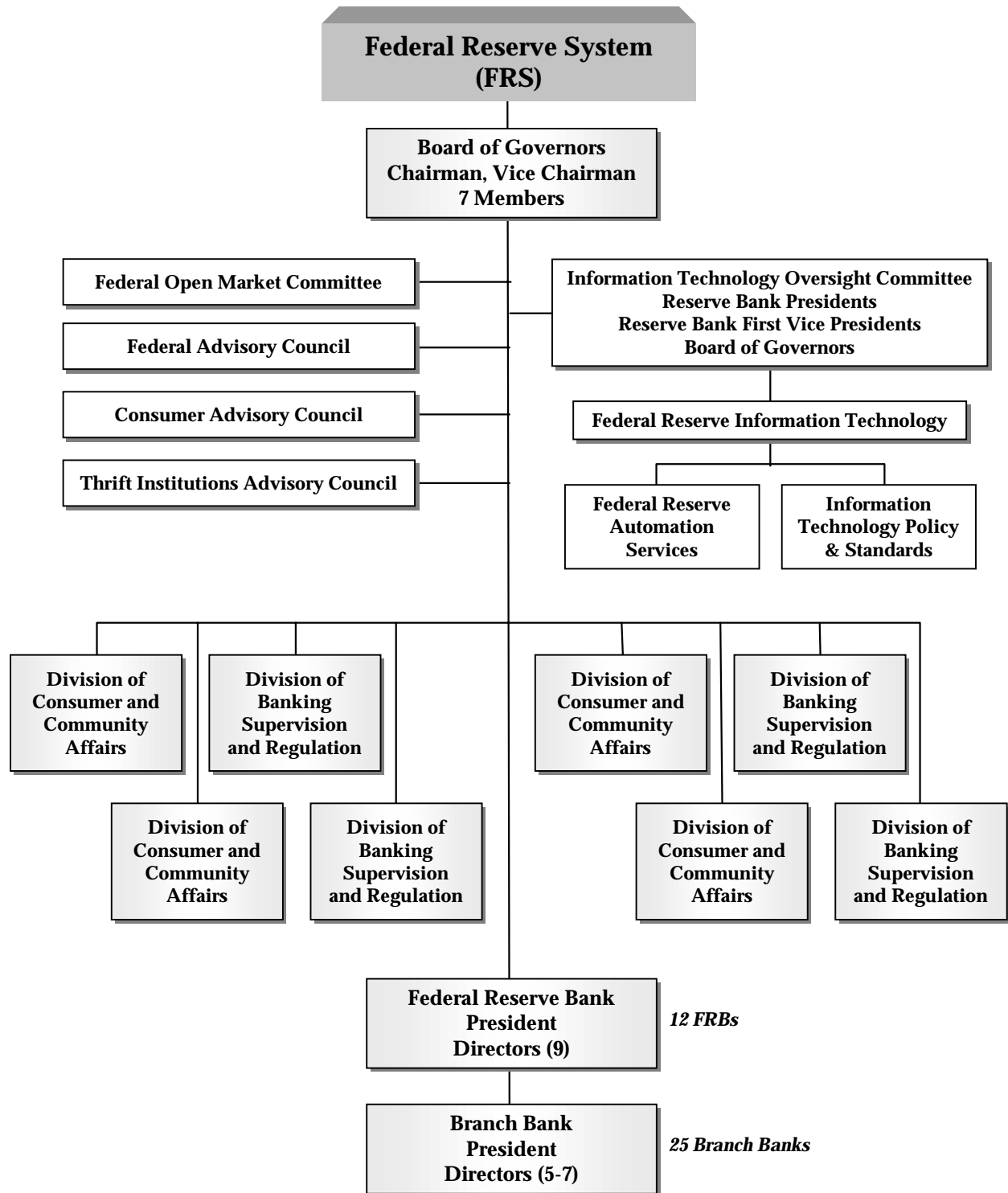
FEMA is an independent federal agency with more than 2,400 full-time employees: at FEMA headquarters in Washington, DC, at 10 regional offices, area offices in Puerto Rico and Hawaii, and at the National Emergency Training Center in Emmitsburg, MD and the Mt. Weather Emergency Assistance Center in Round Hill, VA. 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.

Activities:

- FEMA's Strategic Plan for FY 98-07 includes a number of information technology initiatives:

- Provide emergency alerts and emergency response communications nationwide or regionally by such means as the National Warning System (NAWAS), Emergency Alert System (EAS), and GIS
- Ensure continuity of government and a response capability required for national security emergencies
- Expedite disaster operations with enterprise-wide information and processing services provided through NEMIS
- Improve the timely, reliable, and cost-effective delivery of telecommunications and data infrastructure to any FEMA location by 20 percent.
- FEMA information security strategy focuses on protecting major applications systems that are, by definition, high risk because of the magnitude of harm that may result from the loss, misuse, or unauthorized access to or modifications of information in the applications. Managers are responsible for integrating security safeguards into every phase of each application's life cycle to protect the confidentiality, integrity, and availability of information resources in support of FEMA's mission.
- FEMA's disaster response functions rely on distributed and remote data processing, which introduces vulnerabilities through the communications links that connect these facilities. To reduce the possibility of data contamination, FEMA programs run on dedicated hardware. The FEMA Switched Network allows for dynamic routing and redundant paths through the network and reduces the likelihood of network communications disruption.
- FEMA has established an enterprise security manager position and an incident response team. Internet firewalls protect agency data from unauthorized intrusion. FEMA has also installed intra-lata firewalls to protect sensitive data, financial records, and classified operations.

This page intentionally left blank.



Organization: Federal Reserve System (FRS)

Senior Information Operations Official:

Clyde H. Farnsworth, Jr., Director, Division of Reserve Bank Operations and Payment Systems, 202-452-2787

Steven R. Malphrus, Director, Division of Information Resources, 202-452-2801

Information Assurance Points of Contact:

Kenneth D. Buckley, Assistant Director, Division of Reserve Bank Operations and Payment Systems, 202-452-3646

Anne Paulin, Senior Information Technology Consultant, Division of Reserve Bank Operations and Payments Systems, 202-452-2560

On-Line Resources:

Federal Reserve Banks: <http://www.federalreserve.gov>

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.

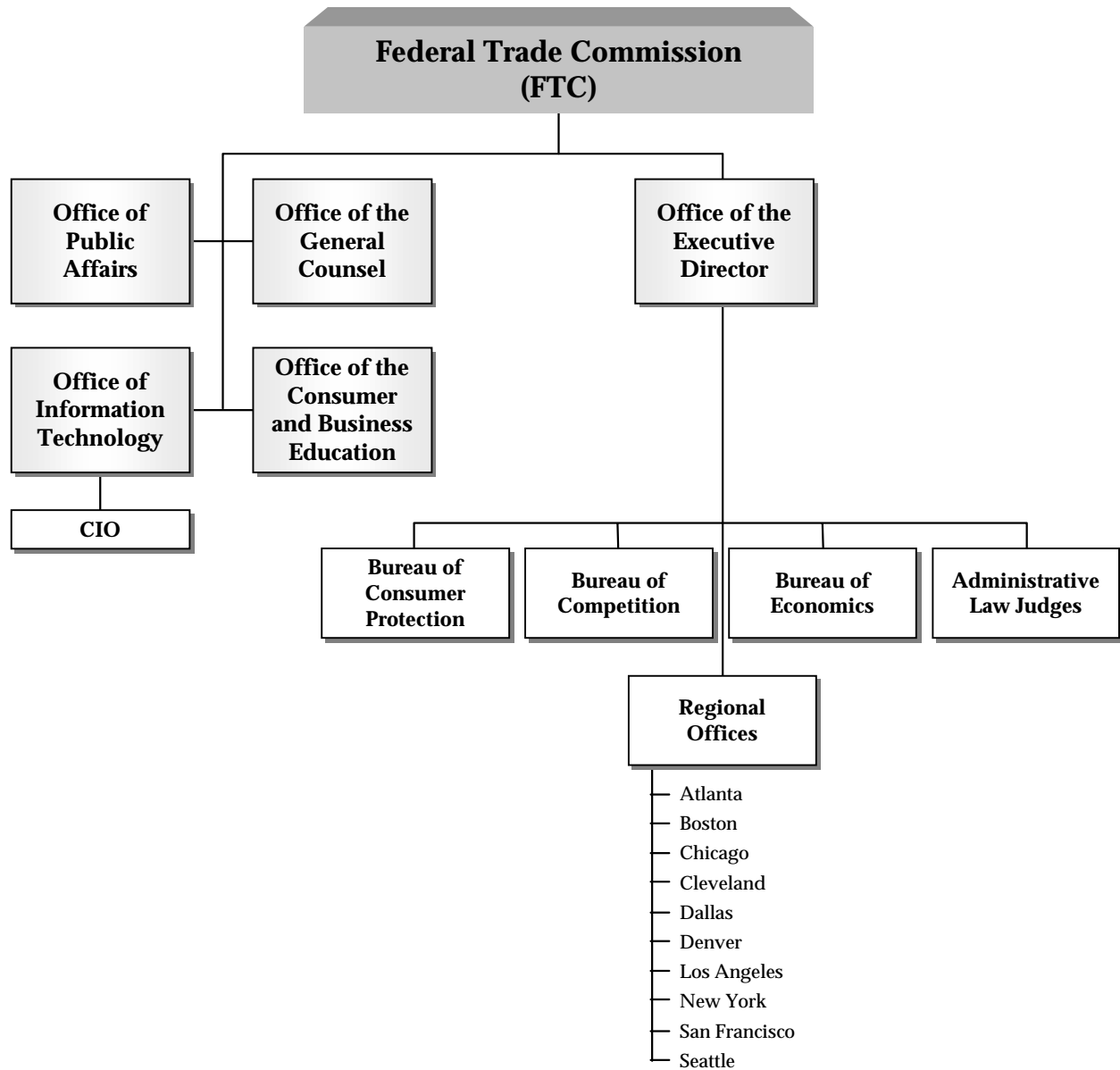
The Board of Directors of each Federal Reserve Bank is composed of nine members: three represent the stockholding member banks and are elected by those banks; three represent commerce, agriculture, or industry in the district and are elected by the stockholding member banks; and three are appointed by 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.

Activities:

- 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. 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 Federal Reserve Information Technology (FRIT) organization provides governance for IT planning, standards, and operations. In this role, FRIT is responsible for data security standards and policy administration. FRIT is advised by Reserve Bank IT and business stakeholders. One of these advisory 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 advises FRIT on 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 drives 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 and are tested regularly.
- FedWire is the real-time payments system application which supports over \$200 trillion annually in funds transfer and government securities transactions between financial institutions. FedNet is the FRS network over which this traffic moves. Fedline is the software that enables financial institutions to access FedWire and other Reserve Bank financial services.
- 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.



Organization: Federal Trade Commission (FTC)

Senior Information Operations Official:

Richard Turner, Chief Information Officer, 202-326-2875

On-Line Resources:

<http://www.ftc.gov>

Missions and Functions:

The Federal Trade Commission enforces a variety of federal antitrust and consumer protection laws. By eliminating acts or practices that are unfair or deceptive, the Commission seeks to ensure that the nation's markets function competitively and are vigorous, efficient, and free of undue restrictions. Its efforts are generally directed toward stopping actions that restrict competition or threaten consumers' ability to exercise informed choice. The Commission also undertakes economic analyses to support its law enforcement efforts and to contribute to the policy deliberations of various federal, state, and local government bodies.

The Office of Information and Technology Management (OITM) was created in 1996 with the goal of increasing Commission productivity and effectiveness by helping agency programs and staff make use of information and technology to improve the quality and quantity of their work. The strategy for meeting that goal had four elements:

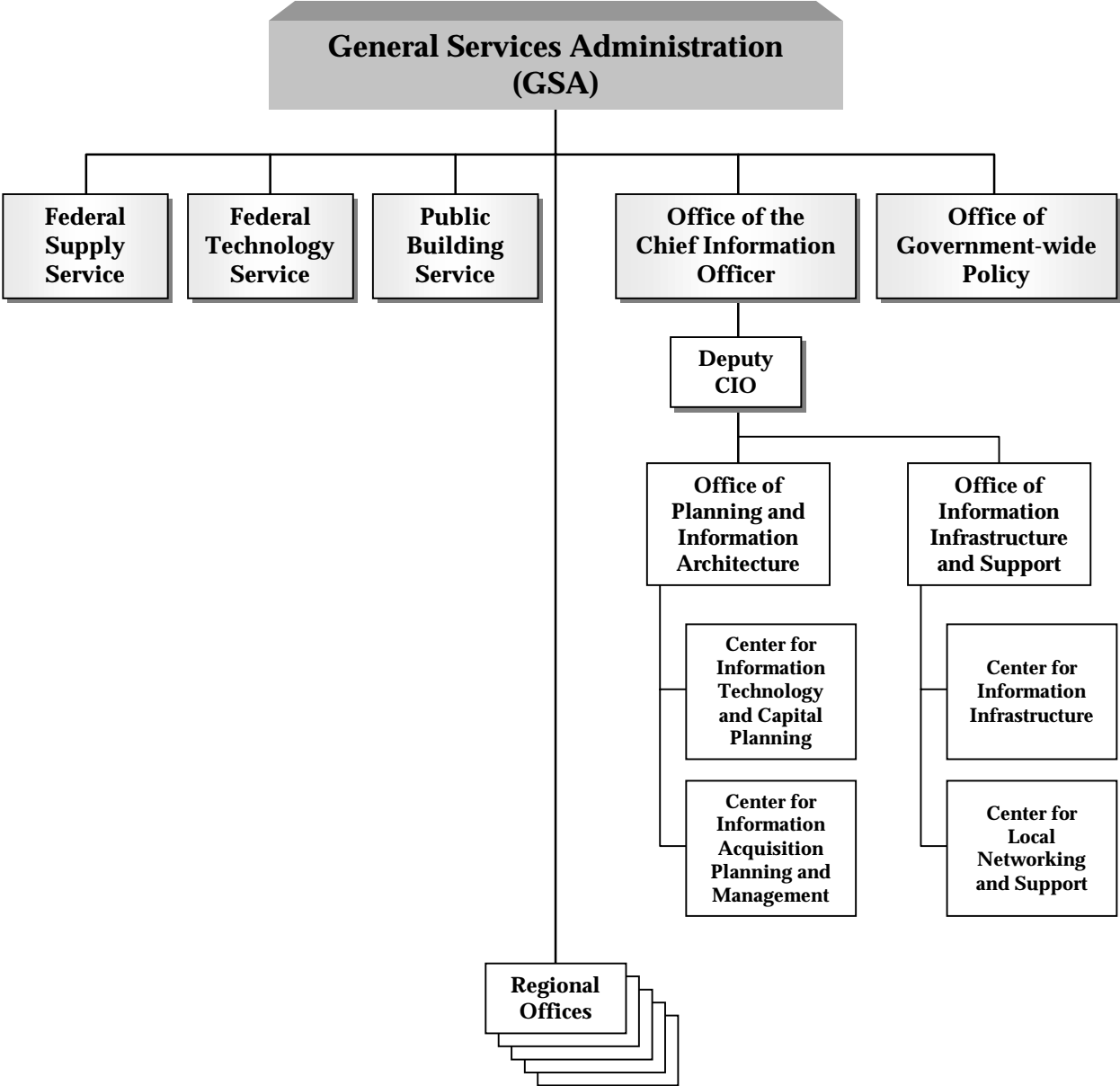
- Installing and maintaining the infrastructure of modern systems and other information resources that are necessary for the Commission's lawyers and economists to do their work
- Training and supporting Commission staff in the use of the infrastructure as effectively as possible
- Working with program managers and staff to focus resources on the Commission's priority law enforcement and consumer/business education goals
- Coordinating and supporting the majority of the Commission's information retrieval and dissemination efforts.

The OITM was structured into eight teams. The Chief Information Officer leads a team to provide overall management and direction to the program as well as administrative support in all areas. The other teams, which provide products and services directly to OITM customers, include Litigation and Customer Support, Library, Information Dissemination, Information Management, Software Development, Technology Operations, and Technology Development.

Activities:

- In 1997, the Office of Inspector General (OIG) conducted a review of the FTC's computer systems security and its computer service continuity policies and procedures and made twelve recommendations for corrective action, all of which have been implemented by the Commission. The OIG conducted penetration tests of the FTC's computer system to assess whether access controls put in place by information resource managers were adequate to prevent an unauthorized user from gaining access to sensitive data bases. The evaluation involved external probes to the firewall via the Internet, external probes through dial-in modems, internal probes of the network from within the FTC, and password control and cancellation of passwords when people left the organization.
- The OIG also examined preventive measures taken to minimize potential service disruptions due to fires, floods, malicious or virus attacks, system malfunctions, and other disasters, and to safeguard information resources should such disruptions occur. The OITM has taken many steps to ensure service continuity and that FTC records are safe from unexpected destruction. It implemented backup procedures to restore lost or damaged data and attached an uninterruptible power supply to each network server to allow for an orderly shutdown of network servers in the event of a power outage. The OITM has also implemented OIG recommendations to update the FTC's Disaster Recovery Plan and establish an independent security program under the direction of the CIO.

This page intentionally left blank.



Organization: General Services Administration (GSA)

Senior Information Assurance Official:

Shereen Remez, Chief Information Officer, GSA, 202-501-1000

Information Assurance Points of Contact:

Thomas Burke, Assistant Commissioner for Information Security, Federal Technology Service, GSA and Chief Infrastructure Assurance Officer for GSA, 202-708-7000

Dennis Fischer, Commissioner, Federal Technology Service, GSA, 703-285-1020

Donald Heffernan, Deputy Chief Information Officer, GSA, 202-501-1000

Diane Savoy, Director of Information Technology Capital Planning, Office of the CIO, GSA, 202-501-3535

Bruce Brignull, Assistant Commissioner for Service Development, Federal Technology Service, GSA, 703-610-2813

On-Line Resources:

GSA Homepage: <http://www.gsa.gov>

Federal Technology Service: <http://fts.gsa.gov>

GSA Office of Information Security: <http://fts.gsa.gov/infosec>

Federal Computer Incident Response Capability: <http://www.fedcirc.gov>

GSA Critical Infrastructure Protection: <http://www.gsa.gov/ciao>

GSA Y2K: <http://www.itpolicy.gsa.gov/mks/yr2000/y2khome>

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 Government wide 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 Federal Technology Service provides common-user telecommunications and other information services to agencies of the Federal government.

The Office of Information Technology Integration (ITI), a component of the Federal Technology Service (FTS), General Services Administration (GSA), provides a wide variety of products and services suitable for use by the information warrior. ITI provides cost-

reimbursable IT services to the civilian and military intelligence communities and to Federal entities concerned with information assurance and security. ITI helps Federal agencies effectively and efficiently acquire, manage, and use information technology resources through four separate, complementary programs tailored to meet the IT needs of its clients. All ITI programs operate on a worldwide basis.

FEDSIM. The Federal Systems Integration and Management Center (FEDSIM) provides technology-driven solutions for information systems problems with a knowledgeable and experienced staff that understands the issues facing the IT warfare community. FEDSIM uses a variety of Government-wide acquisition vehicles that have proven both flexible and cost-effective in meeting the needs of the information warfare community. FEDSIM specializes in IT system acquisition, systems integration, secure office systems, software management and analysis, and secure data center management.

FISSP. The Federal Information Systems Support Program (FISSP) employs highly skilled technical and acquisition professionals to provide comprehensive IT services through a network of regional offices. FISSP provides software definition and design, risk analysis and security support, facilities management services, and comprehensive support of business, administrative, and scientific and engineering services.

FEDCAC. The Federal Acquisition Support Center (FEDCAC) specializes in conducting large-scale IT acquisitions--from project initiation to contract award and administration. FEDCAC has a proven track record of outstanding accomplishments in complex, large-scale IT acquisitions for the Federal law enforcement and intelligence communities.

FAST. The Federal Acquisition in Support of Technology (FAST) program specialized in the rapid acquisition of IT products and commodities, and provides a quick-start mechanism for contracting for more complex products and services that may be required by the information warfare community.

Activities:

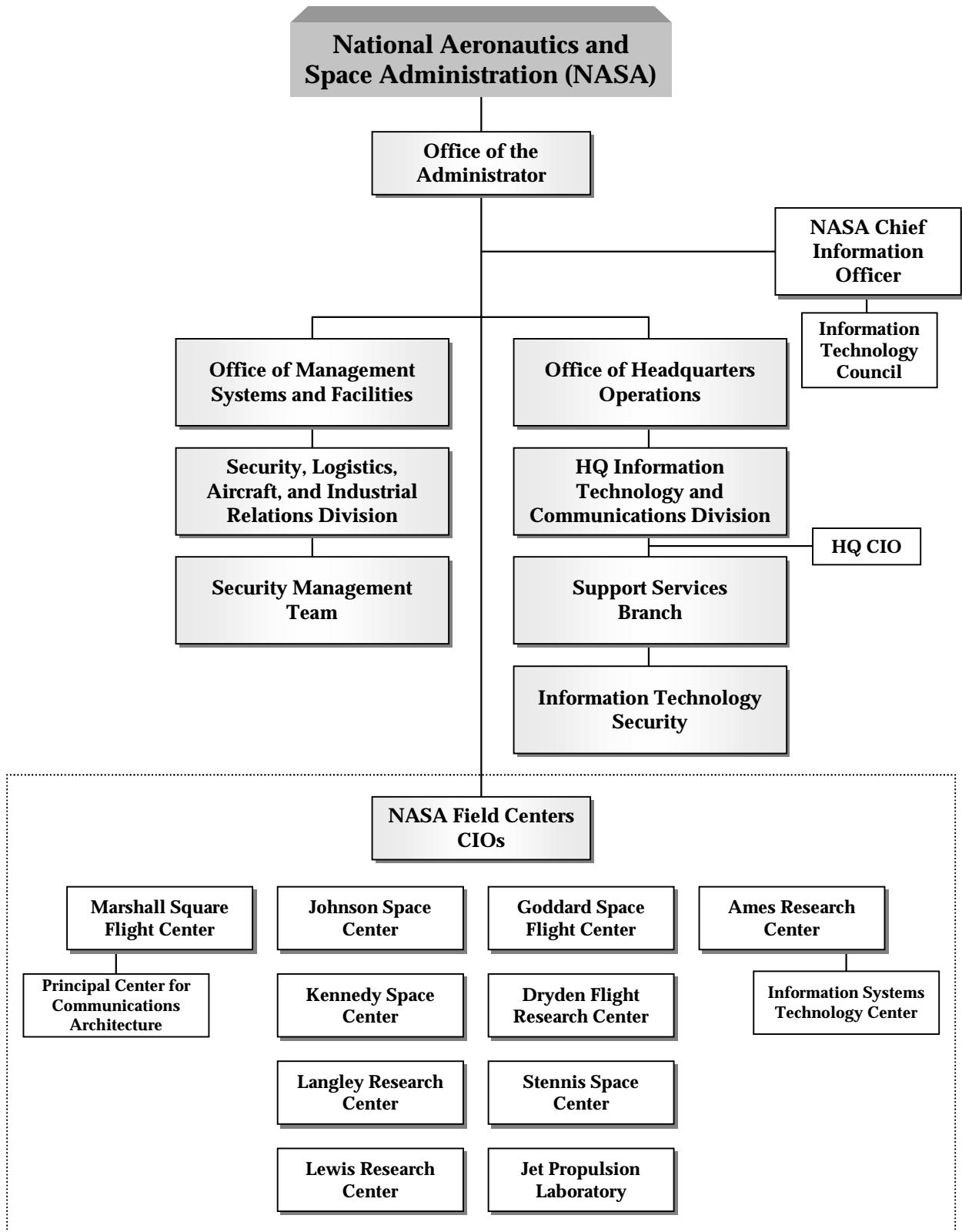
- GSA is involved with infrastructure protection, to include buildings and telecommunications, and works with FEMA and NCS in emergency planning.
- The Chief Infrastructure Assurance Officer for GSA has been named the Executive Agent for the Federal Sector under PDD-63 and is charged with pulling the agencies together to create a Federal model.
- 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 leads the NSTISSC Infrastructure Assurance Group
- GSA is developing a public key solution using digital signatures for Access Control and data integrity.

- GSA manages the Federal Computer Incident Response Capability (FedCIRC) which utilizes the services of the Carnegie-Mellon, Software Engineering Institutes CERT facility as its operational partner.
- Resource reallocation during disruptions of service are managed dynamically by pulled-together teams that draw upon internal assets and expertise.
- 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 participates as a full member in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and co-chairs the Subcommittee for Telecommunications Security of the NSTISSC. OIS also represents GSA on the Military Communications Electronic Board, the Federal Public Key Infrastructure Steering Committee (FPKISC), and the Security Policy Board. OIS also participates in the Federal Agency Computer Security Program Manager's Forum (FACSPMF).
- GSA has two 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 (ECPMO), co-chaired by DOD and GSA, and the Electronic Messaging Program Management Office, chaired by GSA. Both PMO's 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.
- GSA administers the Federal Computer Incident Response Capability (FedCIRC) through the Office of Information Security in the Federal Technology Service. FedCIRC operates a 24 hour hot-line for intrusion report and response utilizing the services of the Computer Emergency Response Team at the Software Engineering Institute of

Carnegie-Mellon University. In addition to this, FedCIRC is dedicated to the improvement in awareness and understanding of the threat facing Federal Agencies from unlawful penetration of Open Systems. Toward this end, FedCIRC seeks a collaborative relationship across the entire Federal Government dedicated to information sharing and education.

- The Federal Technology Service is managing the Access Certificates for Electronic Services (ACES) initiative which seeks to facilitate private citizen electronic access to government services and benefits through the use of public key supported digital signatures.
- Information security policy development for GSA is done by the Information Technology Capital Planning Division, Office of the Chief Information Officer. Policy directives in the form of manuals, handbooks, etc. have been published and cover the traditional areas of computer security.
- The Office of Service Development, Federal Technology Service, operates an interagency group responsible for developing Post FTS2000 acquisition strategy. 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.

This page intentionally left blank.



Organization: National Aeronautics and Space Administration (NASA)

Senior Information Operations Official:

Lee B. Holcomb, NASA Chief Information Officer, 202-358-1824

Jeffrey E. Sutton, Associate Administrator, Office of Management Systems and Facilities,
202-358-2800

Michael D. Christensen, Associate Administrator, Office of Headquarters Operations, | 202-
358-2100

Information Assurance Points of Contact:

Sandra Daniels-Gibson, HQ Information Technology and Communications Division,
202-358-1340

Thomas Walthall, Assistant Manager, Information Technology Security, 202-358-1304

Critical Infrastructure Protection Points of Contact:

Mark R. J. Borsi, Director, Security, Logistics, Aircraft, and Industrial Relations Division,
202-358-2457

Robert E. Turner, Lead Security Management Team, 202-358-2319

On-Line Resources:

NASA Homepage: <http://www.hq.nasa.gov>

Missions and Functions:

The National Aeronautics and Space Administration conducts research for the development of advanced 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 NASA Chief Information Officer is responsible for the development of information resource management strategies, policies, and practices. These encompass strategic planning; standards in computing, networking, and security; establishment of system and information architectures; and incorporation of life-cycle management concepts into information technology acquisitions and management. Separate CIO offices have been established at certain field centers and within the Office of Headquarters Operations to provide guidance within specific parts of the NASA organization.

The Information Technology and Communications Division is responsible for Headquarters-wide information technology management and policy formulation as well as

the delivery of comprehensive ADP and telecommunications services. The Director also serves in the dual capacity of the Headquarters CIO, responsible for working with the NASA CIO and NASA Center CIOs in developing and executing information technology architecture, standards, and policies across the agency.

The overall goal of the Information Technology Security Program at NASA Headquarters is to continually improve the security posture of the Headquarters IT infrastructure in a manner deemed most efficient and effective in terms of incident prevention, damage minimization, resource utilization, and law enforcement.

The Security, Logistics, Aircraft, and Industrial Relations Division provides functional leadership and management for all Agency security programs. The security programs include personnel security, physical security (including NASA resource protection), information security, communications security, automated information security, industrial security, operations security, law enforcement, and program security. These programs, taken together, provide for the protection of the people, facilities, information, and other resources and missions of the Agency.

Ames Research Center, Moffett Field, CA has been designated as NASA's Center for Excellence for Information System technologies, encompassing research in supercomputing, networking, numerical computing software, artificial intelligence, and human factors to enable bold advances in aeronautics and space.

Activities:

- In 1995, in an effort to ensure end-user utility and a manageable, affordable infrastructure for all information technologies, the NASA CIO designated three Agency field centers as "Principle" for the technology components of Communications, Security, and Workgroup Hardware and Software. Marshall Space Flight Center, Huntsville, AL, was designated as the Principle Center for Communications Architecture. The Principle Center Integration Team (PCIT) consists of the Project Managers from each of the three Principal Centers. This team, under the direction of the Office of the Agency CIO, is responsible for the overall prioritization, evaluation, integration and implementation of Agency Information Technology initiatives.
- 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)).

- 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 that loss or destruction of the information or resources might have.
- NASA participates in a variety of interagency information technology security activities that include the National Security Telecommunications and Information Systems Security Committee (NSTISSC), the Information Infrastructure Task Force Security Issues Forum (SIF) Security Policy Board, the Information Systems Security Organization (ISSO), the National Institute of Standards and Technology (NIST) Working Groups, and the Forum of Incident Response and Security Teams (FIRST).

**Director of
Central Intelligence**



**National Intelligence Council
(NIC)**

Organization: National Intelligence Council (NIC)

NIC Leadership:

John Gannon, Chairman, 703-482-6724

Ellen Laipson, Vice Chairman, 703-482-3578

Richard Haver, Chief of Staff, 703-482-9918

Dolores Greene, Director, Evaluation Staff, 703-482-6152

Stuart A. Cohen, Director, Senior Review, Production and Analysis Staff, 703-482-0741

William Nolte, Director, Outreach and Strategic Planning, 703-482-7072

Kay Zerwick, Executive Officer, 703-482-5624

NIO Portfolio:

Robert Houdek, Africa, 703-482-7225

Robert Suettinger, East Asia, 703-482-5721

David Gordon, Economics and Global Issues, 703-482-4128

Barry Lowenkron, Europe, 703-482-6295

John Landry, General Purpose Forces, 703-482-7105

Randy Pherson, Latin America, 703-482-3136

Ben Bonk, Near East and South Asia, 703-482-6834

George Kolt, Russian and Eurasia, 703-482-6297

Lawrence Gershwin, Science and Technology, 704-482-6811

Stuart A. Cohen, Special Activities, 703-482-0741

Robert Walpole, Strategic and Nuclear Programs, 703-482-7424

Robert Vickers, Warning, 703-482-0993

On-Line Resources:

NIC Homepage: <http://www.odci.gov/ic/icagen2.htm>

Missions and Functions:

The NIC manages the Intelligence Community's estimative process, bringing together the best available expertise inside and outside the government on issues of strategic importance. The NIC's Strategic Estimate Program for 1999 will examine broad features of the changing security environment, including the information revolution, the declining authority of the state, future military conflict, and global economic threats. The NIC also supports the ADCI/AP and his counterpart for collection in guiding collectors on requirements. The NIC provides the DCI and key intelligence consumers timely assessments of Intelligence Community analytic priorities, capabilities, and resource needs.

The 12 National Intelligence Officers (NIOs) who serve on the NIC are substantive experts drawn from all elements of the Intelligence Community and from outside the government. NIOs have one or more deputies.

The functions of NIOs include: to advise the DCI on substantive issues; interact regularly with senior intelligence consumers and support their current and longer term needs; produce top-quality estimative intelligence; engage with outside experts to tap their knowledge and insights; assess the capabilities and needs of analytic producers; promote collaboration among Intelligence Community analytic producers on strategic warning, advanced analytical tools, and methodologies; and articulate substantive priorities to guide intelligence collection, evaluation, and procurement.

National Intelligence Estimates (NIEs) are produced by the NIC. They are prepared for the President and other senior policymakers on issues that have strategic implications for the United States. They are the most authoritative written assessments of the DCI and the Intelligence Community because they present the coordinated views of the senior officers of the Intelligence Community. Many NIEs focus on long-range issues that will affect U.S. vital interests.

The NIC actively seeks to collaborate with experts from academia, the corporate world, and think tanks in producing NIEs and other estimative products. Outside experts provide a unique perspective on intelligence issues, and the Community highly values their insights and opinions.

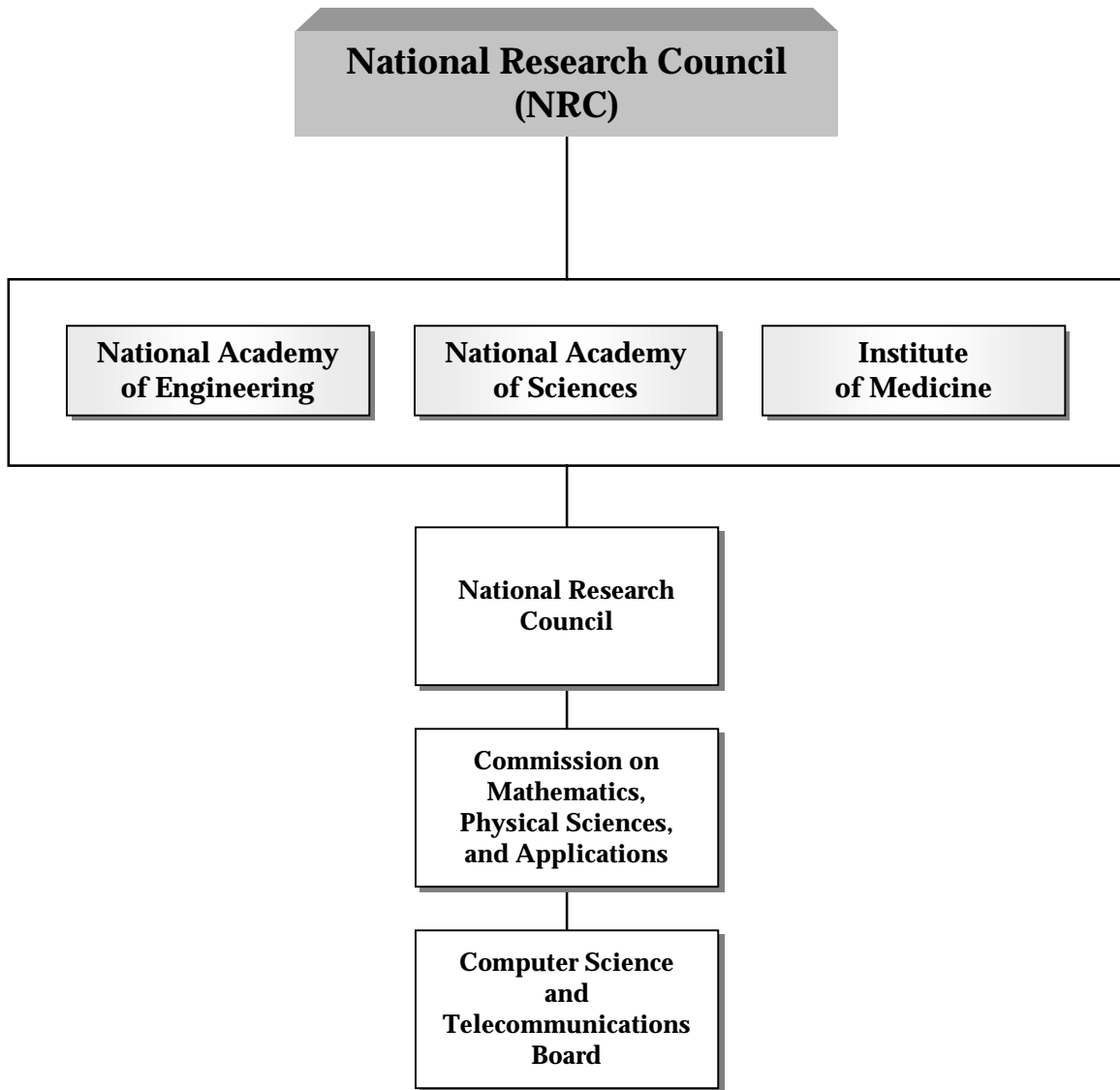
Activities:

In 1999, the NIC is undertaking a systematic research and development program on board, crosscutting issues for the next millennium, which constitutes the DCI's Strategic Estimates program. We envision engaging broadly with experts outside the Intelligence Community in understanding these issues. The program includes a series of conferences, gaming exercises, and other activities to expand on analytic capabilities in these areas.

- **Warning in a Changing Security Environment.** The Intelligence Community will expand its warning competence against new security issues: terrorism proliferation, humanitarian emergencies, narcotics, and severe economic shocks. This project will use "red team" exercises to explore alternative scenarios on such daunting warning problems as Korea.
- **The Future of Military Conflict.** The project will assess the nature and character of future conflicts -- those that affect the United States directly and from a distance. One area of analysis will focus on the changing character of strategic warfare in the 21st century as new states join the strategic "club" armed with new classes of weapons and employment concepts. Priority analyses will also include the security implications of defense industry globalization and foreign approaches to the revolution in military affairs.
- **The Information Revolution.** This project will consider how effectively various regions, countries, and sectors of society can cope with the information revolution, and to what extent the information revolution will bridge the gap, or alternatively, exacerbate the differences between the "haves" and "havenots." It will assess the scope and pace of the information revolution in its technical dimensions. We will examine the consequences

of Y2K failures worldwide in terms of national security concerns, as a near-term example of differences in dealing with the information revolution.

- Declining Authority of the Nation-State. Globalization, ethnic particularism, and the permeability of borders to the movement of people, ideas, and goods (both licit and illicit) will combine to challenge the ability of states to remain the guarantor of the security and well-being of their populations. We will examine how these developments will affect the role of states as the building blocks of the international system.
- Global Economic Threats. Unprecedented market volatility is threatening the economics of various countries and the “Washington Consensus” on such issues as the liberalization of trade and capital flows. Also, economic crises tend to stimulate the growth of illegal activities. We particularly will consider how affected countries are “learning” from the global financial crisis and how that will affect U.S. interests.
- Challenges to the Surviving Superpower. The United States is having increasing difficulty translating its unparalleled power into influence on key developments in the international community. We are particularly interested in understanding how allies and adversaries anticipate the United States will use military power and whether there is a growing discrepancy between American interests and the agendas of other state and non-state actors on humanitarian, environmental, and legal/normative issues.
- Global Trends 2015. The NIC will produce a follow-on to our 1996 study. *Global Trends 2010*, which identified population growth, economic progress, food, communications, energy, and military technology as key factors in shaping the world.



Organization: National Research Council (NRC)

Information Assurance Points of Contact:

Marjory Blumenthal, Director, Computer Science and Telecommunications Board,
202-334-2601

Herbert Lin, Senior Scientist, 202-334-3191

On-Line Resources:

Computer Science and Telecommunications Homepage: <http://www2.nas.edu/cstbweb>

Missions and Functions:

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; and international scientific and technological relations and competition.

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). 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.

Activities:

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.

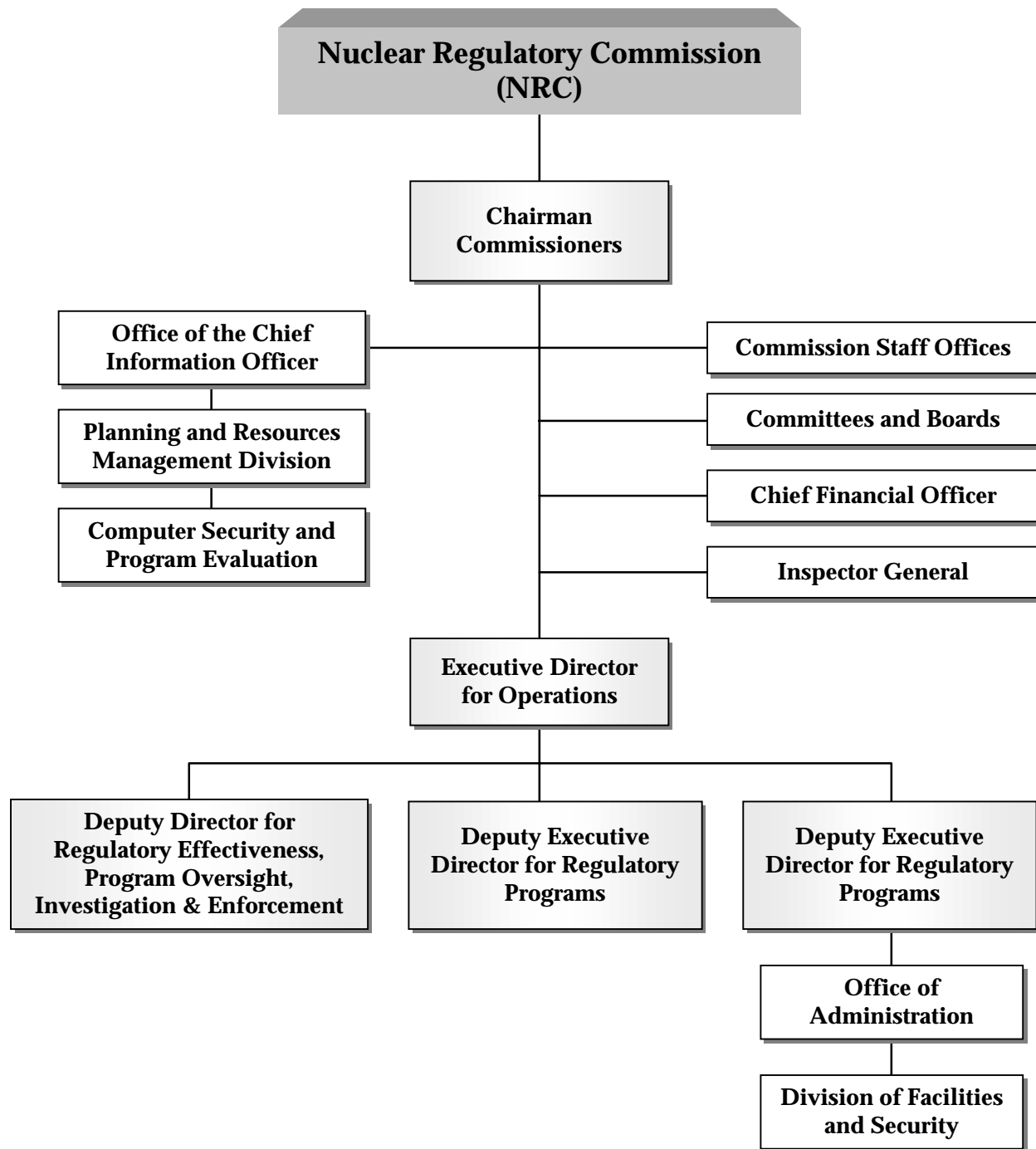
In 1996, the CSTB convened a Committee on Information Systems Trustworthiness to assess the state-of-the-art in technologies that foster the increased trustworthiness of networked information systems, to use this assessment as the basis for identifying the most promising avenues for relevant long-term research of a fundamental or revolutionary (as opposed to incremental) nature, and to provide guidance to DARPA and NSA on how to best facilitate such research advances. The Committee's report, *Trust in Cyberspace*, was released in 1998 and includes the following conclusions and recommendations:

- The Public Telephone network (PTN) and Internet
 - The public telephone network is increasingly dependent on software and databases that constitute new points of vulnerability. Business decisions are also creating new points of vulnerability. Protective measures need to be developed and implemented.
 - In some respects, the Internet is becoming more secure as its protocols are improved and as security measures are more widely deployed at higher levels of the protocol stack. However, the increasing complexity of the Internet's infrastructure contributes to its increasing vulnerability. The end points (hosts) of the Internet continue to be vulnerable. As a consequence, the Internet is ready for some business use, but abandoning the PTN for the Internet would not be prudent for most. The Internet is too susceptible to attacks and outages to be a viable basis for controlling critical infrastructures. Existing technologies could be deployed to improve the trustworthiness of the Internet, although many questions about what measures would suffice do not currently have answers because good basic data (e.g., on Internet outages) are scant.
 - Operational errors represent a major source of outages for the PTN and the Internet. Some of these errors could be prevented by implementing known techniques, whereas others require research to develop preventive measures.
- Software for Networked Information Systems (NIS)
 - The design of trustworthy networked information systems presents profound challenges for system architecture and project planning. Little is understood, and this lack of understanding ultimately compromises trustworthiness.
 - To develop an NIS, subsystems must be integrated, but little is known about doing this. In recent years, academic researchers have directed their focus away from large-scale integration problems; this trend must be reversed.
 - It is clear that NISs will include COTS components into the foreseeable future. However, the relationship between the use of COTS components and NIS trustworthiness is unclear. Greater attention must be directed toward improving our understanding of this relationship.

- Although there are accepted processes for component design and implementation, the novel characteristics of NISs raise questions about the utility of these processes. Modern programming languages include features that promote trustworthiness, and the potential may exist for further gains from research.
- Formal methods are being used with success in commercial and industrial settings for hardware development and requirements analysis and with some success for software development. Increased support for both fundamental research and demonstration exercises is warranted.
- Reinventing Security
 - Security research during the past few decades has been based on formal policy models that focus on protecting information from unauthorized access by specifying which users should have access to data or other system objects. It is time to challenge this paradigm of “absolute security” and move toward a model built on three axioms of insecurity—insecurity exists, insecurity cannot be destroyed, and insecurity can be moved around.
 - Cryptographic authentication and the use of hardware tokens are promising avenues for implementing authentication.
 - Obstacles exist to more widespread deployment of key-management technology, and there has been little experience with public-key infrastructures, especially large-scale ones.
 - Because NISs are distributed systems, network access control mechanisms play a central role in their security. Virtual private networks and firewalls have proven to be promising technologies and deserve greater attention in the future.
 - Foreign code is being used increasingly in NISs. However, NIS trustworthiness will deteriorate unless effective security mechanisms are developed and implemented to defend against attacks by foreign code.
 - Defending against denial-of-service attacks is often critical for the security of an NIS, because availability is often an important system property. Research in this area is urgently needed to identify general schemes for defending against such attacks.
- Trustworthy Systems from Untrustworthy Components
 - Improved trustworthiness may be achieved by the careful organization of untrustworthy components. There are a number of promising ideas, but few have been vigorously pursued. “Trustworthiness from untrustworthy components” is a research area that deserves greater attention.
- Economic and Public Policy Context
 - Imperfect information creates a disincentive to invest in trustworthiness for both consumers and producers, leading to a market failure. Initiatives to mitigate this problem are needed.
 - Consumer and producer costs for trustworthiness are difficult to assess. An improved understanding, better models, and more and accurate data are needed.
 - As a truly multidimensional concept, trustworthiness is dependent on all of its dimensions. However, in some cases, the problems of security are more challenging and therefore deserve special attention.
 - Export control and key-escrow policy concerns inhibit the widespread deployment of cryptography, but there are other important inhibitory factors that deserve increased attention and action.

- In its necessary efforts to pursue partnerships, the federal government also needs to work to develop trust in its relationships with the private sector, with some emphasis on U.S.-based firms.
- The NSA R2 organization must increase its efforts devoted to outreach and recruitment and retention issues.
- DARPA is generally effective in its interactions with the research community, but DARPA needs to increase its focus on information security and NIS trustworthiness research, especially with regard to long-term research efforts.
- An increase in expenditures for research in information security and NIS trustworthiness is warranted.

This page intentionally left blank.



Organization: Nuclear Regulatory Commission (NRC)

Senior Information Operations Official:

Anthony J. Galante, Chief Information Officer, 301-415-8700, ajg@nrc.gov

Information Assurance Points of Contact:

Anthony J. Galante, Chief Information Officer, 301-415-8700, ajg@nrc.gov
Francine F. Goldberg, Director, Planning and Program Support Division, 301-415-7545
James B. Schaeffer, Director, Information Technology Infrastructure Division, 301-415-8720,
jbs@nrc.gov

Critical Infrastructure Protection Points of Contact:

Anthony J. Galante, Chief Information Officer, 301-415-8700, ajg@nrc.gov
Francine F. Goldberg, Director, Planning and Program Support Division, 301-415-7545
James B. Schaeffer, Director, Information Technology Infrastructure Division, 301-415-8720,
jbs@nrc.gov
Thomas O. Martin, Director, Division of Facilities and Security, 301-415-8080, tom@nrc.gov

On-Line Resources:

NRC Homepage: <http://www.nrc.gov>

Missions and Functions:

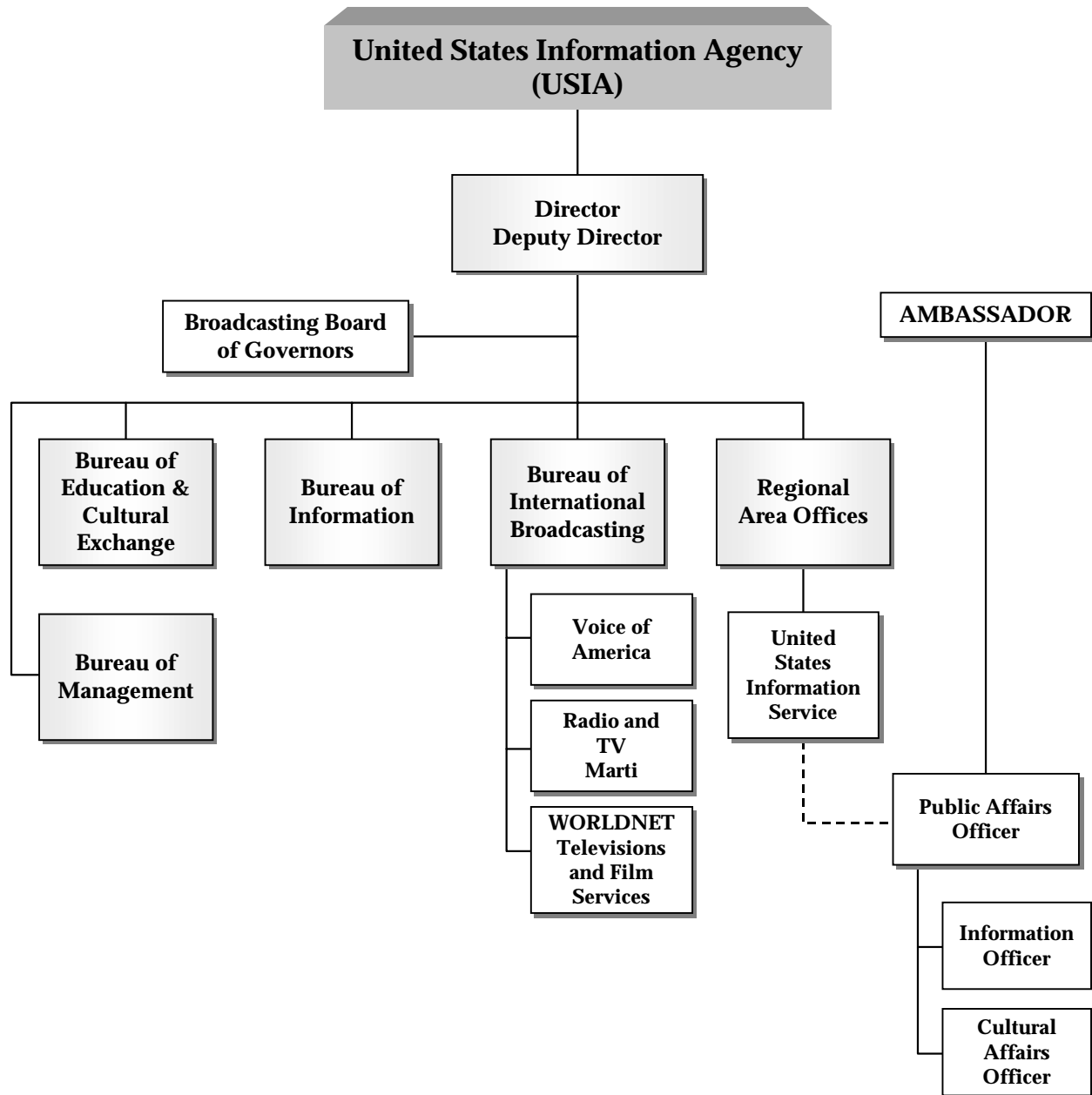
The Office of the Chief Information Officer (OCIO) plans, directs and oversees the delivery of centralized information technology (IT), applications, and information management (IM) services, and the development and implementation of IT and IM plans. Provides principal advice and assistance to ensure the agency IT and IM resources are selected and managed in a manner that maximizes their value, manages risks, and is consistent with Federal laws and regulations. Coordinates agency IT and IM program evaluation, development of agency IT and IM policy, and development and implementation of agency IT training. Directs NRC's computer security program which implements administrative, technical, and physical security measures for the protection of NRC's information, automated systems, and IT infrastructure. Provides technical guidance and direct assistance concerning implementation of agency-wide application systems and IT infrastructure issues and practices. Serves as liaison with application development teams and coordinates program office infrastructure development, operations and support requirements.

The Division of Facilities and Security plans, develops, establishes, and administers policies, standards, regulations and procedures for the overall NRC security program, including the protection of classified and sensitive unclassified information at NRC and NRC contractors, licensees, certificate holders and other facilities; the physical protection of NRC facilities; and the management of the NRC's secure communications capabilities.

Activities:

- OCIO develops, manages, and implements policies and procedures for the NRC Automated Information System Security Program. Managers of the various NRC offices are assisted by OCIO in developing and performing risk assessments, computer security and business continuity plans, as well as system certification testing and accreditation. OCIO conducts independent security reviews and penetration studies. Periodic Computer Security Awareness training is provided for all employees and contractors and specialized training related to selected or requested activities (such as care and handling of classified data). Throughout the year, OCIO contributes computer security related articles to agency news media and on-line announcements, and creates an annual observance of International Computer Security Awareness Day.

This page intentionally left blank.



Organization: United States Information Agency (USIA)

Senior Information Operations Official:

Jonathan Spalter, Chief Information Officer, 202-619-4545

Information Assurance Points of Contact:

Daniel Campbell, Director, USIA Office of Technology, 202-619-5318

Chris Kern, Director, IBB Office of Computing Services, 202-619-2620

Margaret Johnson, Telecommunications Manager, Representative to the NCS, 202-619-5514
Committee of Principals/Council of Representatives

Critical Infrastructure Protection Points of Contact:

Neil Lehrer, Senior Computer Specialist, Network and Internet Security Issues

On-Line Resources:

USIA Homepage: <http://www.usia.gov>
<http://www.mt.usia.gov>

Missions and Functions:

On October 1, 1999, USIA will cease to exist as an independent agency, and most of its functions and resources will be merged into the Department of State. The International Broadcasting Bureau, which is currently part of USIA and includes VOA, Radio and TV Marti, and WORLDNET will become an independent agency.

The USIA mission is to promote the national interest and national security through understanding, informing, and influencing foreign publics and broadening dialogue between American citizens and institutions and their counterparts abroad. One of the primary goals of USIA is to create an open international information environment that encourages the widest possible exchange of ideas and fosters an understanding of U.S. policies and institutions.

Activities:

- USIA's primary communication tools are a daily text and information service, known as the Washington File; electronic journals; pamphlets, posters, and specialized publications; and electronic and library-based research and database access, including the Internet Web site. The Agency also conducts electronic teleconferences and administers programs that send American specialists and professionals overseas to speak on virtually any topic, from intellectual property rights to American literature. Three Foreign Press Centers provide assistance to foreign journalists in the United States; however, by law, USIA is prohibited from directing informational programs

toward its own citizens. Under the United States Information and Educational Exchange Act of 1948, USIA's informational programs have been directed only to overseas audiences.

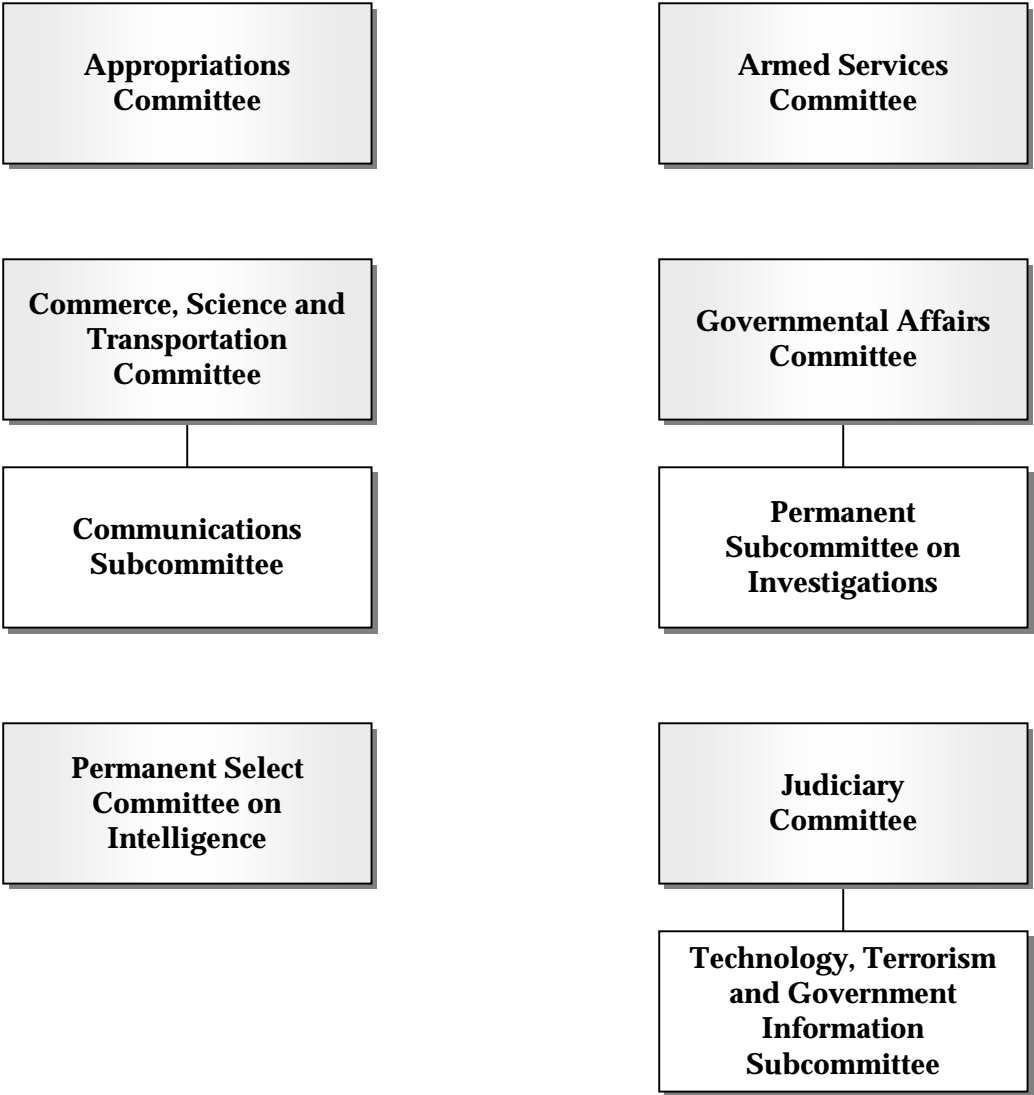
- The Voice of America, the USIA's international radio service, broadcasts more than 800 hours of programming each week on shortwave and medium wave and by satellite in English and other languages. All programming originates from VOA's Washington, D.C. headquarters, which is equipped with 45 radio studios and two television studios, a 150-channel master control, and two centers to record reports from VOA correspondents around the world. A worldwide network of relay stations transmits VOA's programs to its international audience.
- WORLDNET Television and Film Service is the USIA's global public affairs, information, and cultural television network. It transmits its programming by satellite from studios in Washington, D.C. to U.S. embassies, cultural centers, broadcasters, and cable-casters.
- The Office of Cuba Broadcasting operates Radio and TV Marti, which act as surrogate stations focusing on Cuban domestic and international news and information that is not reported by the government-controlled media. Radio Marti broadcasts 24 hours a day, seven days a week, on shortwave and medium wave.
- Over the next six years, USIA plans to upgrade and integrate its worldwide electronic network so that information and programs – text, audio, video, and language – can be digitized and made accessible easily, flexibly, and in real time. Use of the Internet will continue to increase as a means of both transmitting internal communications and making USIA products available to its audience.



Legislative and Judicial

This page intentionally left blank.

Committees of the Senate



Organization: Senate

On-Line Resources:

Senate Homepage: <http://www.senate.gov>

Thomas legislative information: <http://thomas.loc.gov>

Missions and Functions:

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.

Activities:

Committee/Subcommittee: Appropriations Committee

Chairman: Sen. Stevens, Alaska

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Armed Services Committee

Chairman: Sen. Warner, Virginia

Information Assurance Related Missions and Functions:

- Defense budget authorization.

Information Assurance Activities:

Committee/Subcommittee: Committee on Commerce, Science and Transportation

Chairman: Sen. McCain, Arizona

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Communications

Chairman: Sen. Burns, Montana

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Committee

Chairman: Sen. Thompson, Tennessee

Information Assurance Related Missions and Functions:

- Privacy Act, regulatory issues, government performance and results

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Permanent Subcommittee on Investigations

Chairman: Sen. Collins, Maine

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Sen. Shelby, Alabama

Information Assurance Related Missions and Functions:

- Oversight of Intelligence Community Agencies

Information Assurance Activities:

*Report Accompanying S.2052, Intelligence Authorization Act for FY99, included a requirement for a report detailing Intelligence Community's role in critical infrastructure protection and an assessment of the Intelligence Community's information infrastructure.

Committee/Subcommittee: Judiciary Committee

Chairman: Sen. Hatch, Utah

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Judiciary Subcommittee on Technology, Terrorism and Government Information

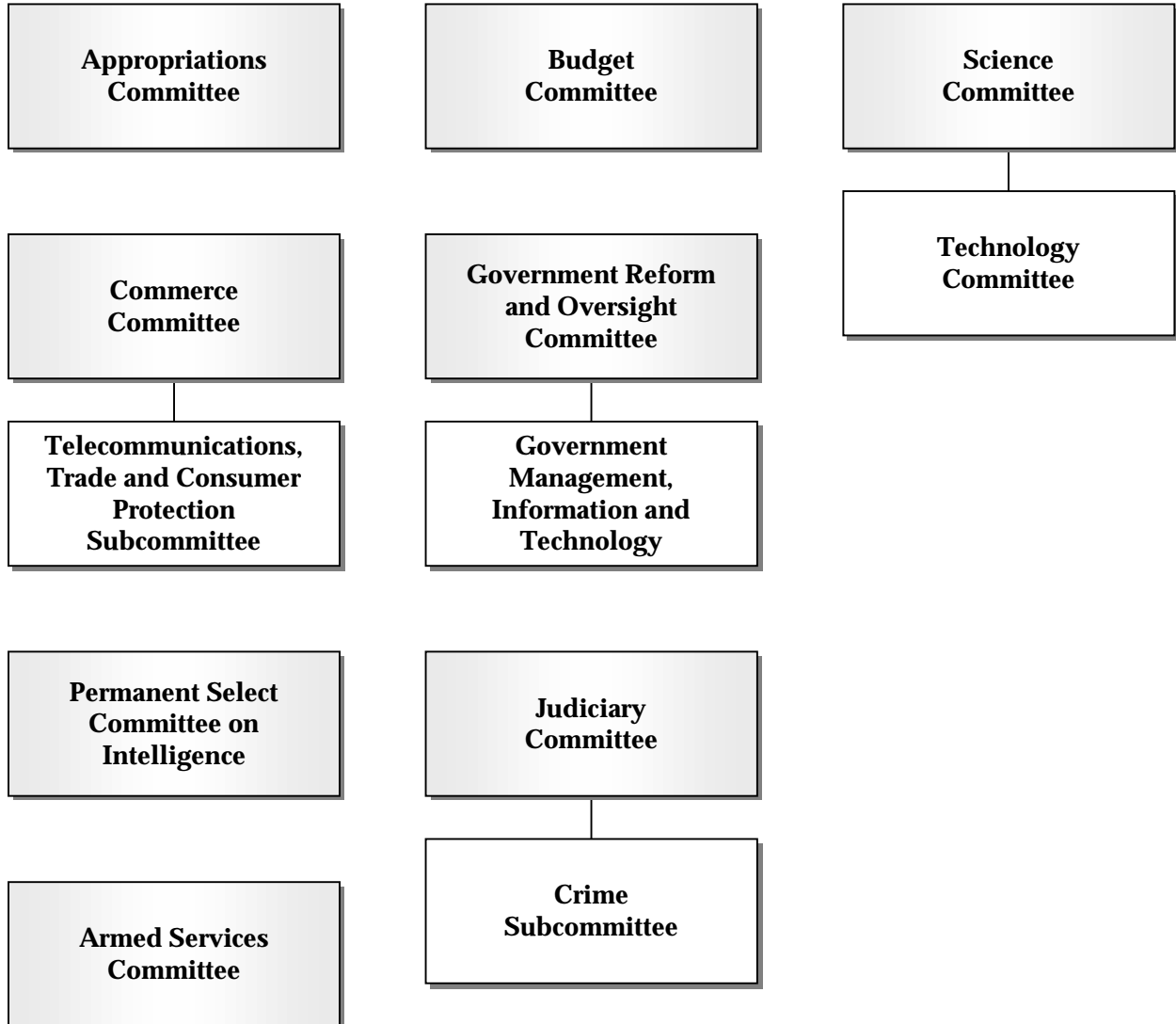
Chairman: Sen. Kyl, Arizona

Information Assurance Related Missions and Functions:

Information Assurance Activities:

This page intentionally left blank.

Committees of the House of Representatives



Organization: House of Representatives (HoR)

On-Line Resources:

House Homepage: <http://www.house.gov>

Thomas legislative information: <http://thomas.loc.gov>

Missions and Functions:

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 is indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

Activities:

Committee/Subcommittee: Appropriations Committee

Chairman: Rep. Young, Florida

Information Assurance Related Missions and Functions:

- Budget

Information Assurance Activities:

Committee/Subcommittee: Armed Services Committee

Chairman: Rep. Spence, South Carolina

Information Assurance Related Missions and Functions:

- Defense Budget “authorizers”

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, Trade, and Consumer Protection

Chairman: Rep. Tauzin, Louisiana

Information Assurance Related Missions and Functions:

- Privacy and telecommunications

Information Assurance Activities:

Committee/Subcommittee: Government Reform and Oversight Committee (formerly Government Operations Committee)

Chairman: Rep. Burton, Indiana

Information Assurance Related Missions and Functions:

- Civil Service, Postal Service, and Washington DC oversight

Information Assurance Activities:

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. Goss, Florida

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:

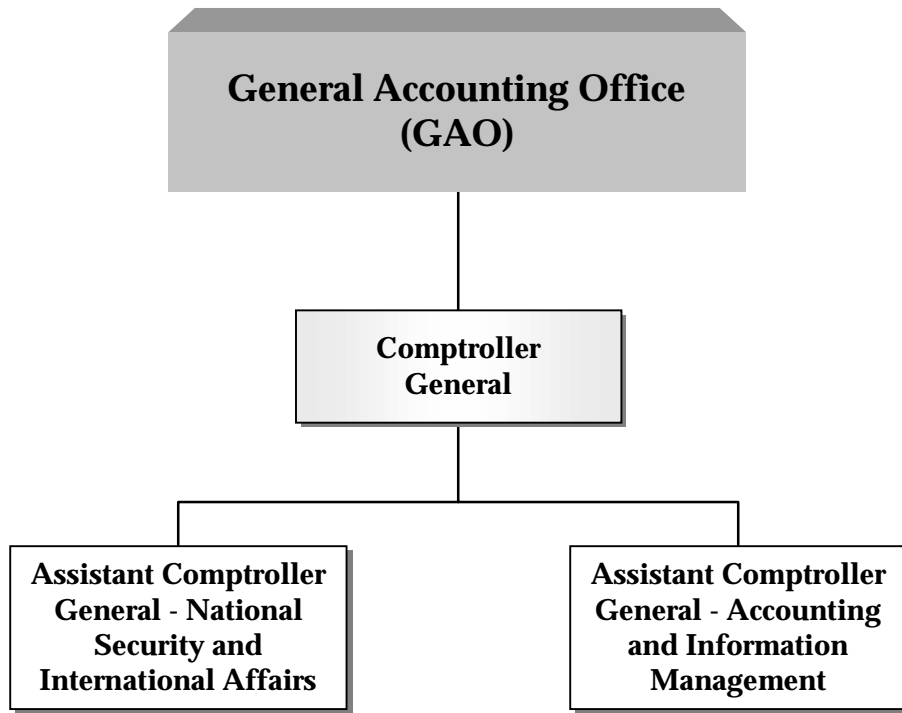
Committee/Subcommittee: Science Committee

Chairman: Rep. Sensenbrenner, Wisconsin

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Science Subcommittee on Technology
Chairman: Rep Morella, Maryland
Information Assurance Related Missions and Functions:
Information Assurance Activities:



Organization: General Accounting Office (GAO)

Senior Information Assurance Official:

Gene Dodaro, Assistant Comptroller General, Accounting and Information Management Division, 202-512-2600, dodarog.aimd@gao.gov

Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, 202-512-6240, brockj.aimd@gao.gov

Robert F. Dacey, Director, Consolidated Audit and Computer Security Issues (financial systems), Accounting and Information Management Division, 202-512-3317, daceyr.aimd@gao.gov

Henry Hinton, Assistant Comptroller General, National Security and International Affairs Division, 202-512-4300, hintonh.nsiad@gao.gov

Information Assurance Points of Contact:

Gene Dodaro, Assistant Comptroller General, Accounting and Information Management Division, 202-512-2600, dodarog.aimd@gao.gov

Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, 202-512-6240, brockj.aimd@gao.gov

Robert F. Dacey, Director, Consolidated Audit and Computer Security Issues (financial systems), Accounting and Information Management Division, 202-512-3317, daceyr.aimd@gao.gov

Henry Hinton, Assistant Comptroller General, National Security and International Affairs Division, 202-512-4300, hintonh.nsiad@gao.gov

Jean Boltz, Assistant Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, 202-512-5247, boltzj.aimd@gao.gov

Critical Infrastructure Protection Points of Contact:

Gene Dodaro, Assistant Comptroller General, Accounting and Information Management Division, 202-512-2600, dodarog.aimd@gao.gov

Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, 202-512-6240, brockj.aimd@gao.gov

Robert F. Dacey, Director, Consolidated Audit and Computer Security Issues (financial systems), Accounting and Information Management Division, 202-512-3317, daceyr.aimd@gao.gov

Henry Hinton, Assistant Comptroller General, National Security and International Affairs Division, 202-512-4300, hintonh.nsiad@gao.gov

Jean Boltz, Assistant Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, 202-512-5247, boltzj.aimd@gao.gov

On-Line Resources:

GAO Homepage: <http://www.gao.gov>

Missions and Functions:

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 of issues, such as information security, that relate to the effective and efficient implementation of those programs. Most of the reports and testimonies resulting from GAO's audits and evaluations are publicly available through GAO's website, www.gao.gov, or by calling (202) 512-6000. In addition, GAO develops audit guidance and conducts "best practices" studies of leading organizations to help identify solutions to deficiencies in federal operations.

Activities:

GAO has a broad strategy for improving federal information security that includes:

- Raising awareness of security issues among members of the Congress and senior federal executives
- Improving the quality of information security audits
- Identifying specific weaknesses at individual federal agencies and recommending corrective actions
- Promoting the best practices of leading organizations
- Working with the Congress and central management agencies to address security issues that affect multiple agencies.

Recent results of GAO's efforts pertaining to federal information security include the following:

- Through audits and evaluations, GAO continues to identify information security weaknesses across federal agencies and, in February 1997, designated information security as one of two government-wide high-risk areas. (The other was the Year 2000 conversion problem.) In September 1998, GAO issued a government-wide summary of these findings in a report entitled Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92).
- GAO has found that an underlying cause of federal security weaknesses is poor security program management. To identify solutions, GAO studied the practices of eight nonfederal organizations and published the results in an executive guide entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).
- GAO has developed a working draft of the Federal Information Systems Controls Audit Manual (GAO/AIMD-12.19.6), which provides a methodology for auditing computer-based controls at federal agencies.

Appendix B **Coordinating Activities**

APPENDIX B
COORDINATING ACTIVITIES

This page intentionally left blank.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
Critical Infrastructure Assurance Office (CIAO)	B-4
Federal Computer Security Program Managers' Forum (FCSPMF)	B-12
National Communications System (NCS).....	B-18
National Science and Technology Council (NSTC).....	B-24
National Security Telecommunications Advisory Committee (NSTAC).....	B-28
National Security Telecommunications and Information Systems Security	B-34
Committee (NSTISSC)	
Network Reliability and Interoperability Council (NRIC).....	B-38
President's Committee of Advisors on Science and Technology (PCAST).....	B-42
United States Security Policy Board (USSPB).....	B-46

Department of Commerce

**Critical Infrastructure
Assurance Office
(CIAO)**

Organization: Critical Infrastructure Assurance Office (CIAO)

Senior Critical Infrastructure Protection Official:

J. Hunker, Chief, Critical Infrastructure Assurance Office, 703-696-9395 ext. 209

Critical Infrastructure Protection Points of Contact:

S. Simens, Chief of Staff, Critical Infrastructure Assurance Office, 703-696-9395 ext. 257

On-Line Resources:

<http://www.ciao.gov/index.html>

Missions and Functions:

The Critical Infrastructure Assurance Office (CIAO) was established on May 22, 1998, by Presidential Decision Directive (PDD) 63. PDD-63, titled "Critical Infrastructure Protection," directed that a National Plan Coordination Staff be formed to assist in government and industry-wide efforts to implement the provisions of the PDD. The PDD also directed that the Transition Office of the President's Commission on Critical Infrastructure Protection form the basis of this staff, and that the staff become an office of the Department of Commerce in FY 1999. The mission of the CIAO is to:

- Integrate the various infrastructure sector plans into a National Infrastructure Assurance Plan
- Coordinate analyses and a remedial plan to mitigate the U.S. Government's own dependencies on critical infrastructures; including coordination of an expert review of these plans
- Coordinate legislative affairs to integrate infrastructure assurance issues into the current legal structure
- Coordinate public affairs to support PDD implementation
- Conduct analyses and studies to assist the National Coordinator in evaluating and promulgating infrastructure policies, programs, and initiatives
- Provide support, as requested by the National Coordinator, for summarizing key infrastructure assurance laws; identifying and compiling cyber and physical security standards; cataloging training programs; and reflecting model mutual aid agreements to assist state and local government and the private sector in protecting and restoring critical facilities
- Serve as Executive Secretariat to the interagency Critical Infrastructure Coordinating Group
- Provide administrative and operational support to the National Infrastructure Assurance Council
- Coordinate the preparation of annual and other reports to the President on the implementation of the directives in PDD-63.

Activities:

The CIAO has analyzed the Presidential Decision Directive on Critical Infrastructure Protection (PDD-63) and drafted six objectives from the document. They are as follows:

- Strategic Objective One: Promote a partnership between government and infrastructure owners and operators, beginning with increased information sharing relating to threats, vulnerabilities, and interdependencies.
 - Section Liaison Officials assisted by respective Sector Coordinators, will develop and implement a sector Vulnerability Education and Awareness Program.
 - The National Coordinator, Sector Liaison Officials, Sector Coordinators, Special Function Coordinators, and the National Economic Council representative, as appropriate, will consult with owners and operators to encourage creation of a private sector Information Sharing and Analysis Center (ISAC).
 - The National Coordinator, with the assistance of the Critical Infrastructure Coordinating Group and the National Economic Council, will identify possible methods of providing federal assistance to facilitate ISAC start-up.
 - The National Infrastructure Protection Center (NIPC) will be established to provide a national focal point for gathering information on threats to infrastructures; and, as a national warning center, will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. The NIPC will establish its own relations directly with others in the private sector and with any private sector-created ISAC entity.
 - The National Coordinator will commission studies on the following:
 - » Liability issues arising from participation by private sector companies in the information sharing process
 - » Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
 - » Necessity of document and information classification, its impact on useful dissemination, methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who would misuse it.
 - » The improved protection, including secure dissemination/information handling systems, of industry trade secrets and other confidential business, data, law enforcement information and evidential material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, is unwise to disclose.
- Strategic Objective Two: Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs.

- Lead Agencies will designate Sector Liaison Officials, and will work with the private sector to identify Sector Coordinators to address infrastructure issues, and recommend components of the National Infrastructure Assurance Plan.
- Functional Agencies will designate respective Functional Coordinators.
- A Critical Infrastructure Coordinating Group, including Sector Liaison Officials and Functional Coordinators will be established to provide interagency coordination of infrastructure issues.
- A high-level National Infrastructure Advisory Council will be established to advocate infrastructure protection and advise the President as appropriate.
- All Government departments and agencies will appoint a Chief Information Officer/Chief Information Assurance Officer.
- Principals Committee, in coordination with National Coordinator, will submit a schedule for completing a National Infrastructure Assurance Plan, within 180 days.
- Develop a system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.
- Establish a system to reconstitute minimum required capabilities rapidly, for varying levels of successful infrastructure attacks.
- The Department of Defense will retain Executive Agent responsibilities for the National Communications System and support of the National Security Telecommunications Advisory Council.
- The National Coordinator will participate as a full member of the Deputies Committee or Principals Committee meetings when infrastructure issues are considered, to ensure interagency coordination for policy development and implementation.
- The National Coordinator will review crisis management activities concerning infrastructure events with significant foreign involvement and provide budgetary advice for critical infrastructure protection.
- The National Security advisor will appoint a Senior Director for Infrastructure Protection on the National Security Council staff.
- The National Plan Coordination Staff will integrate sector plans into National Infrastructure Assurance Plan and coordinate analyses of the US Government's own dependencies on critical infrastructures.
- Effective in fiscal year 1999, the National Plan Coordination Staff will become an office of the Department of Commerce.
- The Office of Personnel Management will provide necessary assistance to facilitate National Plan Coordination Office operations.
- The Intelligence Community will develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber and information warfare threat.
- The National Coordinator, in coordination with Office of Management and Budget, will evaluate the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, in order to make ameliorative recommendations to the President.

- Strategic Objective Three: Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.
 - Establish Vulnerability Awareness and Education Programs within both the government and the private sector.
 - The White House, under National Coordinator oversight, with relevant Cabinet agencies, shall consider a series of conferences for education and awareness.
 - The National Academy of Science and the National Academy of Engineering will consider a round table of federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.
 - The Intelligence Community and Law Enforcement community will expand existing programs for briefing infrastructure owners and operators and senior government officials.
 - The National Coordinator, in coordination with the private sector, will launch a continuing national awareness campaign, emphasizing improving infrastructure security.

- Strategic Objective Four: Initiate a series of best practices as well as information security management activities and related programs demonstrating government leadership.
 - Conduct vulnerability analyses for each sector of the economy and each sector of the government, followed by periodic updates and a determination of the minimum essential infrastructure in each sector. A recommended remedial plan will be completed based upon vulnerability assessments.
 - The National Plan Coordination staff will help coordinate a national education and awareness program, legislative affairs, and public affairs.
 - The National Coordinator will establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign.
 - The Department of Commerce, the General Services Administration, and the Department of Defense will assist federal agencies in the implementation of best practices for information assurance within their individual agencies.
 - The Department of Transportation, in conjunction with the Department of Defense, will undertake an evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System, assessing risks to civilian users of Global Positioning System-based systems.
 - The Federal Aviation Administration will develop and implement a comprehensive National Airspace System (NAS) security program to protect and modernize NAS from information-based or other disruptions and attacks.
 - All federal agencies will designate representatives who may authorize access to their computer systems to facilitate vulnerability and red-teaming analyses.
 - The National Coordinator will coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.
 - The National Coordinator will commission a study on the potential benefit of security standards for mandating, subsidizing, or otherwise assisting in the

provision of insurance for selected critical infrastructure providers; and, requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the US.

- The National Coordinator and the National Infrastructure Advisory Council, will propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.
 - The Department of Commerce and the Department of Defense will work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.
 - The National Coordinator will coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.
 - The National Coordinator will provide annual reports on the progress of the Presidential Decision Directive, and in the year 2000, conduct a zero-based review of infrastructure protection issues.
- Strategic Objective Five: Evaluate the Executive Branches legislative authorities and budget priorities regarding critical infrastructure, and make recommendations as necessary.
 - Establish a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.
 - The National Coordinator will commission a study on implications of sharing information with foreign entities where such sharing is deemed necessary to the security of US infrastructures.
 - The Intelligence Community will elevate and formalize priority for enhanced collection and analysis of information on the foreign cyber and information warfare threat.
 - The Federal Bureau of Investigation, the Secret Service, and other appropriate agencies will recruit undergraduate and graduate students with relevant technical skills; and facilitate the hiring and retention of qualified analytic and investigatory personnel.
 - The Department of Justice will establish legal guidelines to facilitate vulnerability assessments of US Government entities.
 - Identify large procurements related to infrastructure assurance, studying the procurement process for infrastructure protection issues and proposing revisions where required.
 - The Office of Management and Budget will direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Review Act.
 - The Departments of Justice and Treasury will sponsor a study compiling demographics of computer crime, comparing state approaches to computer crime, and developing ways to deterring and responding to computer crime by juveniles.

- Strategic Objective Six: Increase investment in infrastructure assurance research. Coordinate Federally-sponsored research and development with private sector research, and ensure adequate funding to minimize our vulnerabilities on a rapid but achievable timetable.
 - The Office of Science and Technology (OSTP), through the National Science and Technology Council, will coordinate research and development efforts among department and agencies in support of infrastructure protection. A research and development agenda, subject to multi-year planning and taking into account private sector research, will be developed to manage funding and minimize vulnerabilities on a rapid but achievable timetable.
 - As soon as possible, develop and deploy an enhanced system for detecting and analyzing cyber attacks, with maximum possible participation of the private sector.
 - Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.

This page intentionally left blank.

**Federal Computer Security Program
Managers' Forum
(FCSPMF)**

Organization: Federal Computer Security Program Managers' Forum (FCSPMF)

Information Assurance Point of Contact

Marianne Swanson, National Institute of Standards and Technology, Acting Chair,
301-975-3293

On-Line Resources:

Mission and Functions:

The Federal Computer Security Program Managers' Forum is an informal group sponsored by the National Institute of Standards and Technology (NIST) to promote the sharing of computer security information among federal agencies. The Forum discusses current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems [except "Warner Amendment" systems, as defined in 44 USC 3502 (2)].

The objectives of this group are:

- To provide an ongoing opportunity for managers of federal computer security programs to exchange computer security materials and information of use to other programs in a timely manner, build upon the experiences of other programs, and reduce possible duplication of effort.
- To provide an organizational mechanism for NIST to exchange information directly with federal agency computer security program managers in fulfillment of its leadership mandate under the Computer Security Act of 1987.
- To establish and maintain relationships with other individuals or organizations that are actively addressing computer security issues within the federal government.
- To establish and maintain a strong proactive stance identifying and resolving strategic and tactical computer security issues involved in the development and application of new and emerging information technologies.

Membership includes the following organizations:

- Department of Agriculture
 - Farm Service Agency
 - Food & Safety Inspection Service
 - U.S. Forest Service
- Department of Commerce
 - Bureau of the Census
 - National Oceanographic & Atmospheric Administration
 - National Institute of Standards and Technology
 - National Technical Information Service
 - National Telecommunications & Information Administration
 - Patent and Trademark Office

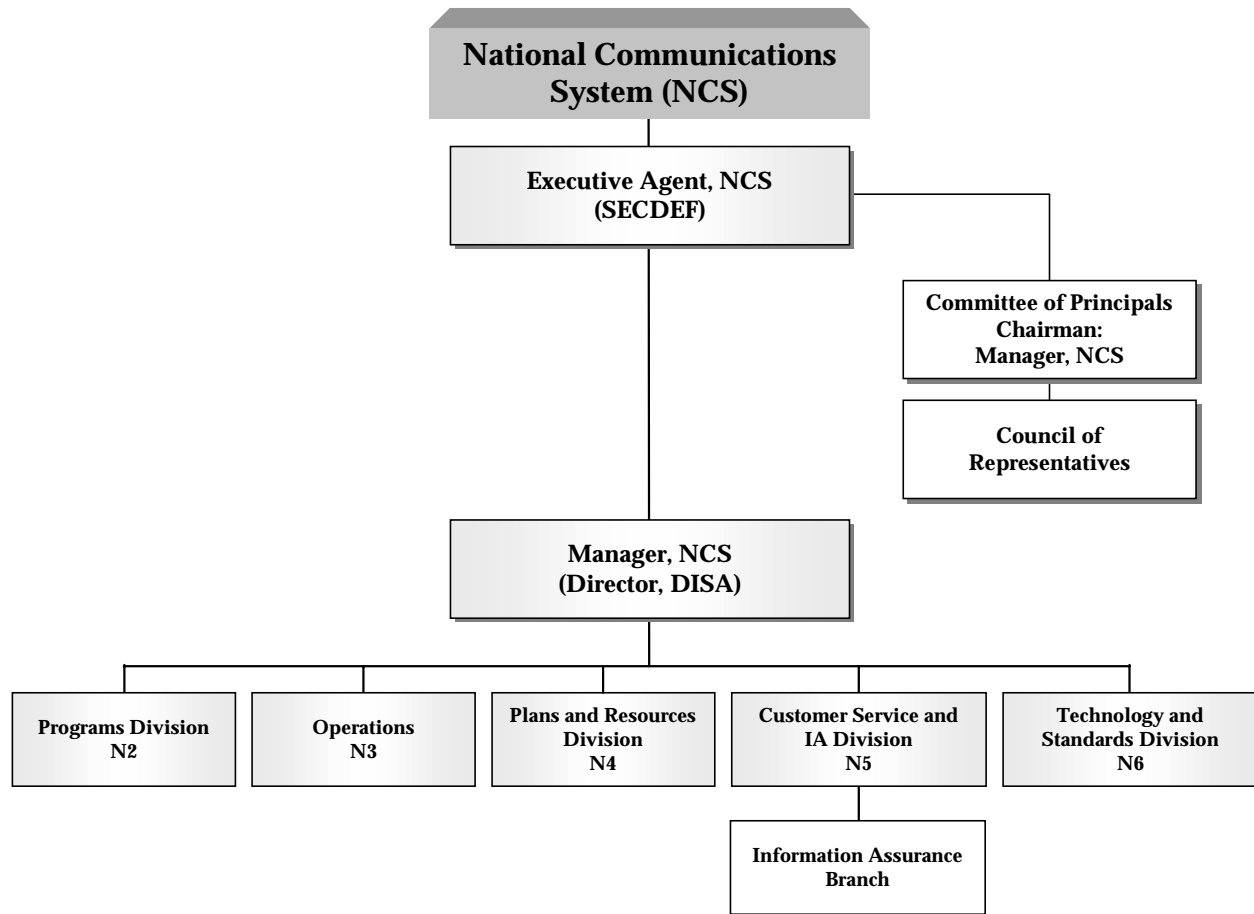
- Congress
 - General Accounting Office
 - Library of Congress
 - U.S. House of Representatives
 - U.S. Senate
- Department of Defense
- Ballistic Missile Defense Organization
- Defense Information Systems Agency
- Defense Investigative Organization
- National Security Agency
- U.S. Air Force
- Department of Education
- Department of Energy
- Equal Employment Opportunity Commission
- Environmental Protection Agency
- Executive Office of the President
- Export-Import Bank
- Farm Credit Administration
- Federal Communications Commission
- Federal Deposit Insurance Corporation
- Federal Emergency Management Agency
- Federal Maritime Commission
- Federal Reserve System
- General Services Administration
- Department of Health & Human Services
 - Administration for Children & Families
 - Agency for Health Care Policy & Research
 - Centers for Disease Control and Prevention
 - Food and Drug Administration
 - Health Care Financing Administration
 - Health Resources & Services Administration
 - Indian Health Service
 - National Institutes of Health
 - Substance Abuse and Mental Health Services
- Department of Housing & Urban Development
- Department of Interior
- Department of Justice
 - Federal Bureau of Investigation
 - Immigration & Naturalization Service
- Department of Labor
 - Bureau of Labor Statistics
 - Employment & Training Administration
 - Employment Standards Administration

- Occupational Safety & Health Administration
- Office of the Solicitor
- Pension & Welfare Benefits Administration
- Veterans Employment & Training Administration
- National Aeronautics & Space Administration
- National Labor Relations Board
- National Science Foundation
- Nuclear Regulatory Commission
- Office of Personnel Management
- Securities & Exchange Commission
- Small Business Administration
- Social Security Administration
- Department of State
- Department of Transportation
 - Federal Aviation Administration
 - Federal Highway Administration
 - Federal Transit Administration
 - Maritime Administration
 - National Highway Traffic Safety Administration
 - Office of the Secretary
 - Research & Special Programs Administration
 - U.S. Coast Guard
- Department of the Treasury
 - Bureau of Alcohol, Tobacco & Firearms
 - Bureau of Engraving & Printing
 - Bureau of Public Debt
 - Financial Crimes Enforcement Network
 - Financial Management Service
 - Internal Revenue Service
 - Office of Security
 - Office of the Comptroller of the Currency
 - Office of the Inspector General
 - Office of Thrift Supervision
 - U.S. Customs Service
 - U.S. Mint
 - U.S. Secret Service
- U.S. Information Agency
- U.S. International Development Cooperation Agency
- U.S. Supreme Court
- Department of Veterans Affairs

Activities:

- Half-day meetings of the Forum are held bi-monthly in the Washington, DC area (often at the NIST campus in Gaithersburg, Maryland).
- Forum meetings typically include briefings on topics of general interest to the federal community and provide time for informal sharing of information (e.g., incidents) and requests for assistance regarding the security of federal systems.
- The forum holds a two-day off-site meeting to concentrate on current security issues.

This page intentionally left blank.



Organization: National Communications System (NCS)

Senior Information Operations Official:

LTG, David J. Kelly, USA, Manager, NCS

Information Assurance Points of Contact:

Mr. Jim Kerr, Chief, Information Assurance Branch, 703-607-6133, kerrj@ncs.gov

Critical Infrastructure Protection Points of Contact:

Mr. Jim Kerr, Chief, Information Assurance Branch, 703-607-6133, kerrj@ncs.gov

On-Line Resources:

NCS Homepage: <http://www.ncs.gov>

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.

Members:

- 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.

The work of the NCS is carried out by a Committee of Principals (COP) and a Council of Representatives (COR). The Committee of Principals is a Presidentially designated interagency group that provides advice and recommendations on NS/EP telecommunications to the Executive Office of the President. The Council of Representatives is a working level forum of the COP. The COP and the COR are composed of high-level government officials representing Federal operational, policy, regulatory, and enforcement organizations. Its diverse representation across 23 Federal departments and agencies embraces the full spectrum of Federal telecommunications assets and responsibilities. As an interagency group, it serves as a forum for members to review, evaluate, and present views and recommendations on current or prospective NCS programs to the Manager, the Executive Agent, and the Executive Office of the President (EOP). The COR was established by the COP as a permanent, subordinate working group to assist the COP in researching and developing complex NS/EP telecommunication issues.

Activities:

Some of the key NCS programs include the following.

- *Government Emergency Telecommunications Service (GETS)*. GETS supports NS/EP telecommunications users with priority switched voice and voice band data service in the public switched network (PSN). Developed in response to White House tasking, GETS provides authenticated access, enhanced routing, and priority treatment in local and long-distance telephone networks. Users access GETS through a simple dialing plan and personal identification number (PIN).

GETS is designed for, and maintained in, a constant state of readiness to make maximum use of all available commercial and Government telephone resources if outages occur from congestion or damage during an emergency, crisis, or war.

Users access GETS by dialing a universal access number (1-710-NCS-GETS) using such common telephone equipment as standard desk set, secure telephone unit, facsimile,

modem, or cellular phone. A tone prompts the user to enter a PIN, and a voice prompt requests the destination telephone number. Once the system authenticates the caller as a valid user, the call becomes an NS/EP call and receives enhanced routing and priority treatment throughout the PSN.

- *Cellular Priority Access Service (CPAS)*. CPAS is being accomplished in response to White House direction resulting from NSTAC recommendations. Several recent natural disasters illustrate the importance of cellular technology in providing timely emergency telecommunications for Federal, State, and local users at a disaster site or mobile responders under a stressed environment. However, increased personal use of cellular communications often created network congestion and high levels of call blocking to critical disaster relief officials when they need communications. As a result, the OMNCS, working with industry leaders, industry associations, State representatives, and standard bodies, developed the CPAS specification. CPAS aims to facilitate and coordinate the development of a cost-effective, uniform, nationwide CPAS capability that enhances NS/EP user access to the PSN.

The Cellular Priority Service (CPS) Program is working on the following activities leading toward the implementation of a cellular priority capability that enhances NS/EP access to the PSN: standards, administration, regulatory, and technical aspects of implementation.

- *Advanced Intelligent Network (AIN)*. AIN is an emerging telecommunications technology identified by the President's NSTAC and the OMNCS as having the potential capability to meet the NS/EP telecommunications needs of NCS member organizations.

AIN technology supports a telecommunications architecture consisting of signaling systems, switches, computer processors, databases, and transmission media. The convergence of these elements allows for customized software-denied network services that can be flexibly, rapidly, and cost effectively configured to meet changing customer needs. Among other capabilities, AIN provides priority recognition, user authentication, enhanced routing, and network management alternatives in support of NS/EP contingency operations.

In the competitive market environment ushered in by the *Telecommunications Act of 1996*, PSN carriers are becoming increasingly dependent on AIN capabilities to deliver services to their customers. Carriers are using AIN to deploy local number portability, as mandated by the FCC, to open networks to new third-party service providers, and to meet customer demand for new service capabilities (e.g., mobility, data, and Internet access). Because AIN has become a vital component of the PSN, the OMNCS must determine its reliability and availability to support NS/EP communications.

- *National Coordinating Center for Telecommunications*. The NCC is an industry-Government organization that assists in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services and facilities.

The commercial telecommunications industry has the majority of telecommunications assets, including the facilities, equipment, and personnel trained to restore NS/EP services. These assets are the primary resources for the NCC. Industry personnel located in the NCC are in direct contact with their companies' senior management and field counterparts. The NCC also collects information about Government-owned systems from Government representatives to the NCC. Industry can route information and requests for assistance to Government or vice versa depending on the scenario.

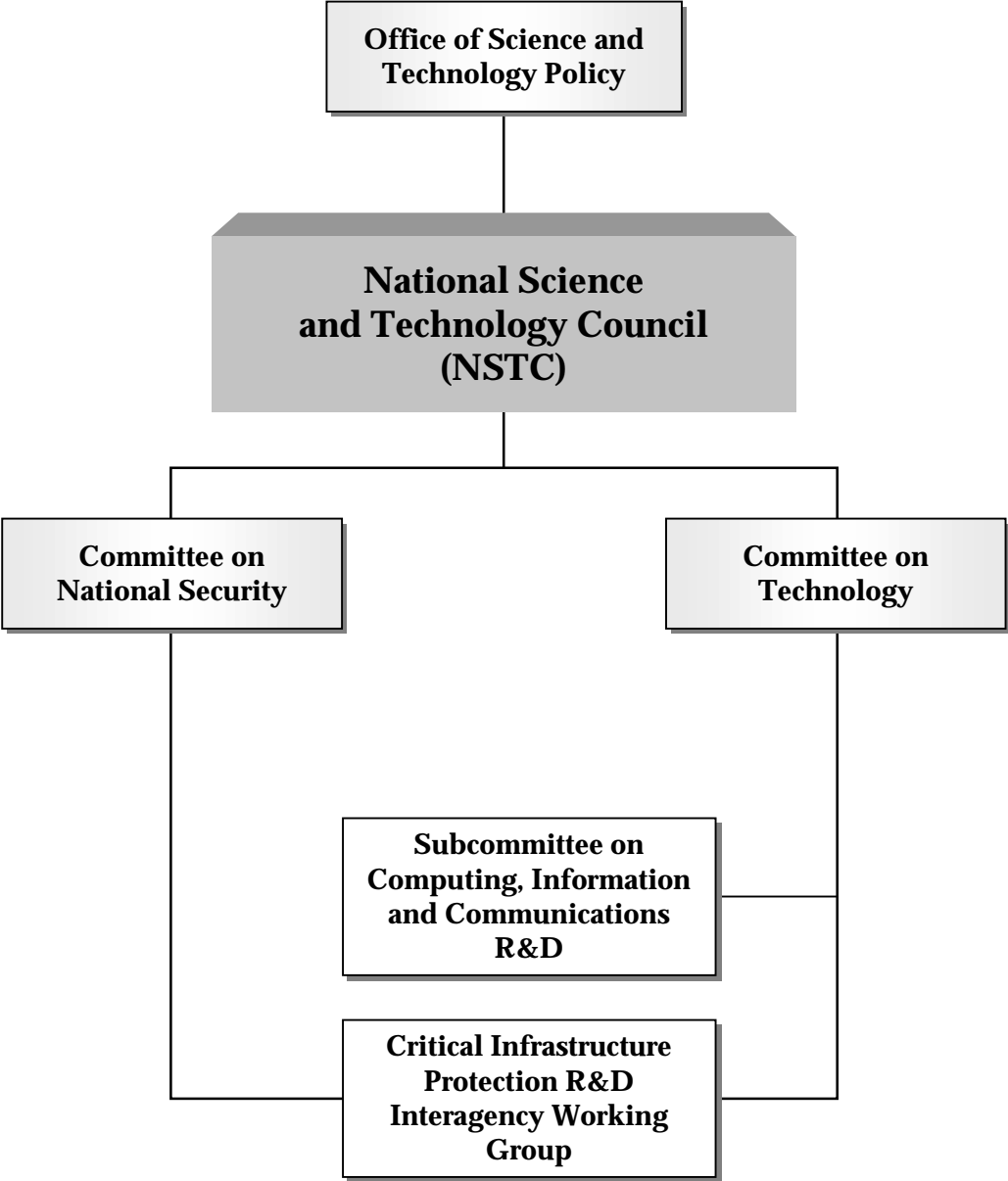
The National Coordinating Center recently conducted a 120-day pilot Indications, Assessment, and Warning (IAW) effort. This first-ever computer incident reporting effort involved all industry and government members of the NCC and was designed primarily to test procedures and develop trust among the reporting entities and the NCC. The voluntary effort was designed to complement the DOD and Federal government reporting activities. NCC members are currently addressing the lessons learned from the pilot effort and have converted the pilot effort into an on-going activity. Members of the NCC are also exploring information sharing concepts and procedures with the National Infrastructure Protection Center. The NCC also serves as the alerting mechanism for NS/EP situations.

- *Telecommunications Service Priority (TSP) System.* The TSP System continues to facilitate the priority provisioning and restoration of NS/EP telecommunications services. During FY97, the Office of Priority Telecommunications (OPT) (formerly the TSP Program Office) received a weekly average of 220 requests for TSP assignments. Priority provisioning of telecommunications services was critical in supporting relief efforts following flooding in the Northwest, Kentucky, and the Red River areas, and other regions nationwide that experienced heavy rains and flooding.
- *Telecommunications Electric Service Priority (TESP).* The U.S. Government telecommunications policy is to meet NS/EP requirements and supply adequate and secure electric energy to critical telecommunications facilities. In 1987, the Department of Energy (DOE), in coordination with the NCS and the Energy Task Force of the President's NSTAC, developed the TESP initiative.

Essential national defense and civilian requirements may not be met if an event disrupts electric supplies to critical telecommunications facilities. Electric utilities have systems and processes in place for restoring electric service to specific customers in the event of threatened or actual electric power supply emergencies. Before TESP, the existing priority restoration systems reflected only essential State and local needs. The TESP Program promotes modification of the existing electric utility emergency priority restoration systems to include telecommunications facilities considered critical to NS/EP.

Currently, 239 telecommunications service providers and 475 electric utilities support the TESP Program. As of June 1997, the total number of telecommunications facilities exceeded 3,200.

- *Communications Resource Information Sharing (CRIS)*. The CRIS initiative continues to support NS/EP requirements. It establishes an information source that provides resource points of contact, associated communications resources, and supporting information for use by the participating NCS member organizations. Today, 26 Federal and industry organizations contribute more than 40 communications assets, services, and capabilities that could be shared with other Federal departments and agencies during emergencies.



Organization: National Science and Technology Council (NSTC)

Senior Information Operations Official:

Dr. Colleen N. Hartman, Senior Policy Analyst, Office of Science and Technology Policy,
202-456-6104, chartman@ostp.eop.gov

Information Assurance Points of Contact:

Dr. Steven Rinaldi, Office of Science and Technology Policy, 202-456-6057,
srinaldi@osotp.eop.gov

Critical Infrastructure Protection Points of Contact:

Dr. Steven Rinaldi, Office of Science and Technology Policy, 202-456-6057,
srinaldi@osotp.eop.gov

On-Line Resources:

Homepage:

http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html

Missions and Functions:

President Clinton established the National Science and Technology Council (NSTC) by Executive Order 12881 in November 1993. The NSTC is a cabinet-level council that coordinates R&D policies and activities across the federal agencies. It consolidates the responsibilities previously carried out by a number of interagency councils, including the Federal Coordinating Council for Science, Engineering, and Technology, the National Space Council, and the National Critical Materials Council.

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 aimed at accomplishing multiple national goals.

The major functions of the NSTC are to:

- Coordinate the formulation of S&T policy
- Ensure S&T policy decisions and programs are consistent with the president's stated goals
- Help implement and integrate the president's S&T policy agenda across the Federal government

- Ensure S&T are considered in the development and implementation of all Federal policies and programs
- Further international cooperation in S&T.

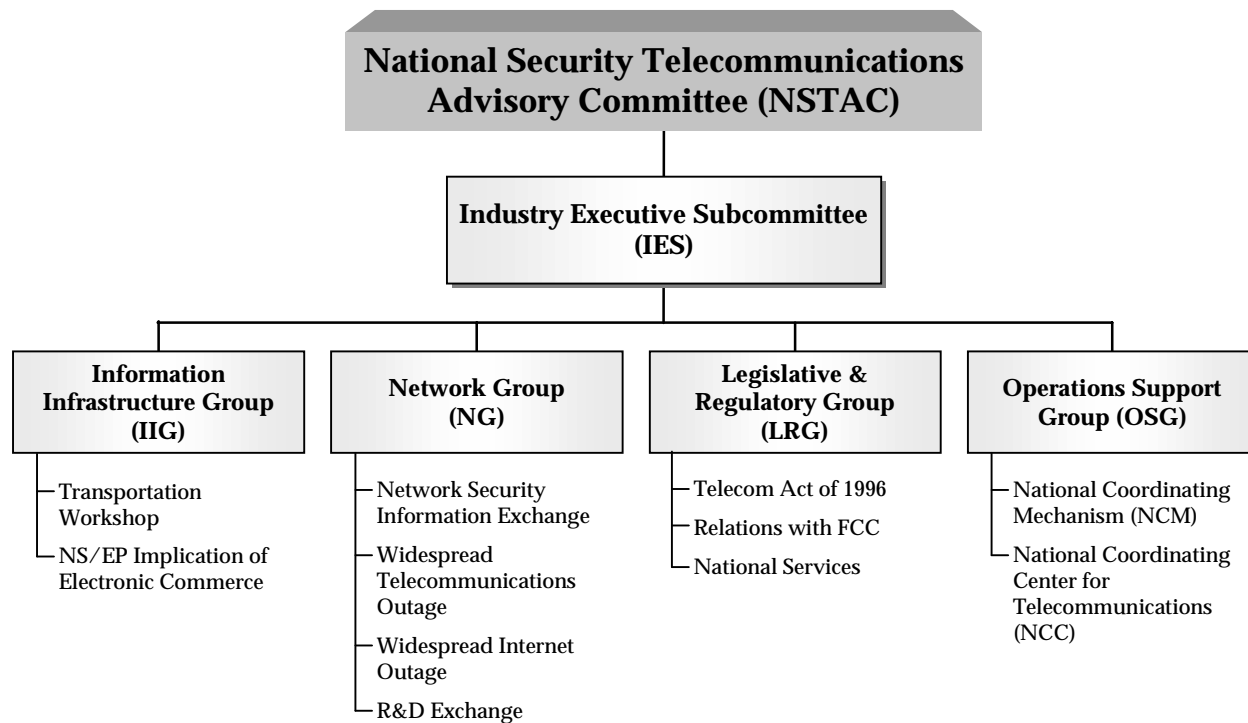
Members:

- The President
- The Vice President
- Secretary of State
- Secretary of the Treasury
- Secretary of Defense
- Secretary of the 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
- Secretary of Veterans Affairs
- Administrator, Environmental Protection Agency
- Director, Office of Management and Budget
- Chair, Council of Economic Advisors
- Director, Central Intelligence Agency
- Assistant to the President for National Security Affairs
- Assistant to the President for Science and Technology
- Assistant to the President of Domestic Policy
- Assistant to the President of Economic Policy
- Director, Arms Control and Disarmament Agency
- Administrator, National Aeronautics and Space Administration
- Director, National Science Foundation
- Director, National Institutes of Health

Activities:

For activities, contact the Point of Contact or visit the on-line resource.

This page intentionally left blank.



Organization: National Security Telecommunications Advisory Committee (NSTAC)

Senior Information Operations Official:

Mr. Van B. Honeycutt, President and CEO, Computer Sciences Corporation is the current Chairman of the NSTAC.

Information Assurance Points of Contact:

Marilyn Witcher, Branch Chief, Customer Service Office, 703-607-6214, witcherm@ncs.gov

Critical Infrastructure Protection Points of Contact:

Mr. Jim Kerr, Chief, Information Assurance Office, NCS, 703-607-6133, kerrj@ncs.gov

On-Line Resources:

<http://www.ncs.gov>

Missions and Functions:

The NSTAC is a Presidential Advisory Committee that was established in September of 1982 to provide advice and expertise to the President and the Executive Agent, NCS, on issues and problems related to implementing NS/EP telecommunications policy. The NSTAC consists of up to 30 senior corporate leaders representing major telecommunications-related industries, who constitutes an opportunity for Federal departments and agencies to tap into a vast amount of telecommunications expertise. The NSTAC's Industry Executive Subcommittee (IES), and the IES subgroups analyze NS/EP telecommunications issues and report their findings to the NSTAC to advise the President. Because the NCS serves as the focal point for joint industry/Government planning, the NSTAC and NCS have developed a close partnership.

Members of the NSTAC include Chairmen, CEOs, Presidents, and COOs of the following companies:

- Advanced Digital Technologies Company (ADTC)
- AT&T
- BankAmerica Corporation
- Computer Sciences Corporation (CSC)
- COMSAT Corporation
- Electronic Data Systems (EDS)
- Executive Security & Engineering Technologies, Inc. (ESET)
- GTE Corporation
- Hughes Electronics Corporation
- ITT Industries, Incorporated

- Lockheed Martin Corporation
- MCIWorldCom
- Motorola, Incorporated
- National Telecommunications Alliance, Inc. (NTA)
- Nortel
- Raytheon Company
- Rockwell International Corporation
- Science Applications International Corporation (SAIC)
- Sprint Corporation
- Teledesic Corporation
- The Boeing Company
- TRW, Incorporated
- U.S. West, Incorporated
- Unisys Corporation
- United States Telephone Association (USTA)

Activities:

- The Information Infrastructure Group (IIG) has concentrated their efforts on issues related to information assurance, infrastructure protection, electronic commerce, and cyber security. The IIG established two subgroups to investigate these topics, the Transportation Information Infrastructure Risk Assessment Subgroup and the Electronic Commerce (EC)/Cyber Security Subgroup.
- The Transportation Information Infrastructure Risk Assessment Subgroup conducted a workshop for the transportation industry on telecommunications and information systems dependencies on September 10, 1997. On the basis of findings from that event, the subgroup submitted an interim report to the December 1997 NSTAC XX meeting. The report recommended that more information be gathered, particularly in the area of intermodal transportation, and concluded that broader participation from the transportation industry was desirable. The subgroup anticipates completing the risk assessment in the beginning of the NSTAC XXII cycle.
- The EC/Cyber Security Subgroup was established in response to a briefing the Deputy Secretary of Defense gave at the December 1997 NSTAC XX meeting. The subgroup agreed to examine national security and emergency preparedness (NS/EP) implications of EC as both industry and Government incorporate EC into their business practices. After meeting with key officials in industry and Government on security issues related to EC, the subgroup developed an issue paper that focused on one aspect of EC-cyber security training and forensics. That paper centers on the importance of industry and Government cooperation in addressing cyber security. The subgroup is also developing further analyses of EC to be completed in preparation for the NSTAC XXII meeting.

- The Legislative and Regulatory Group (LRG) continues to examine the implementation of the Telecommunications Act of 1996 (Telecom Act) and other legislative, regulatory, and judicial actions for their potential impact on national security and emergency preparedness (NS/EP) telecommunications based on a framework for analysis it established in 1997.

In addition to monitoring the implementation of the Telecom Act, the IES tasked the LRG to address several other issues following NSTAC XX.

- The LRG also examined options for enhancing communication on NS/EP telecommunications matters between and among industry, the Federal Communications Commission (FCC), and other relevant Government organizations. Numerous discussions with National Communications System (NCS), FCC, and Office of Science and Technology Policy (OSTP) staff prompted the LRG to develop procedural guidelines to help telecommunications carriers and the FCC restore critical emergency telecommunications services in a timely manner.
 - The LRG formed a National Services subgroup, which developed a forward-looking analytical approach to help the Government and the telecommunications industry, including the NSTAC and its subordinate groups, address the potential effects of emerging National Services on NS/EP telecommunications. The subgroup's analytical approach formed the basis of a white paper to facilitate public awareness of selected NS/EP-critical telecommunications functions and promote the continued consideration of NS/EP telecommunications requirements by Government and the telecommunications industry during the National Services planning process.
 - Finally, the LRG reviewed the legislative and regulatory recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) for their potential implications for NS/EP telecommunications. The LRG's analysis revealed that many of the PCCIP's legal and regulatory recommendations were consistent with previous NSTAC work and recommendations. Also, the LRG conducted a preliminary analysis of a Presidential Decision Directive on critical infrastructure protection (PDD-63), which built on the PCCIP's recommendations. Concerns raised by the LRG regarding the lack of specific roles for the NSTAC and the NCS in the Administration's new infrastructure protection policy framework were communicated to the IES.
- In collaboration with Purdue University's Computer Operations, Audit, and Security Technology Laboratory (COAST), the Institute of Electrical and Electronics Engineers (IEEE), and the Office of Science and Technology Policy (OSTP), the Network Group conducted a network security R&D exchange in October 1998. The R&D Exchange addressed the growing convergence of telecommunications and the Internet and methods for improving the collaboration among Government, industry, and academia on their R&D efforts.
 - In June 1998, the Government and NSTAC Network Security Information Exchanges sponsored a workshop on the insider threat to information systems. The workshop offered an overview of the emerging insider threat and suggested measures organizations could take to reduce their vulnerability to it. The NSIEs developed two

white papers to provide background material for the workshop and are developing an after action report reflecting the insights that emerged from the workshop discussion so this material can be shared with a broader audience.

- Following discussion at NSTAC XX, the Network Group began to examine how NS/EP operations might be affected by Internet failures over the next three years. The NG has approved an outline for its Internet report and is currently gathering data on the Internet's architecture, its vulnerabilities, and how the Internet will be used to support NS/EP operations. The report will be provided to NSTAC at its next meeting, in the summer of 1999.
 - The Widespread Outage report was also a topic of discussion at NSTAC XX. The Widespread Outage Subgroup was asked to re-examine the conditions that may contribute to a widespread telecommunications outage and subsequently developed conclusions to provide to NSTAC XXI.
 - The Network Group also examined the status of efforts to address the Year 2000 (Y2K) problem and prepare the telecommunications infrastructure for the millennium change, factors that may affect those efforts, and problems that may result if those efforts are not fully effective. The NG will continue to monitor the Y2K readiness of the telecommunications infrastructure as test results become available, and provide its insight on this matter, through NSTAC, to the President.
- The President's National Security Telecommunications Advisory Committee's (NSTAC) Operations Support Group (OSG) was formed in April 1997 to evaluate the overall progress and direction of national security and emergency preparedness (NS/EP) operational activities. Among its specific taskings, the OSG was instructed to refine NSTAC's national coordinating mechanism (NCM) concept and develop standardized intrusion incident information reporting criteria for the National Coordinating Center for Telecommunications (NCC). Two OSG subgroups, the NCC Vision-Operations Subgroup and the NCM Subgroup, addressed these actions respectively. This report presents the charge, activities, analysis, conclusions, and recommendations of the OSG and its two subgroups.
 - An NCM process would provide senior Federal Government decision makers with real-time information from related components of critical national infrastructures to enhance NS/EP. In May 1998, the President released Presidential Decision Directive (PDD)-63, a critical infrastructure protection directive establishing the National Infrastructure Protection Center (NIPC) and calling for industry to voluntarily participate in the Government's efforts to ensure the security of the Nation's infrastructures. In a series of meetings with Government officials from the President's Commission on Critical Infrastructure Protection Transition Team and the NIPC, members of the Industry Executive Subcommittee and the NCM Subgroup shared their NCM concept, describing how a virtual information sharing process based on the NCM concept and the NCC could be established. PDD-62 was also issued in May 1998 establishing a structure for overseeing a wide range of Government agency policies and programs to defeat terrorism.

- The IES approved the NCC Vision-Operations Subgroup’s *NCC Intrusion Incident Reporting Criteria and Format Guidelines* in May 1998 for use in the NCC’s 120 day-long electronic intrusion incident information processing pilot. The NCC officially began the pilot program in June 1998 for processing reports from industry and Government service providers and network operators regarding public network electronic intrusions.
- 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. There are ten agencies represented on the government NSIE and 20 companies represented on the NSTAC NSIE. 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. Exhibit B-1 illustrates the entities that were created to facilitate this sharing of information.

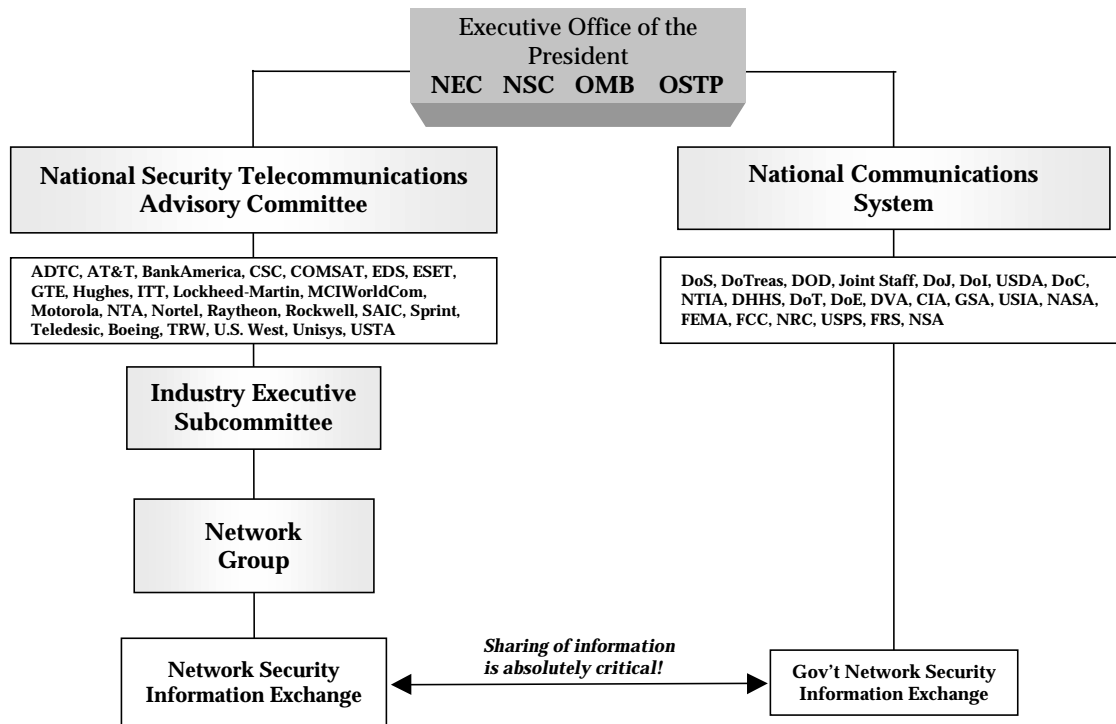
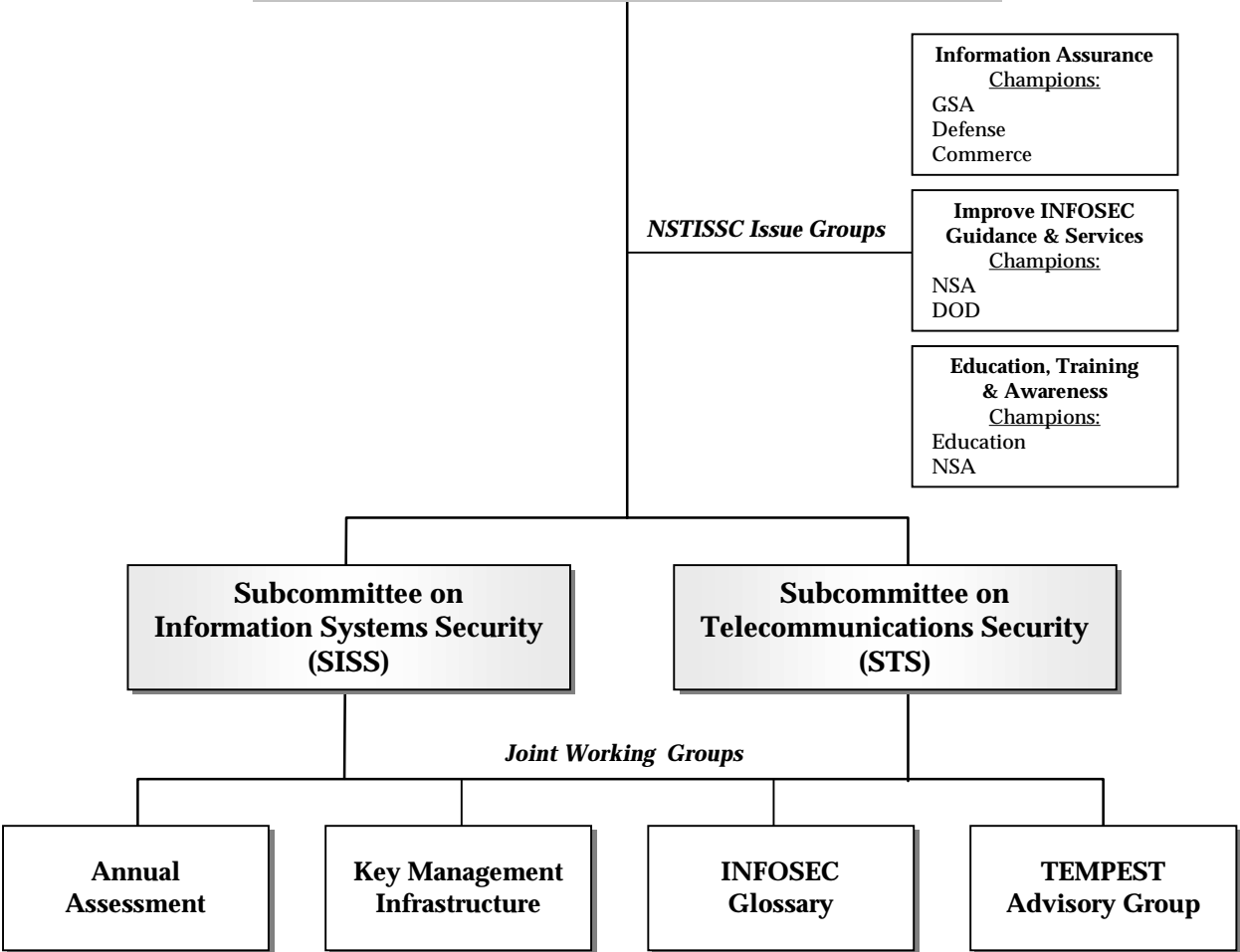


Exhibit B-1. NSTAC-NCS Model for Sharing Sensitive Information

**National Security Telecommunications
and Information Systems Security
Committee (NSTISSC)**



Organization: National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Senior Information Operations Official:

Daniel J. Knauf, Executive Secretary, 410-854-6906

Information Operations Points of Contact:

Elaine L. Gist, Secretariat Manager, 410-854-6906

On-Line Resources:

NSTISSC Homepage: <http://www.nstissc.gov>

Missions and Functions:

The NSTISSC was established by National Security Directive 42 (NSD 42), issued on 5 July 1990. Predecessor organizations to the NSTISSC have existed since 1952 under various names: the U.S. Communications Security (COMSEC) Board (USCSB), the National COMSEC Committee (NCSC), and just prior to the NSTISSC, the National Telecommunications and Information Systems Security Committee (NTISSC).

The NSTISSC provides a forum for discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems through the NSTISSC Issuance System. National security systems include the following: (1) systems that process classified information or information involving intelligence activities; (2) cryptologic activities related to national security, command and control of military forces; and (3) equipment that is an integral part of a weapon or weapon system(s) or is critical to the direct fulfillment of military or intelligence missions.

The NSTISSC is composed of members from 21 U.S. Government executive branch departments and agencies, as well as observers representing ten additional agencies. The Committee is chaired by the Senior Civilian Official for the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I).

NSD 42 established two subcommittees under the NSTISSC: the Subcommittee on Telecommunications Security (STS), which is chaired by Thomas R. Burke, GSA, and the Subcommittee on Information Systems Security (SISS), which is chaired by John C. Davis, the Director of the National Computer Security Center at the National Security Agency.

Much of the work of the NSTISSC is accomplished by Committee-level Issue Groups and Subcommittee Working Groups. Currently operating are three NSTISSC Issue Groups: (1) Information Assurance, (2) Improve INFOSEC Guidance & Services, and (3) Education, Training & Awareness. Four Subcommittee Working Groups are also operating:

(1) Annual Assessment, (2) Key Management Infrastructure, (3) INFOSEC Glossary, and (4) the TEMPEST Advisory Group.

The Committee is responsible for:

- Developing and issuing National policy and standards
- Developing and issuing guidelines, instructions, advisory memoranda, technical bulletins, incident reports, and special reports
- Assessing the “health” of national security systems
- Approving release of INFOSEC products and information to foreign governments
- Creating and maintaining national issuance system; establishing and maintaining
- Liaisons/partnerships with other security fora.

The NSTISSC is composed of members from 21 U.S. Government executive branch departments and agencies, as well as observers representing nine additional agencies. The Committee is chaired by the Assistant Secretary of Defense for Command, Control, Communication and Intelligence (ASD C³I).

- The Secretary of State
- The Secretary of the Treasury
- The Secretary of Defense
- The Attorney General
- The Secretary of Commerce
- The Secretary of Transportation
- The Secretary of Energy
- Director, Office of Management and Budget
- Assistant to the President for National Security Affairs
- Director of Central Intelligence
- Chairman of the Joint Chiefs of Staff
- Director, Federal Bureau of Investigation
- Director, Federal Emergency Management Agency
- Administrator, General Services Administration
- The Chief of Staff, United States Army
- The Chief of Naval Operations
- The Chief of Staff, United States Air Force
- Commandant, United States Marine Corps
- Director, National Security Agency
- Manager, National Communications System
- Director, Defense Intelligence Agency.

The NSTISSC is also composed of nine observers:

- Defense Information Systems Agency
- U.S. Department of Education

- Federal Communications Commission
- National Aeronautics Space Administration
- National Imagery and Mapping Agency
- National Institute of Standards and Technology
- U.S. Nuclear Regulatory Commission
- Chairman, Subcommittee on Information Systems Security
- Security Policy Board Staff.

Activities:

For activities, contact the Point of Contact or visit the on-line resource.

**Network Reliability and
Interoperability Council
(NRIC)**

Organization: Network Reliability and Interoperability Council (NRIC)

Information Assurance Points of Contact:

Henry M. Kluepfel, Corporate Vice President, Science Applications International Corporation, 973-543 7064, henry.m.kluepfel@cpmx.saic.com

On-Line Resources:

<http://www.nric.gov>

Missions and Functions:

The Network Reliability and Interoperability Council (NRIC) is a Federal Advisory Committee chartered by the Federal Communications Commission (FCC).¹ The charter was renewed for a fourth term, on July 30, 1998, with the appointment of AT&T CEO Michael Armstrong as the NRIC-IV Chairman. Under its amended charter, the Council will advise the Commission on the efforts of the industry to prepare for Year 2000 conversion. During NRIC-III, the Council was charged by the FCC to advise it on how it might best accomplish the responsibilities of Section 256 of the then recently enacted Telecommunications Act of 1996. The final report of NRIC-III, entitled "NRIC Network Interoperability: The Key to Competition," contains a number of IA-related recommendations and practices for the security and reliability of the public telecommunications network.² In essence, the NRIC's recommendations to the FCC helped establish the expectations, rules, and potential outcome for each industry service provider participant in the new open market, interconnected local exchange environment.

Members of the Council include Chief Executive Officers and other executives of major wireline and wireless 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.

Activities:

- Three subordinate NRIC-IV focus groups exist to help address the Year 2000 tasking of the Council as follows:
 - What is the impact of the "year 2000 problem" on access to the telecommunications networks?
 - What is the impact of the "year 2000 problem" on access to the telecommunications networks and services (i.e. CPE perspective)?
 - What is the current status of network reliability?

¹ <http://www.nric.org/>

² <http://www.fcc.gov/oet/nric/>

- At its January 14, 1999 meeting, the Council heard reports from each of the three Focus groups with renewed confidence that the PN would be year 2000 compliant and continue excellent reliability performance. The exceptions to the reports confidence were related to international readiness for Year 2000 in several high volume, high risk countries around the globe.³

³ <http://www.nric.org/meetings/>

This page intentionally left blank.

**Office of Science and
Technology Policy**

**President's Committee of Advisors
on Science and Technology
(PCAST)**

Organization: Committee of Advisors on Science and Technology (PCAST)

Senior Information Operations Official:

Dr. Joan P. Porter, Executive Secretary, Office of Science and Technology Policy,
202-456-6100, jporter@ostp.eop.gov

Information Assurance Points of Contact:

202-456-6100

Critical Infrastructure Protection Points of Contact:

202-456-6100

On-Line Resources:

PCAST Homepage: <http://www.whitehouse.gov/wh/eop/ostp/nstc/pcast/pcast.html>

Missions and Functions:

President Clinton established the President's Committee of Advisors on Science and Technology (PCAST) by Executive Order 12882 in November 1993. The committee advises the president on the administration's science and technology budgets and policies. PCAST meets in public session an average of four times a year.

The responsibilities of PCAST are "to advise the president on issues involving science and technology and their roles in achieving national goals, and to assist the National Science and Technology Council (NSTC) in securing private sector participation in its activities." NSTC is a cabinet-level council chaired by the president that coordinates research and development policies and activities across federal agencies. The formal link between PCAST and NSTC ensures that the private sector perspective is included in the policy-making process.

Members:

Neal F. Lane - Assistant to the President for Science and Technology and Director, Office of Science and Technology Policy (co-chair)

John A. Young - Former President and CEO, Hewlett-Packard Co. (co-chair)

Norman R. Augustine - Chairman and CEO, Lockheed Martin Corporation

Francisco J. Ayala - Donald Bren Professor of Biological Sciences, Professor of Philosophy, University of California-Irvine

John M. Deutch - Institute Professor, Dept. of Chemistry, Massachusetts Institute of Technology

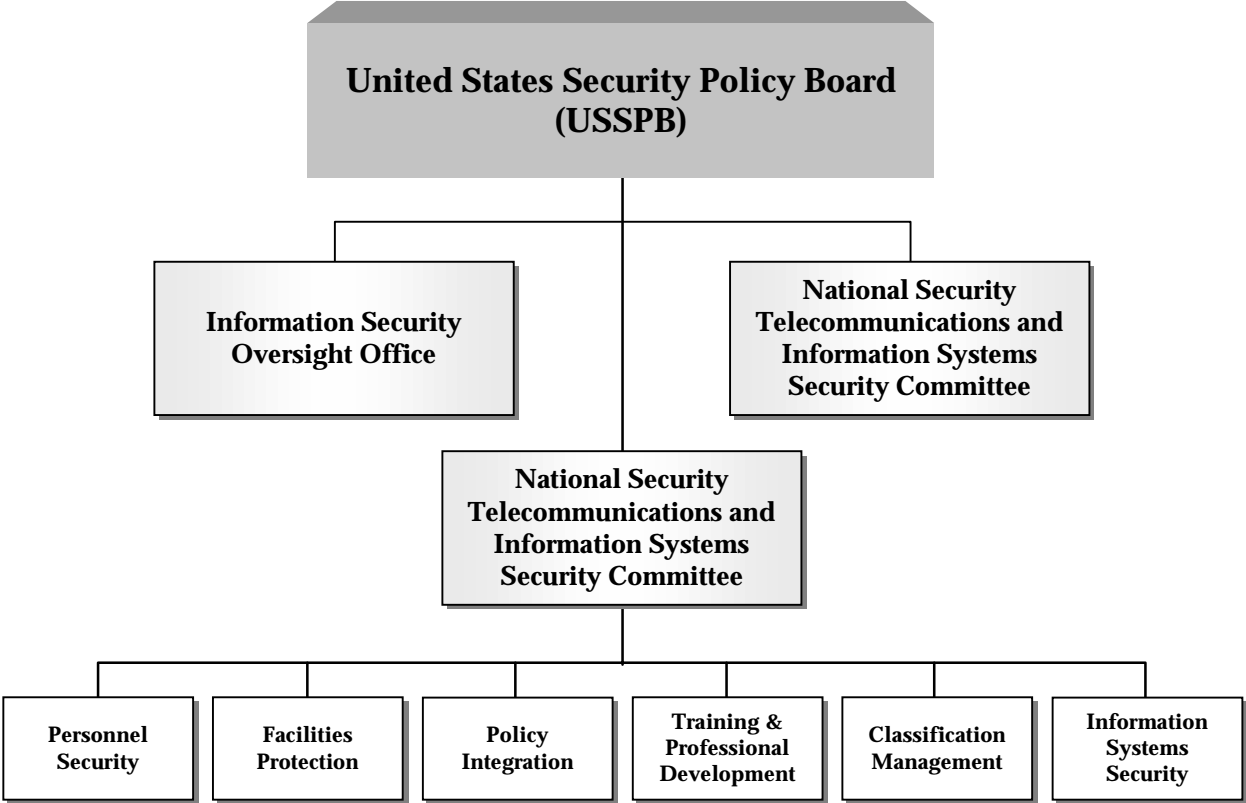
Murray Gell-Mann - Professor, Santa Fe Institute; R.A. Millikan Professor Emeritus of Theoretical Physics, California Institute of Technology

David A. Hamburg - President Emeritus, Carnegie Foundation of New York
John P. Holdren - Teresa and John Heinz Professor of Environmental Policy, John F.
Kennedy School of Government, Harvard University
Diana MacArthur - Chair and CEO, Dynamac Corporation
Shirley M. Malcom - Head, Directorate for Education and Human Resources Programs,
American Association for the Advancement of Science
Mario J. Molina - Institute Professor, Department of Earth, Atmospheric and Planetary
Sciences, Massachusetts Institute of Technology
Peter H. Raven - Director, Missouri Botanical Garden; Engelmann Professor of Botany,
Washington University in St. Louis
Sally K. Ride - Professor of Physics, University of California-San Diego
Judith Rodin - President, University of Pennsylvania
Charles A. Sanders - Former Chairman, Glaxo-Wellcome Incorporated
David E. Shaw - Chairman, D.E. Shaw and Co. and Juno Online Services
Charles M. Vest - President, Massachusetts Institute of Technology
Virginia V. Weldon - Director, Center for the Study of American Business, Washington
University in St. Louis
Lilian Shiao-Yen Wu - Member, Research Staff, Thomas J. Watson Research Center, IBM

Activities:

For activities, contact the Point of Contact or visit the on-line resource.

This page intentionally left blank.



Organization: U.S. Security Policy Board (USSPB)

Information Assurance Points of Contact:

Chris Bythewood, 703-602-0866, chris.bythewood@spb.gov

Critical Infrastructure Protection Points of Contact:

Bill Isaacs, 703-602-0363, bill.isaacs@spb.gov

On-Line Resources:

USSPB Homepage: <http://www.spb.gov>

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.”

PDD-29 established the U.S. Security Policy Board as one component of a tripartite security policy structure, along with the Overseas Security Policy Board (under State Department sponsorship) and the National Counterintelligence Policy Board. The SPB was intended to provide the NSC a process-centric interagency authority to develop security policy based on a new, threat-based (as opposed to risk avoidance) paradigm stressing flexibility, consistency and economy. While the recommendations of the JSC addressed information systems security (ISS) and classification/declassification issues as well as personnel, physical and technical security, the existence of the National Telecommunications and Information Systems Security Committee, and the Information Security Oversight Office, placed constraints on the SPB's ability to be effective as an umbrella policy group under which all the elements of security are organized. It shares responsibility for classification management with ISOO, and for ISS with the NSTISSC. 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 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.
- 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.
- A Classification Management Committee (CMC) charged with the development of classification management policy within the context of the overall security policy framework.
- An Information Systems Security Committee - TBD.

As of 1 June 1995, all committees have been established except the Information Systems Security Committee.

Activities:

- In response to a report by the President's Commission on Critical Infrastructure Protection, the Security Policy Board is developing recommendations to the President on the criteria for and a means of protecting sensitive but unclassified private sector information on threats and vulnerabilities to critical infrastructures.

Appendix C Legal Reference Guide

APPENDIX C
LEGAL REFERENCE GUIDE

This page intentionally left blank.

TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
C.1	LEGISLATION C-5
C.1.1	Electronic Freedom of Information..... C-5
C.1.2	Computer Security Enhancement Act of 1997 C-5
C.1.3	Computer Fraud and Abuse Act of 1986 C-6 (Title 18 U.S.C Section1030)
C.1.4	Economic Espionage Act of 1996 C-7 (Title 18 U.S.C. Section 1831 - Section 1839)
C.1.5	Telecommunications Act of 1996 C-8
C.1.6	National Defense Authorization Act for Fiscal Year 1996 (Section 1053-Kyl Amendment..... C-10
C.1.7	Uniform Code of Military Justice (UCMJ) C-11
C.1.8	Communications Assistance for Law Enforcement Act of 1994..... C-12 (Digital Telephone Act)
C.1.9	Violent Crime Control and Law Enforcement Act of 1994 C-13
C.1.10	Communications Assistance for Law Enforcement Act of 1994..... C-14
C.1.11	Computer Security Act of 1987 C-15
C.1.12	Electronic Communications Privacy Act of 1986..... C-17
C.1.13	Foreign Intelligence Surveillance Act of 1978 C-18
C.1.14	Privacy Act of 1974..... C-20
C.1.15	Communications Act of 1934..... C-21
C.2	EXECUTIVE ORDERS..... C-23
C.2.1	Executive Order 12333 - United States Intelligence Activities,..... C-23 December 4, 1981
C.2.2	Executive Order 12356 - National Security Information, C-24 April 1, 1982
C.2.3	Executive Order 12382 - President's National Security C-25 Telecommunications Advisory Committee, September 13, 1982
C.2.4	Executive Order 12472 - Assignment of National Security and C-25 Emergency Preparedness Telecommunications Functions, April 3, 1984
C.2.5	Executive Order 12958 - Classified National Security C-27 Information, April 17, 1995
C.2.6	Executive Order 13010 - Critical Infrastructure Protection..... C-28
C.2.7	Executive Order 12958 - Classified National Security Information... C-31
C.2.8	Executive Order 13011 - Federal Information Technology C-31
C.2.9	Executive Orders 13020 and 13026, Amendments to Executive..... C-33 Order 12924 - Administration of Export Controls on Encryption Products
C.3	FEDERAL REGULATIONS..... C-35
C.3.1	Export of Encryption..... C-35

This page intentionally left blank.



Legislation

C.1 LEGISLATION

C.1.1 Electronic Freedom of Information

Purpose: This law requires that agencies provide electronic copies of reports, discussions, and paper, via the Internet or on CD ROMs or diskettes. Items such as E-mail can be requested under the *Electronic Freedom of Information Act* (EFOIA).

Discussion: Implementation of the Act began 1 April 1997. The law, an update to the 1966 *Freedom of Information Act* (FOIA), was passed in September of 1996.

When the original FOIA was passed in 1966, there was a flood of requests from persons and organizations, including foreign embassies. The result of early FOIA requests was sometimes the revelation of more information than required, such as the names and other descriptors of personnel or information that was useful in discovering confidential sources of information. This presented problems for certain law enforcement investigations and even endangered lives. It will be interesting to see what types of electronic information will be requested by persons with malicious intent toward the Government information infrastructure, such as hacker groups or foreign intelligence organizations.

While EFOIA extended the time allowed for answering requests from 10 to 20 days, the new Act levies extensive requirements of each agency involved. The Act requires that each agency maintains electronic records to promote wider access; submits an EFOIA section in its annual report to Congress; and satisfies EFOIA requirements established by the Attorney General in October 1966.

C.1.2 Computer Security Enhancement Act of 1997

Purpose: The legislation is aimed at strengthening computer security throughout the Federal government. The legislation updates guidance given in the *Computer Security Act of 1987* to accommodate the many technological advances that have occurred since 1987.¹

Discussion: In his press release, Sensenbrenner cites a General Accounting Office (GAO) finding that, owing to inadequate security in "Federal civilian computer systems," which GAO characterizes as "an enormous problem," Federal computer security is a high-risk, government-wide problem.

¹United States House of Representatives Committee on Science, Press Release on H.R. 1903, the Computer Security Enhancement Act of 1997, by F. James Sensenbrenner, Jr., Chairman (17 June 1997) on Internet at <http://www.house.gov/science/welcome.htm>, United States House of Representatives Committee on Science Internet site.

The 1997 bill's major provisions and updates are as follows:

- Requires that NIST promote the acquisition and usage of already existing computer security technology
- Increases the input of the Computer System Security and Privacy Advisory Board into NIST's decision-making process
- Develops standardized tests to evaluate the strength of foreign encryption products
- Limits NIST's involvement to assisting Federal agencies in the acquisition of security technologies and not restricting the production or use of encryption by the private sector
- Updates the *Computer Security Act of 1987* to account for changes in technology over the last decade
- Establishes an academic fellowship program for graduate and undergraduate students studying computer security.

C.1.3 Computer Fraud and Abuse Act of 1986 (Title 18 U.S.C. Section 1030)

Purpose: As amended October 3, 1996, Section 1030 is also known as the *Computer Fraud and Abuse Act of 1986*. It remains the major statute for prosecution of DOD and active-duty military personnel for computer crime. Generally, this Act prohibits gaining unauthorized access or exceeding authorized access to computers, as well as attempts to obtain such access. The acts of gaining or attempting to gain unauthorized access and exceeding authorized access to obtain information are essential elements of the crimes. National security, financial, and medical information are specifically extended protection under this section, and Section 1030 (a)(2)(C) protects against interstate or foreign theft of any information by computer. Also, of note is the fact that "obtaining information" includes the act of reading information.

Discussion: Computer crime historically has been prosecuted under various Title 18 U.S.C. sections. Examples include: Section 1343 (fraud by wire), Section 1363 (malicious mischief), Section 1029 (access devices), Section 1030 (computer fraud and abuse), Section 785 (communicating a threat), and Section 251 (wiretap). *The National Information Infrastructure Protection Act of 1995* was an attempt to reform Title 18 of the U.S.C. and bring the necessary options for prosecuting under Section 1030. It is intended that all future fine tuning of the statutes that becomes necessary as new technologies develop should be focused at Section 1030.

The statute specifies that it does not prohibit lawfully authorized law enforcement or intelligence agency actions.

Punishment ranges from 1 to 20 years and/or fines, with the heaviest punishments unauthorized or exceeded access to and disclosure of national security information, as described in (a)(1). Civil action is allowed for compensatory damages and injunctive or other equitable relief. Civil damages are limited to economic damages.

The following important definitions are found in Section 1030:

- A **protected computer** is one that is:
 - Exclusively for the use of a financial institution or the U.S. Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the U.S. Government and the conduct constituting the offense affects that use by or for the financial institution or the Government
 - Which is used in interstate or foreign commerce or communications.
- **Damage** means “any impairment to the integrity or availability of data, a program, a system, or information,” that
 - Causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals
 - Modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals
 - Causes physical injury to any person
 - Threatens public health or safety.

C.1.4 Economic Espionage Act of 1996 (Title 18 U.S.C. Section 1831 - Section 1839)

Purpose: The *Economic Espionage Act of 1996*, codified at Title 18 U.S.C., Chapter 90- Protection of Trade Secrets, Section 1831 - 1839, recognizes that foreign government and other agents are attempting to gain economic advantage by stealing information that is not necessarily considered national security information. The *Act*, therefore, extends Federal protection to trade secrets.

Discussion: While establishing new avenues for prosecution, the *Act* specifies that it does not preempt or displace other remedies. The *Act* specifies the actions of downloading, uploading, and transmitting as elements of the crime, and amends Section 102 (Wire and electronic communications interception and interception of oral communications) and Section 2516(1)(c) to include economic espionage.

The sections of the *Act* are briefed as follows. Note how the *Act* is constructed to address the intangible aspects of information, which is vital in prosecuting information-assurance-related matters and is a stride forward in promoting such legal thinking.

Section 1831 – Economic Espionage: (Agent of Foreign Power); Penalties: Persons - \$500,000, 15 years; Organizations: \$10,000,000. This section refers to economic espionage committed by or connected with a foreign power. Legitimate reporting activities of embassy personnel, such as gross national product data, publicly available commerce figures and agricultural output are not proscribed by the *Act*. As with other espionage statutes, the prosecutor must demonstrate the perpetrator’s intent to aid the foreign power.

Section 1832 – Theft of Trade Secrets: (Commercial Espionage); Penalties: Persons: \$500,000, 10 years; Organizations: \$5,000,000. This section addresses the theft, misappropriation, wrongful conversion, duplication, alteration, or destruction of a trade secret. In prosecuting

under this section, the prosecutor must show the perpetrator's intent to "convert a trade secret to the economic benefit of someone other than the rightful owner and intended to or knew that the offense would harm or injure the rightful owner. Prosecutors also must show that the accused knowingly engaged in the misconduct charged."² This high threshold of proof is intended to separate criminal conduct from innocent or careless conduct.

Section 1833 – Exceptions: Law enforcement activity is exempt.

Section 1834 – Criminal Forfeiture: In addition to any other sentence imposed, the court may order the convicted perpetrator to forfeit: (1) any property derived from violation, (2) any property used to commit or facilitate commission of violation, (3) victim restitution from Victims' Fund.

Section 1835 – Orders to Preserve Confidentiality: Court may take action to preserve confidentiality of trade secrets. Such confidentiality is intended to encourage victim reporting.

Section 1836 – Civil Proceedings to Enjoin Violations: This section allows the United States Attorney to seek civil remedies to prevent and restrain violations of the *Act*. These actions include ordering persons to divest themselves of interest in an enterprise; imposing restrictions on future activities or investments of persons who may wish to engage in activities similar to the illegal activity charged; dissolving or reorganizing an organization.

Section 1837 – Applicability to Conduct Outside the United States: Extraterritorial jurisdiction applies if (1) offender is a citizen or permanent resident alien, or an organization organized under the laws of the United States; (2) an act in furtherance of offense was committed in the United States.

Section 1838 – Construction with Other Laws: The *Act* does not preempt or displace other remedies, such as state laws.

Section 1839 – Definitions: (3) (Trade Secret): A trade secret is defined as a reasonably protected property, intangible or tangible, having economic value.

C.1.5 Telecommunications Act of 1996

Purpose: The United States' 1996 *Telecommunication Act* seeks to ensure the opportunity for free competition, fairness, and adequate enforcement within the United States' telecommunications industry.

Discussion: The United States has promulgated these ideals through its strong support of international agreements, such as the World Trade Organization's (WTO) 1997 *Basic Telecommunications Services Agreement* and the 1995 *Information Technology Agreement*, which reduce tariffs, establish pro-competitive regulation, and open information technology

² Ibid.

markets in over 90 percent of the WTO's 130 member nations. The *Basic Telecommunications Services Agreement* was fully implemented as of 1 January 1998, allowing U.S. corporations to establish a presence in foreign nations and acquire, in whole or in part, ownership of foreign telecommunications companies. In this way, the United States may help ensure the availability of information services by eliminating the need to use undesirable systems. The agreement also opened the door for foreign entities to operate in the United States and acquire ownership of U.S. corporations.³

DISA General Counsel, in its analysis of the *Telecommunication Act*, raises concerns for the Department of Defense. These concerns are also pertinent to the *Basic Telecommunications Services Agreement*. The General Counsel analysis states the following: "The language of both House and Senate versions of the *Act* when it went to conference committee contained extensive provisions dealing with foreign ownership of telecommunications companies. These provisions raised some serious national security concerns. Almost all of these provisions were eliminated in conference. Only one survived — a provision which lifted a restriction against having foreign officers and directors in certain U.S. companies. Foreign ownership issues continue to percolate in Congress and before the Federal Communications Commission (FCC) and they raise serious national security concerns."⁴

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.

³ Charlene Barshefsky, Statement of Ambassador Charlene Barshefsky: "Basic Telecom Negotiation" (15 February 1997). U.S. Trade Representative Internet site, <http://www.ustr.gov/agreements/telcom/barshefsy.html>

⁴ *Telecommunications Act of 1996*.

- 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.

C.1.6 National Defense Authorization Act for Fiscal Year 1996 (Section 1053 – Kyl Amendment)

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

Discussion:

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:

- 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.
- 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:
 - 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

- 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.

C.1.7 Uniform Code of Military Justice (UCMJ)

This defines crimes and describes punishments for members of the military service, but provides certain avenues not available under civilian law.

As any person residing in the United States, active-duty military and DOD civilian employees can be charged with violations of Federal, state, and local statutes. The major statute for prosecution of DOD and active-duty military personnel for computer crimes remains Title 18 U. S. C. Section 1030. However, the UCMJ, codified at Title 10 U.S.C. Chapter 47, gives the U.S. Government additional options for courts-martial of active-duty military personnel.

The following discussion of UCMJ Articles 92 through 134 is quoted with permission⁵ from *Legal Guide to Computer Crime (A Primer for Investigators and Lawyers)*, which is a comprehensive reference of statutes, case law, and procedures for investigating and prosecuting computer crime cases. Although the purpose of the document is for investigating and prosecuting cases within the DOD, the document would be highly useful to outside agencies as well.⁶

Article 92: Failure to Obey Order or Regulation. Makes it unlawful to violate or fail to obey any lawful general order or regulation. Can be used in conjunction with punitive Service regulations. Further research will be needed, at the time of the incident, to see what punitive Service regulations were in effect at the time of the alleged criminal act. The status, again at the time of incident, of the definition of a lawful general order (and whether the definition includes federal computer crime statutes) will also need to be researched.⁷

Article 106(a): Espionage. Any Service member who transmits a document or other information with the intent or reason to believe that the document or other information will be used to injure the United States (or to the advantage of a foreign nation), is subject to court martial for espionage.⁸

Article 107: False Official Statements. Using another's password could constitute a false official statement. No distinction should be made whether the entity receiving the statement was a person or a machine. The investigator and attorney should key on whether the statement or password was required for gaining illegal access to the computer system.

⁵ Permission granted by Robert E. Giovagnoni, General Counsel, President's Commission on Critical Infrastructure Protection.

⁶ Department of the Air Force, Office of the Staff Judge Advocate, Air Force Office of Special Investigations *Legal Guidance*, by Elizabeth A. Banker, Robert E. Giovagnoni, Alexander R. Smith, and John T. Soma (1996).

⁷ *Ibid.*, p. 6.

⁸ *Ibid.*, p. 6.

The focus must be on “an official statement,” and whether logging onto a computer is an official statement.⁹

Article 121: Larceny and Wrongful Appropriation. Defines larceny and wrongful appropriation as the wrongful taking, obtaining, or withholding, “by any means, from the possession of the owner or any other person any money, personal property, or article of value of any kind.” The object of the computer theft, however, must be tangible property, such as a printed document.¹⁰

Article 123: Forgery. The Article has been used to prosecute a subject for the altering of keypunch cards before the cards were used to process payroll checks by the computer. *United States v. Langston*, 41 C.M.R. 1013 (1970). The subject’s action allowed him to increase his payroll check. Even though the accused did not actually make false writings, his actions in altering the computer input to increase the face amount of the check constituted a forgery. This analogy should hold true in all instances where a person has altered the computer’s operation, at either the input or programming states, to effect the creation of a false writing.

Article 132: Frauds Against the United States. Makes punishable frauds against the United States. May provide a better remedy than forgery in those instances where the individual submits paperwork to set the computer crime in motion instead of altering the computer program. Entering false documents to receive a payroll or TDY check would be an example.¹¹

Article 134: General Article. This general article has been used for theft of intangible items such as time or services. Prohibits anyone from willfully and unlawfully altering, concealing, removing, mutilating, or destroying a public record. The removal of a computer record will probably entail making a copy of the record, thereby leaving the original unaltered so as to minimize detection. Copying a computer record may be punishable under Article 134 by incorporating the same theory used in *United States v. DiGilio*. 538 F. 2d 972 (3rd Cir. 1976). In *DiGilio*, the defendant made unauthorized photocopies of FBI files using Government equipment. The unauthorized copies were considered Government records and the removal of the copies constituted theft under section 641. The court held that “any record” under 641 also included the content of the record.

C.1.8 Communications Assistance For Law Enforcement Act of 1994 (Digital Telephone Act)

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.

⁹ Ibid., pp. 6-7.

¹⁰ Ibid., p. 7.

¹¹ Ibid., p. 7.

Discussion:

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.

C.1.9 Violent Crime Control and Law Enforcement Act of 1994

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.

Discussion:

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).

C.1.10 Communications Assistance for Law Enforcement Act of 1994

Purpose: The *Communications Assistance for Law Enforcement Act of 1994* (CALEA) was designed to ensure that telephone companies can accommodate all Federal, state, and local law enforcement agency court-approved intercept needs through 1998 and beyond.

Discussion: It was intended to protect this capability despite changing technologies that could inhibit electronic surveillance. CALEA does not give law enforcement any new authority in obtaining or conducting electronic surveillance and should not, in and of itself, result in an increase in the use of the technique. Section 104 of CALEA requires that the Attorney General publish in the Federal Register and give notice to telecommunications carriers of: 1. the actual number of simultaneous communication interceptions, pen registers, and trap-and-trace devices that the Attorney General estimates will be needed by October 1998 (“actual capacity”); and 2. the maximum capacity that will be required to accommodate all simultaneous communication interceptions, pen registers, and trap-and-trace devices that the Attorney General estimates will be needed after October 1998 (“maximum capacity”).¹²

According to the FBI, approximately 90 percent of the estimated capacity will be used for pen registers and trap-and-trace devices. “In addition to the Federal government, 41 states, Puerto Rico, the Virgin Islands, and the District of Columbia have statutes allowing for the use of court-authorized wiretaps by law enforcement in the investigation of the most serious criminal acts. All states provide for law enforcement access to dialed telephone numbers using the less intrusive pen registers and trap and trace devices . . .”¹³

The FBI has stated that law enforcement has thus far enjoyed the ability to carry out virtually all court-ordered electronic surveillance successfully. New technologies, such as modernized telephone systems, may limit this ability. CALEA does not suggest technological solutions for effecting electronic surveillance; it only seeks to ensure that the required capacity of telephone equipment, facilities, and services is available to law enforcement.

C.1.11 Computer Security Act of 1987

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

The *Computer Security Act of 1987* (P.L. 100-235) named the National Institute of Standards and Technology as the lead agency for computer security for Federal civilian agencies. The 1987 Act assigned NIST the task of developing standards and guidelines to ensure cost-effective security and privacy of sensitive information in Federal computer systems.

¹² Department of Justice, Federal Bureau of Investigation “Implementation of Section 104 of the Communications Assistance for Law Enforcement Act: Second Notice and request for comments,” *Federal Register* 62 (14 January 1997).

¹³ Ibid.

- 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.
- 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.

C.1.12 Electronic Communications Privacy Act of 1986

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

Discussion:

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 communication 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.

C.1.13 Foreign Intelligence Surveillance Act of 1978

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.

Discussion:

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.
- 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.

C.1.14 Privacy Act of 1974

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.

Discussion:

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.

C.1.15 Communications Act of 1934

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.

Discussion:

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.
 - 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.



Executive Orders

C.2 EXECUTIVE ORDERS

C.2.1 Executive Order 12333 - United States Intelligence Activities, December 4, 1981

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 counter-espionage directed against government, corporations, establishments, or persons.

Discussion:

Restrictive Clauses

- Agencies will not use electronic surveillance techniques except in accordance with procedures established by 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.
- 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.

C.2.2 Executive Order 12356 - National Security Information, April 1, 1982

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.

Discussion:

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.
 - Appoint a senior agency official to administer its information security program.

C.2.3 Executive Order 12382 - President's National Security Telecommunications Advisory Committee, September 13, 1982

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

Discussion:

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.

C.2.4 Executive Order 12472 - Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984

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

Discussion:

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 government 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
 - Provide 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
 - Provide recommendations 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.
- 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.

C.2.5 Executive Order 12958 - Classified National Security Information, April 17, 1995

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

Discussion:

General Provisions

- Two major purposes of the EO are:
 - Prevent unauthorized disclosure of information
 - 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.

C.2.6 Executive Order 13010¹ - Critical Infrastructure Protection

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.

¹ Executive Order 13010, *Critical Infrastructure Protection* (15 July 1996).

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 Energy
 - The Department of Justice
 - Central Intelligence Agency
 - The Department of Defense
 - Federal Emergency Management Agency
 - The Department of Commerce
 - The Federal Bureau of Investigation
 - The Department of Transportation
 - The National Security Agency.
- *The Principals Committee* consisting of:
 - The Secretary of the Treasury
 - The Secretary of Defense
 - The Director of the Office of Management and Budget
 - The Attorney General
 - The Secretary of Commerce
 - The Director of the Federal Emergency Management Agency
 - The Secretary of Transportation
 - The Secretary of Energy
 - The Assistant to the President for National Security Affairs
 - The Director of Central Intelligence
 - 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.

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, other support services, and funds and may, at the Commissions request, contract for the services of non-governmental 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.

C.2.7 Executive Order 12958 - Classified National Security Information²

Purpose: Executive Order 12958, *Classified National Security Information*, issued 17 April 1995, specifies that the President can designate officials with the authority to classify national security information.

Discussion: On 26 February 1997, President Clinton authorized the Chair of the PCCIP to originate classified documents at the Top Secret level for the period of time that the commission exists. The Chair may delegate this authority, according to section 1.4 (c) of Executive Order 12958. This order was necessary to enable the PCCIP to work with sensitive national security information.

C.2.8 Executive Order 13011 - Federal Information Technology³

Purpose: Executive Order 13011, *Federal Information Technology*, issued 16 July 1996, states that the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996* provide the opportunity to significantly improve the way the Government acquires and manages information technology.

Discussion: To achieve this, the Order specifies that executive agencies of the U.S. Government shall:

- Implement the *Paperwork Reduction Act of 1995* and the *Information Technology Management Reform Act of 1996*
- Refocus their information management and acquisition processes to directly support their strategic missions, with a review process that ensures that budgets are being expended to an efficient and effective end
- Establish clear accountability for information resources management activities through Chief Information Officers (CIOs), who will participate in the investment review process, monitor and evaluate performance of information systems based upon applicable performance measures; and advise the head of agency when modification or termination of systems is warranted
- Cooperate to promote a “coordinated, interoperable, secure, and shared Government-wide infrastructure,” supported by diverse private sector supplies and well-trained information technology professionals
- Establish an interagency support structure that can provide expertise and advice to “enhance interoperability, minimize unnecessary duplication of effort, and capitalize on agency successes.”

² Executive Order 12958 *Classified National Security Information* (17 April 1995). White House Internet site, <http://www.whitehouse.gov/>

³ Executive Order 13011, *Federal Information Technology* (17 July 1996). White House Internet site, <http://www.whitehouse.gov/>

Heads of agencies are responsible for carrying out these activities within their own agencies. They are to enter into contracts for multi-agency acquisitions of information technology “if and in the manner that the Director of OMB considers it advantageous to do so.”

The Order establishes three interagency organizations to aid OMB, the Departments of Commerce and State, and the General Services Administration in implementing the use of information technology. It sets out the purpose and functions of the Chief Information Officers (CIO) Council,⁴ Government Information Technology Services (GITS) Board,⁵ and the Information Technology Resources (ITR) Board.⁶ Exhibit C-1 summarizes the responsibilities of these entities.

ITRB	CIO Council	GITS Board
<ul style="list-style-type: none"> • Conducts independent assessment to aid in acquiring, developing, and managing selected major information systems. • Composed of U.S. Government IT practitioners with expertise in managing and developing major information systems. • Provides peer perspective on systems under review. • Provides recommendations to agency heads and OMB. 	<ul style="list-style-type: none"> • Principal forum for U.S. Government coordination of Executive Order 13011. • Composed of CIOs and deputy CIOs of 28 executive agencies, as well as OMB representatives. • Identifies opportunities for cross-agency coordination. • Provides advice on IT strategy. • Assesses IT education and training needs. 	<ul style="list-style-type: none"> • Ensures continued implementation of the IT recommendations of the National Performance Review. • Composed of agency representatives. • Consults experts on matters of concern. • Makes recommendations to the agencies, CIO Council, OMB. • Promotes development of innovative technologies, standards and practices.

Exhibit C-1. Organizations Established by Executive Order 13011

The order also specifies that GSA will continue the FTS2000 long distance telecommunications service (provided by contract to the Federal Telecommunications Service (FTS)). Also, the Department of Commerce will carry out the standards responsibilities established by the *Computer Security Act of 1987*. The Department of State conducts liaison, consultation, and negotiations with foreign governments and foreign intergovernmental agencies and ensures that the United States participates in setting information technology standards in the international arena.

OMB has submitted a progress report, entitled *Getting Federal Computers Ready for 2000*,⁷ which is aimed at assuring agency accountability in addressing the year 2000 computer problem. The report cites OMB Memorandum M-97-13,⁸ which requires quarterly reports from U.S. Government agencies on the fifteenth of February, May, August, and November,

⁴ See CIO Council Internet site, <http://www.cio.fed.gov/>

⁵ See GITS Internet site, <http://www.gits.fed.gov/>

⁶ See ITRB Internet site, <http://www.gsa.gov/irms/ka/mka/itrb/>

⁷ U.S., Executive Office of the President, OMB, “Getting Federal Computers Ready for 2000” (15 May 1997). CIO Council Internet site, <http://www.cio.fed.gov/yr2krev.htm>

⁸ Executive Office of the President, OMB, “Computer Difficulties Due to the Year 2000 - Progress Reports” (7 May 1997).

1997, and states that agencies in the Executive Branch have made good progress toward addressing the problem.

C.2.9 Executive Orders 13020 and 13026, Amendments to Executive Order 12924⁹ - Administration of Export Controls on Encryption Products

Encryption has been a hotly contested topic. Executive Orders 13020, and 13026 were issued 15 November 1996 as continuations of Executive Order 12924, *Administration of Export Controls on Encryption Products*, 19 August 1994. Until the 15 November 1996 order, encryption was defined as a munition and was regulated by the International Traffic in Arms Regulations (ITAR) and the *Arms Export Control Act* (AECA), which was administered by the U.S. Department of State. Encryption was subject to the controls of the U.S. Munitions List. The 15 November 1996 order transferred authority to regulate the export of non-military encryption to the U.S. Department of Commerce Bureau of Export Administration (BXA), to be regulated as a dual-use technology on the Commerce Control List (CCL) under the *Export Administration Regulations* (EAR), as are other export-controlled commercial products.¹⁰

⁹ Executive Order 12924, *Administration of Export Controls on Encryption Products* (30 December 1996). White House Internet site, <http://www.whitehouse.gov/>

¹⁰ U.S. Code of Federal Regulations, *Export Administration Regulations (EAR)*, 15 CFR Parts 730-774 (7 January 1997).

This page intentionally left blank.



Federal Regulations

C.3 FEDERAL REGULATIONS

C.3.1 Export of Encryption

As stated above, non-military encryption is now regulated by EAR, 15 CFR Parts 730-774, which makes it illegal to export encryption software that exceeds 56-bit encoding. The new regulations allow the export of 56-bit DES, provided the exporter submits plans and demonstrates work in developing a key management structure that is consistent with Government specifications. The regulations also include procedures concerning the development of “a key management infrastructure.” The most important of these is the creation of a license exemption that would allow “recoverable encryption products of any strength and key length to be exported freely after a single review by Commerce, Justice, and DOD.”¹

The new regulations expand the definition of products that are eligible for the key recovery license exemption, so that it includes “key escrow” systems, which use a trusted third party, as well as other systems, for recovery of keys or plain text. Self-escrow and escrowing of keys overseas under certain circumstances is allowed in order to make key recovery products more attractive in export markets. The Department of Commerce has developed pilot projects to demonstrate key recovery.²

The National Institute of Standards and Technology has formed an industry advisory committee to develop requirements and standards for key recovery. The advisory committee has invited foreign government representatives to meetings to aid in ensuring coordination and compatibility on a multilateral basis. The President has appointed the U.S. ambassador to the Organization for Economic Cooperation and Development (OECD) as his Special Envoy on Encryption and has learned that several OECD countries have begun their own key recovery programs.³

In addition to setting out requirements for interoperability features and design, implementation, and operational assurance, Supplement No. 4 to Part 742 of the EAR, *Key Escrow or Key Recovery Products Criteria*, describes required key recovery feature as follows:

- The key(s) or other material/information required to decrypt ciphertext shall be accessible through a key recovery feature.
- The product's cryptographic functions shall be inoperable until the key(s) or other material/information required to decrypt ciphertext is recoverable by government officials under proper legal authority and without the cooperation or knowledge of the user.
- The output of the product shall automatically include, in an accessible format and with a reasonable frequency, the identity of the key recovery agent(s) and information

¹ William A. Reinsch, “Administration Encryption Policy,” testimony before the Subcommittee on International Economic Policy and Trade House Committee on International Relations, 8 May 1997. U.S. Department of Commerce, Bureau of Export Administration Internet site, <http://www.bxa.doc.gov/warcong7.htm>

² Ibid.

³ Ibid.

sufficient for the key recovery agent(s) to identify the key(s) or other material/information required to decrypt the ciphertext.

- The product's key recovery functions shall allow access to the key(s) or other material/information needed to decrypt the ciphertext regardless of whether the product generated or received the ciphertext.
- The product's key recovery functions shall allow for the recovery of all required decryption key(s) or other material/information required to decrypt ciphertext during a period of authorized access without requiring repeated presentations of access authorization to the key recovery agent(s).⁴

Supplement No. 5 to EAR Part 742, *Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures*, describes the criteria the Department of Commerce will use in the export approval process. EAR Key Recovery Agent Requirements are:

- (1) (a) A key recovery agent must identify by name, date, place of birth, and social security number, individual(s) who:
 - (i) Is/are directly involved in the escrowing of key(s) or other material/information required to decrypt ciphertext; or
 - (ii) Have access to key(s) or other material/information required to decrypt ciphertext; or
 - (iii) Have access to information concerning requests for key(s) or other material/information required to decrypt ciphertext; or
 - (iv) Respond to requests for key(s) or other material/information required to decrypt ciphertext; or
 - (v) Is/are in control of the key recovery agent and have access or authority to obtain key(s) or other material/information required to decrypt ciphertext, and
- (b) Must certify that such individual(s) meet the requirements of the following paragraphs (b)(i) or (b)(ii). BXA reserves the right to determine at any time the suitability and trustworthiness of such individual(s). Evidence of an individual's suitability and trustworthiness shall include:
 - (i) Information indicating that the individual(s):
 - (A) Has no criminal convictions of any kind or pending criminal charges of any kind;
 - (B) Has not breached fiduciary responsibilities (e.g., has not violated any surety or performance bonds); and
 - (C) Has favorable results of a credit check; or,

⁴ U.S. Department of Commerce, Bureau of Export Administration Internet site, <http://www.bxa.doc.gov/supp4.htm>.

- (ii) Information that the individual(s) has an active U.S. Government security clearance of Secret or higher, issued or updated within the last 5 years.
- (2) The key recovery agent shall timely disclose to BXA when an individual no longer meets the requirements of paragraphs I.(1)(b)(i) or (ii).
- (3) A key recovery agent must, to remain eligible for License Exception Key Management Infrastructure (KMI), identify to BXA by name, date, place of birth, and social security number any new individual(s) who will assume the responsibilities set forth in paragraph I.(1)(a) of this Supplement. Before that individual(s) assumes such responsibilities, the key recovery agent must certify to BXA that the individual(s) meets the criteria set forth in subparagraphs I.(1)(b)(i) or (b)(ii) of this Supplement. BXA reserves the right to determine at any time the suitability and trustworthiness of such personnel.
- (4) If ownership or control of a key recovery agent is transferred, no export may take place under previously issued approvals until the successor key recovery agent complies with the criteria of this Supplement.
- (5) Key recovery agents shall submit suitable evidence of the key recovery agent's corporate viability and financial responsibility (e.g., a certificate of good standing from the state of incorporation, credit reports, and errors/omissions insurance).
- (6) Key recovery agents shall disclose to BXA any of the following which have occurred within the 10 years prior to the application:
 - (a) Federal or state felony convictions of the business;
 - (b) Material adverse civil fraud judgments or settlements; and
 - (c) Debarments from Federal, state, or local government contracting.The applicant shall also timely disclose to BXA the occurrence of any of the foregoing during the use of License Exception KMI.
- (7) Key recovery agent(s) shall designate an individual(s) to be the security and operations officer(s).
- (8) A key recovery agent may be internal to a user's organization and may consist of one or more individuals. BXA may approve such key recovery agents if sufficient information is provided to demonstrate that appropriate safeguards will be employed in handling key recovery requests from government entities. These safeguards should ensure: the key recovery agent's structural independence from the rest of the organization; security; and confidentiality.

Supplement 5, Section II, *Security Policies*, sets out criteria aimed at ensuring the confidentiality, integrity, and availability of the keys and other material required for decryption of the ciphertext. Supplement 5, Section III, *Key Recovery Procedures*, states that key recovery agents must be designed to maintain the capability to make needed information available to decrypt within two hours of receipt of a request, maintain an audit

trail of requests and responses, and have a back up/recovery system if the original system ceases to function properly or is deemed untrustworthy.

Enforcement and protective measures for export matters are codified at 15 CFR Part 764, which specifies conduct that constitutes a violation of the *Export Administration Act* (EAA) and/or the EAR. It sets out criminal sanctions through Federal court and other sanctions that are “neither administrative nor criminal.” It identifies protective administrative measures that the BXA may take pursuant to its regulatory authority.⁵

According to the BXA, criminal penalties for knowing violations of the EAR include a fine of \$50,000 or five times the value of the exports involved, whichever is greater, and or imprisonment. Administrative sanctions may also be imposed. These include revocation of validated export licenses; general denial of export privileges; exclusion from practice; and/or fines of up to \$10,000 per violation, or for a violation of national security export controls, \$100,000. The maximum civil penalty allowed by law during periods in which regulations are continued by Executive Order, pursuant to the *International Economic Emergency Powers Act* (IEEPA), is \$10,000 per violation.⁶

The Assistant Secretary for Export Enforcement also can issue Temporary Denial Orders, which deny any or all export privileges of a company or individual to prevent an imminent export control violation. Such orders deny the right to export from the United States, but also the right to receive or participate in exports from the United States.⁷

Section 11(h) of the *Export Administration Act* empowers the Secretary of Commerce to revoke any export license a party has at the time of a conviction. Section 11(h) also provides that, “at the discretion of the Secretary of Commerce, no person convicted of a violation of the EAA, IEEPA, or Section 38 of the *Arms Export Control Act* (or any regulation, license, or order issued under any of these laws) will be eligible to apply for or use any export license issued under the EAA for up to 10 years from the date of the conviction.”⁸

The EAR does not prohibit the import of such technology, as long as the U.S. vendor took no part in its development and Sun Microsystems is planning to offer a Russian encryption product that provides 128-bit and triple DES encryption over the Internet. Sun will resell the product under the name PC SunScreen SKIP E+. SKIP E+ will support a variety of algorithms, including 56- and 64-bit DES, two- and three-key triple DES, and 128-bit codes.⁹

Sun did not seek government approval for the product and claims to have taken no part in its development. Sun is planning to provide the product to international offices of U.S.-based companies and others through third-party distributors. “SKIP E+ provides encryption and authentication of any IP-based communication, including Telnet, HTTP,

⁵ 15 CFR Part 764, Sec. 764.1.

⁶ U.S. Department of Commerce, Bureau of Export Administration Internet site, <http://www.bxa.doc.gov/eeprgm.htm>

⁷ Ibid.

⁸ Ibid.

⁹ John Fontana, “Sun Crypto Skirts Feds,” *Communications Week* (19 May 1997).

SQL requests and SMTP, while it manages encryption keys, negotiates data transfers, and controls access to data through a three-tiered approval process. Sun has not yet completed work on creating a management model for the access lists that network administrators would need to create for a global system.”¹⁰

¹⁰ Ibid.

This page intentionally left blank.

Appendix D Information Assurance Guide

APPENDIX D
A SUMMARY GUIDE TO INFORMATION ASSURANCE:
PUBLIC LAW, EXECUTIVE ORDERS, AND POLICY DOCUMENTS

This page intentionally left blank.

FOREWORD

This *Summary Guide to Information Assurance Policy* is an update and revision of several earlier versions. It contains summaries of public law, executive orders, national policies, and Department of Defense and Joint Staff policies relevant to information assurance (IA). The documents are grouped according to issuing organization and listed in chronological order. As an exception, DOD directives, instructions, and regulations, as well as Joint Staff publications are listed in numerical order. Summaries of public law, except as noted, summarize the original act, with coverage of any subsequent amendment(s).

This page intentionally left blank.

TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
D.1	PUBLIC LAW	D-11
D.1.1	P.L. 73-416, <i>Communications Act of 1934</i>	D-11
D.1.2	P.L. 93-579, <i>Privacy Act of 1974</i>	D-11
D.1.3	P.L. 95-511, <i>Foreign Intelligence Surveillance Act of 1978</i>	D-11
D.1.4	P.L. 99-508, <i>Electronic Communications Privacy Act of 1986</i>	D-12
D.1.5	P.L. 100-235, <i>Computer Security Act of 1987</i>	D-12
D.1.6	P.L. 103-62, <i>Government Performance and Results Act of 1993</i>	D-13
D.1.7	P.L. 104-13, <i>Paperwork Reduction Act of 1980, 1995</i>	D-13
D.1.8	P.L. 104-104, <i>Telecommunications Act of 1996/Communications.....</i> <i>Decency Act of 1996</i>	D-14
D.1.9	P.L. 104-106, <i>Information Technology Management Reform.....</i> <i>Act of 1996</i>	D-15
D.1.10	P.L. 104-201, <i>National Defense Authorization Act for Fiscal Year 1997...</i>	D-15
D.1.11	P.L. 104-294, Title I, <i>Economic Espionage Act of 1996</i>	D-16
D.1.12	P.L. 104-294, Title II, <i>National Information Infrastructure Protection.....</i> <i>Act of 1996</i>	D-16
D.2	EXECUTIVE ORDERS	D-19
D.2.1	Executive Office of the President, Executive Order 12333,	D-19
	<i>United States Intelligence Activities</i>	
D.2.2	Executive Office of the President, Executive Order 12472,	D-19
	<i>Assignment of National Security and Emergency Preparedness</i> <i>Telecommunications Functions</i>	
D.2.3	Executive Office of the President, Executive Order 12958,	D-20
	<i>Classified National Security Information</i>	
D.2.4	Executive Office of the President, Executive Order 13010,	D-21
	<i>Critical Infrastructure Protection</i>	
D.2.5	Executive Office of the President, Executive Order 13011,	D-23
	<i>Federal Information Technology</i>	
D.3	OTHER NATIONAL POLICY.....	D-25
D.3.1	Presidential/National Security Directives.....	D-25
D.3.1.1	PD/NSC 24, <i>Telecommunications Protection Policy (U)</i>	D-25
D.3.1.2	PDD/NSC 29, <i>Security Policy Coordination</i>	D-25
D.3.1.3	PDD 39, Secret, <i>U.S. Policy on Counterterrorism</i>	D-26
D.3.1.4	PDD 62, <i>Combating Terrorism</i>	D-27
D.3.1.5	PDD 63, <i>Protecting America's Critical Infrastructures</i>	D-28
D.3.1.6	NSD 42, <i>National Policy for the Security of National</i>	D-29
	<i>Security Telecommunications and Information Systems</i>	

TABLE OF CONTENTS (Continued)

<u>Section</u>	<u>Page</u>
D.3.2	Office of Management and Budget..... D-30
D.3.2.1	Office of Management and Budget, OMB Bulletin 90-08,.... D-30 <i>Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information</i>
D.3.2.2	Office of Management and Budget, OMB Circular A-76,.... D-30 <i>Performance of Commercial Activities</i>
D.3.2.3	Office of Management and Budget, Supplement to OMB... D-31 <i>Circular A-76, Performance of Commercial Activities</i>
D.3.2.4	Office of Management and Budget, OMB Circular A-123,.. D-32 <i>Management Accountability and Control</i>
D.3.2.5	Office of Management and Budget, OMB Circular A-130,.. D-33 <i>Management of Federal Information Resources</i>
D.3.3	National Institute of Standards and Technology..... D-34
D.3.3.1	National Institute of Standards and Technology (NIST), D-34 <i>NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook</i>
D.3.3.2	National Institute of Standards and Technology (NIST), D-34 <i>NIST Special Publication 800-13, Telecommunications Security Guidelines for Telecommunications Management Network</i>
D.3.3.3	National Institute of Standards and Technology (NIST), D-35 <i>Generally Accepted Principles and Practices for Security Information Technology Systems (Draft)</i>
D.3.4	National Security Telecommunications and Information Systems.... D-35 Security
D.3.4.1	NCSC-1, <i>National Policy For Safeguarding and Control of</i> D-35 <i>Communications Security Material</i>
D.3.4.2	NCSC-5 w/ App 1 and 2, <i>National Policy on Use of</i> D-35 <i>Cryptomaterial by Activities Operating in High Risk Environments</i>
D.3.4.3	NCSC-11, <i>National Policy for the Protection of</i> D-36 <i>Telecommunications Systems Handling Unclassified National Security-Related Information (U)</i>
D.3.4.4	NCSC-8, Confidential, <i>National Policy on Security Voice</i> D-36 <i>Communications (U)</i>
D.3.4.5	NACAM - 83/1, Confidential, <i>Advisory Memorandum on</i> D-36 <i>Protection of COMSEC Information Related to Foreign Governments and International Organizations (U)</i>
D.3.4.6	NCSC-2, <i>National Policy on Release of Communications</i> D-36 <i>Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources</i>

TABLE OF CONTENTS (Continued)

<u>Section</u>	<u>Page</u>
D.3.4.7 NACAM - 84/1, <i>Advisory Memorandum on Protection of... Unclassified National Security-Related Telecommunications</i>	D-37
D.3.4.8 NTISSP No. 1, <i>National Policy on Application of..... Communications Security to U.S. Civil and Commercial Space Systems</i>	D-37
D.3.4.9 NTISSP No. 200, <i>National Policy on Controlled Access..... Protection</i>	D-37
D.3.4.10 NTISSP No. 100, Confidential, <i>National Policy on Application of Communications Security to Command Destruct Systems (U)</i>	D-38
D.3.4.11 NTISSP No. 3, FOUO, <i>National Policy for Granting Access. to U.S. Classified Cryptographic Information</i>	D-38
D.3.4.12 NSTISSD No. 600, FOUO, <i>Communications Security (COMSEC) Monitoring</i>	D-38
D.3.4.13 NSTISSP No. 4, FOUO, <i>National Policy on Electronic Keying</i>	D-39
D.3.4.14 NSTISSD No. 501, <i>National Training Program for..... Information Systems Security (INFOSEC) Professionals</i>	D-39
D.3.4.15 NSTISSD No. 502, <i>National Security Telecommunications... and Automated Information Systems Security</i>	D-39
D.3.4.16 NSTISSD No. 500, FOUO, <i>Information Systems Security (INFOSEC) Education, Training and Awareness</i>	D-39
D.3.4.17 NSTISSD No. 501, <i>National Training Program for..... Information Systems Security (INFOSEC) Professionals</i>	D-40
D.3.4.18 NSTISSP No. 5, FOUO, <i>National Policy for Incident..... Response and Vulnerability Reporting for National Security Systems</i>	D-40
D.3.4.19 NSTISSD No. 503, FOUO, <i>Incident Response and..... Vulnerability Reporting for National Security Systems</i>	D-40
D.3.4.20 NSTISSP No. 300, FOUO, <i>National Policy on Control of..... Compromising Emanations</i>	D-41
D.3.4.21 NSTISSI No. 7000, Confidential NOFORN, <i>TEMPEST..... Countermeasures for Facilities (U)</i>	D-41
D.3.4.22 NSTISSP No. 6, <i>National Policy on Certification and..... Accreditation of National Security Telecommunications and Information Systems</i>	D-41
D.3.4.23 NSTISSP No. 7, <i>National Policy on Secure Electronic Messaging Services</i>	D-42
D.3.4.24 NSTISSI No. 4011, <i>National Training Standard for..... Information Systems Security (INFOSEC) Professionals</i>	D-42
D.3.4.25 NSTISSI No. 4009, <i>National Information Systems Security .. Glossary</i>	D-42

TABLE OF CONTENTS (Continued)

<u>Section</u>		<u>Page</u>
	D.3.4.26 NSTISSI No. 4012, <i>National Training Standard for.....</i> <i>Designated Approving Authority (DAA)</i>	D-43
	D.3.4.27 NSTISSI No. 4013, <i>National Training Standard for.....</i> <i>System Administrators in Information Systems Security</i> <i>(INFOSEC)</i>	D-44
	D.3.4.28 NSTISSI No. 4014, <i>National Training Standard for.....</i> <i>Information Systems Security Officers (ISSO)</i>	D-44
D.4	DEPARTMENT OF DEFENSE.....	D-47
	D.4.1 DoDD TS-3600.1, Top Secret NOFORN, <i>Information Warfare (U)</i>	D-47
	D.4.2 DoDD S-3600.1 Secret NOFORN, <i>Information Operations (U)</i>	D-47
	D.4.3 DoDI S-3600.2, Secret NOFORN, <i>Information Warfare Security</i>	D-48
	<i>Guidance (U)</i>	
	D.4.4 DoDD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems	D-48
	D.4.5 DoDI 4630.8, Procedures for Compatibility, Interoperability, and Integration of C3I Systems	D-48
	D.4.6 DoDD 5000.1, <i>Defense Acquisition</i>	D-48
	D.4.7 DoD Regulation 5000.2-R, <i>Mandatory Procedures for Major Defense</i> <i>Acquisition Programs (MDAPS) and Major Automated Information</i> <i>Systems (MAIS) Acquisition Programs</i>	D-49
	D.4.8 DoDD 5105.19, <i>Defense Information Systems Agency</i>	D-49
	D.4.9 DoDD 5111.1, <i>Under Secretary of Defense for Policy</i>	D-50
	D.4.10 DoDD 5137.1, <i>Assistant Secretary of Defense for C3I</i>	D-51
	D.4.11 DoDD 5160.54, <i>Critical Assets Assurance Program</i>	D-53
	D.4.12 DoDD 5200.1, <i>DoD Information Security Program</i>	D-54
	D.4.13 DoD 5200.1-R, <i>Information Security Program Regulation</i>	D-54
	D.4.14 DoDD 5200.2, <i>DoD Personnel Security Program</i>	D-55
	D.4.15 DoDD C-5200.5, Confidential, <i>Communications Security</i>	D-55
	<i>(COMSEC) (U)</i>	
	D.4.16 DoDD C-5200.19, Confidential, <i>Control of Compromising</i>	D-55
	<i>Emanations (U)</i>	
	D.4.17 DoDD 5200.28, <i>Security Requirements for Automated Information</i>	D-56
	<i>Systems</i>	
	D.4.18 DoD 5200.28-M, <i>ADP Security Manual; Techniques and Procedures</i> <i>for Implementing, Deactivating, Testing, and Evaluating - Secure</i> <i>Resource-Sharing ADP Systems</i>	D-58
	D.4.19 DoD 5200-28-STD, <i>DoD Trusted Computer System Evaluation</i>	D-59
	<i>Criteria</i>	
	D.4.20 DODD 5200.40, <i>Defense Information Technology Security</i>	D-59
	<i>Certification and Accreditation Process</i>	

TABLE OF CONTENTS (Continued)

<u>Section</u>	<u>Page</u>
D.4.21 DoDD 5205.2, <i>DoD Operations Security Program</i>	D-60
D.4.22 DoDD 5215.1, <i>Computer Security Evaluation Center</i>	D-60
D.4.23 DoDI 5215.2, <i>Computer Security Technical Vulnerability Reporting</i> <i>Program</i>	D-61
D.4.24 DoDD 5220.22, <i>DoD Industrial Security Program</i>	D-61
D.4.25 DoDD 5240.11, <i>Damage Assessments</i>	D-61
D.4.26 DoDD 7740.1, <i>DoD Information Resources Management Program</i>	D-61
D.4.27 DoDD 8000.1, <i>Defense Information Management (IM) Program</i>	D-61
D.4.28 DoD, Office of the Secretary of Defense, <i>National Industrial</i> <i>Security Program (NISP) Operating Manual (NISPOM)</i>	D-62
D.4.29 DoD, Office of the Under Secretary of Defense for Acquisition..... and Technology Defense Science Board (DSB). <i>Report of the Defense</i> <i>Science Board Task Force on Information Warfare – Defense</i>	D-62
D.5 JOINT STAFF	D-65
D.5.1 CJCSI 3210.01A, <i>Secret, Joint Information Operations Policy (U)</i>	D-65
D.5.2 CJCSI 6510.01B, <i>Defensive Information Operations</i>	D-66
D.5.3 Joint Pub 3-13, <i>Joint Doctrine for Information Operations</i>	D-68
D.6 OTHER	D-69
D.6.1 DCID 1/16, <i>Secret, Security Policy for Uniform Protection of</i> <i>Intelligence Processed in Automated Information Systems and</i> <i>Networks (U)</i>	D-69
D.6.2 DCID 1/16, <i>FOUO, Security Policy on Intelligence and DOD SAP</i>	D-69
<i>Information Systems: Policy, Draft Five</i>	

This page intentionally left blank.



Public Law

D.1 PUBLIC LAW

D.1.1 P.L. 73-416, Communications Act of 1934, 19 Jun 34

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.

- Neither the Communications Act of 1934 or the Telecommunications Act of 1996 assigned responsibilities to DOD.

D.1.2 P.L. 93-579, Privacy Act of 1974, 31 December 1974

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. It also levies civil and criminal penalties for violations of the provisions of the Act. As a Federal agency, DOD's responsibilities under the Act include:

- Implementation of physical security practices, information management practices, and computer and network controls necessary to ensure individual privacy.

D.1.3 P.L. 95-511, Foreign Intelligence Surveillance Act of 1978, 25 Oct 78

The Foreign Intelligence Surveillance Act of 1978 [50 USCS §§ 1801 ET SEQ.] (FISA) is used to obtain electronic surveillance and physical searches without warrant, but under court order, in cases of foreign intelligence, international terrorism, or sabotage activities that are perpetrated by a foreign power or its agent. It is an alternative to Title III warrants, which are used in most cases that concern the potential criminal prosecution of US Persons. The major legal difference in the two statutes is that to obtain a court order under FISA, the applicant does not have to prove the level of probable cause that is required for Title III electronic surveillance or for search warrants. The reason for this is that the primary purpose of a FISA order is to collect foreign intelligence information and not to prosecute US Persons. The Act has been upheld in numerous challenges, including cases of courts

martial of on-duty servicemen who were charged under the Uniform Code of Military Justice.

The FISA is used by the DOD, and in fact, *The Executive Order Number 12139 of May 23, 1979, 44 Fed. Reg. 30311*, provides that the Secretary of Defense and the Deputy Secretary of Defense may be appointed by the President, with the advice and consent of the Senate, to make certifications to the Attorney General, as required by the Act, that the application being submitted to the Foreign Intelligence Surveillance Court conforms to the requirements of the Act. This certification power applies to applications for electronic surveillance as well as physical searches.

D.1.4 P.L. 99-508, Electronic Communications Privacy Act of 1986, 21 October 1986

P.L. 99-508 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 Telephone 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.

D.1.5 P.L. 100-235, Computer Security Act of 1987, 8 January 1988

The Computer Security Act declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and creates a means for establishing minimum acceptable security practices for such systems. It assigns NIST responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems. NIST will draw on the technical advice and assistance (including work products) of the National Security Agency, where appropriate. [In 1989, NIST and NSA executed an MOU to clarify roles and responsibilities under the Act].

The Act specifically excludes from NIST purview, Federal classified and Warner Exempt systems. NIST is authorized to assist the private sector, upon request, in using and applying the results of its programs and activities. The Act also 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 scope is limited to Federal unclassified systems. Key responsibilities include:

- In coordination with NIST, each government agency must establish a computer security policy commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in the system.
- Each government agency will develop security plans by all operators of Federal computer systems that contain sensitive information.
- Summaries of agency security plans shall be included in the information resources management plan required by the Paperwork Reduction Act of 1980.
- Each government agency will provide mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

D.1.6 P.L. 103-62, Government Performance and Results Act of 1993, 3 August 1993

The purpose of the Government Performance and Results Act (GPRA) is to reform Federal program performance with a series of pilot projects in setting program goals, measuring program performance against these goals, and public reporting on their progress. The Act requires agencies to submit strategic plans for program activities to OMB and Congress by September 30, 1997, and to establish performance goals for program activities, which are objective, quantifiable, and measurable.

D.1.7 P.L. 104-13, Paperwork Reduction Acts of 1980, 1995, 22 May 1995

The Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, is 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 agencies to acquire/use IT to improve service delivery and program management, increase productivity, enhance the quality of decision-making, and reduce fraud and waste. It also requires that agencies develop 5-year plans 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 assigned OMB responsibility for improving Federal government administrative efficiency through the use of new technologies such as electronic mail and electronic document storage (imaging). The Act makes OMB responsible for developing governmentwide guidance on information security and overseeing agency practices. The Paperwork Reduction Act of 1995, in 44 U.S.C. 3505 and 3506, requires agencies to establish computer security programs and it tasks OMB to develop and oversee the implementation of policies, principles, standards and guidelines on security. It also requires Federal Agencies to identify and provide security protection consistent with the Computer Security Act of 1987 (40 U.S.C. 759 note) and directs OMB to require Federal agencies to apply a risk management process for information collected or maintained by or on behalf of an agency. DOD responsibilities under the Paperwork Reduction Act include:

- Complying with policies issued by the Director, OMB.
- Designating a senior official, reporting directly to the Secretary of Defense (or Service Secretaries) to carry out the responsibilities of the Act.
- With respect to general information resources management, each agency shall -- manage information resources to -- ...improve the integrity, quality, and utility of information to all users within and outside the agency, including capabilities for ensuring...protections for privacy and security.
- With respect to privacy and security, each agency shall --
 - implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosures and sharing of information collected or maintained by or for the agency;
 - assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, the Computer Security Act of 1987, and related information management laws; and
 - consistent with the Computer Security Act of 1987, identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collects or maintained by or on behalf of an agency.

D.1.8 P.L. 104-104, Telecommunications Act of 1996/Communications Decency Act of 1996, 8 February 1996

This Act is known by two different names as indicated above, depending upon the emphasis applied by the reader to different aspects of the law. The main part of the Act is to provide for a pro-competitive, de-regulatory national policy framework. It was designed to accelerate private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening all telecommunications markets to competition. Noteworthy were the provisions of Title V on obscenity and violence which have incited much litigation since the law's enactment (hence its other enactment short title).

The Telecommunications Act of 1996 will in time revolutionize the telecommunications industry by greatly expanding the numbers and types of telecommunications carriers and combinations of services. It is the most significant overhaul of national telecommunications policy since the Communications Act of 1934. This Act is seen as a completion of the Bell System divestiture and de-regulation of the 1970s in that it allows long-distance telephone companies to re-enter the local service market and the local companies, such as GTE, to enter the long distance market. Today software and advanced switching equipment make it possible for numerous competitive local telephone companies to interconnect and provide seamless communication. Changes to public law contained in the Act require all incumbent local telephone monopolies to interconnect with new competitors' networks.

The intention is that consumers will have more choices because competing companies will develop better technology and offer better service to their customers to keep them. And the customers served by this Act include users in the government - especially it provides for military bases and other users to select a service with self-healing SONET fiber optic rings

or to stay with non-redundant copper wires to reduce cost. Switching to a Competitive Local Exchange Carrier (CLEC) should be easy. The switchover will require neither a change in any phone numbers nor new equipment. The user will be able to elect to: access local fiber optic networks as well as select local, long distance and enhanced services from any number of providers. The act also provides for a wide range of services and media, including radio and television, broadcast, cable services, and most telecommunications services.

It addresses: unfair billing practices; privacy; facilities siting; mobile services access to long distance carriers; encouragement of advanced telecommunications capabilities; encouragement and support to the National Educational Telecommunications Funding Corporation. Finally it provides for a report to Congress by the Departments of Commerce, and Health and Human Services regarding studies and demonstrations on telemedicine funded by the Public Health Service or other Federal agencies. The report examines questions related to patient safety, the efficacy and quality of the services provided as well as other legal, medical, and economic issues related to the use of advanced telecommunications services for medical purposes. All of these provisions affect military readiness and ability to perform the mission either directly through telecommunications services, or indirectly through many personnel morale and welfare issues.

D.1.9 P.L. 104-106, Information Technology Management Reform Act of 1996, National Defense Authorization Act for Fiscal Year 1996, 10 February 1996

The Information Management Reform Act of 1996 (ITMRA) is a subordinate act (Division E) of the National Defense Authorization Act for Fiscal Year 1996. The ITMRA was later renamed the Clinger-Cohen Act. The ITMRA 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 ITMRA 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. Together with the Paperwork Reduction Act, as amended, the Acts explicitly outline OMB's responsibilities for overseeing agency practices regarding information privacy and security. The ITMRA also reemphasizes OMB, NIST and agency responsibilities regarding information security.

D.1.10 P.L. 104-201, National Defense Authorization Act for Fiscal Year 1997, 23 September, 1996

The National Defense Authorization Act for Fiscal Year 1997 (Subtitle F--Other Matters, Section 1061, Policy on Protection of National Information Infrastructure Against Strategic Attack) directs the President to submit a report to Congress which sets forth national policy on protecting the national information infrastructure against strategic attack. In addition to providing an update of a similar report requested in the 1996 Defense Authorization Act (Kyl Amendment), Congress asks the President to include the following in the policy:

- Plans to meet essential government and civilian needs during a national security emergency associated with a strategic attack against the NII.
- The identification of information infrastructure functions that must be performed during such an emergency.
- The assignment of responsibilities to federal departments and agencies and a description of the roles of government and industry relating to indications and warning, assessment, response to, and reconstitution after such an attack.
- Matters that are in need of further study and resolution such as technology and funding shortfalls.
- Legal and regulatory considerations relating to the national policy.

The National Defense Authorization Act for Fiscal Year 1997 (Section 1062, Information Systems Security Program) also directs the Secretary of Defense to allocate to the information systems security program (program element 0303140K) an amount equal to the percentages indicated below of the funds appropriated for the Defense Information Infrastructure (DII). The allocated funds are to be in addition to funds allocated to NSA and DARPA. Additionally, the Secretary is to submit a report to Congress, no later than November 15, 1997, on the information security activities of the DOD:

- For FY 99, 2.5%
- For FY 00, 3.0%
- For FY 01, 3.5%
- For FY 02, 4.0%.

D.1.11 P.L. 104 - 294, Title I, Economic Espionage Act of 1996, 11 October 1996

The Economic Espionage Act resolves many gaps and inadequacies in existing federal laws by specifically proscribing the various acts defined under economic espionage, and addressing the national security aspects of the crime. It also provides forfeiture of proceeds obtained as a result of economic espionage, preserves the confidentiality in any prosecution, and provides for extraterritorial jurisdiction. It makes the theft of trade secrets a federal crime and provides stiff penalties and prison sentences for specific acts of economic espionage. It also eliminates gaps in criminal laws covering attacks against computers and the information they contain.

D.1.12 P.L. 104-294, Title II, National Infrastructure Protection Act of 1996, 11 October, 1996

The NII Protection Act resulted from an Executive Branch initiative to address protecting the confidentiality, integrity, and availability of data and systems and revise the Computer Fraud and Abuse Act (18 U.S.C. 1030). Key changes to 18 USC 1030 include:

- Section 1030 (a) (1), the espionage clause, explains the criminality of the unauthorized use (insider or outsider) of a computer to obtain information that *could be used* to injure the U.S. Previous wording required proof that the information *is to be used to* injure the

U.S. One of the reasons for this lessened burden of proof is that violation of this clause carries with it only a maximum of 10-year imprisonment.

- Section 1030 (a) (2) is designed to protect the confidentiality of computer data. This is confidentiality as it relates to privacy. The DOD view of confidentiality relating to national security information is actually captured in Section 1030 (a) (1) which, as noted above, addresses computers used in espionage
- The 1994 amendment inadvertently may have decriminalized some activity when it replaced the former term “federal interest computer” with the term “ computer used in interstate commerce or communications.” The 1996 amendment introduces the term “protected computer” which includes government computers, financial institution computers, and any computer used in interstate or foreign commerce or communications.
- Section 1030 (a) (5). Both the 1994 and the 1996 amendments ensured that insider abuse, in excess of authority, was included. All insider abuse had been previously excluded from the provisions of this statute. Under the existing code, intentional damage is a felony, be it an insider or outsider. For an outsider, reckless damage is also a felony, while negligent damage is a misdemeanor. Reckless or negligent damage caused by insiders is not a federal crime. The rationale for this is there are a range of administrative sanctions (from firing to ...) available for insiders who recklessly or negligently cause damage. Federal sanctions are reserved for those insiders who intentionally cause damage.
- Under the 1994 amendment, “Damage” was considered to include financial losses in excess of \$5,000 and impact on medical treatment. The 1996 Act adds causing physical damage to any person and threatening public health and safety.
- "Threats to the normal operation of a computer" was added as Subsection 1030 (a) (7).
- The amendment explicitly maintains the status quo of the FBI and the Secret Service shared jurisdiction.

This page intentionally left blank.



Executive Orders

D.2 EXECUTIVE ORDERS

D.2.1 Executive Office of the President, Executive Order 12333, United States Intelligence Activities, The White House, Washington DC, 4 December 1981

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). DOD responsibilities include:

- 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.”
- Agencies of the Intelligence Community:
 - May provide specialized equipment, technical knowledge, or assistance of expert personnel to support law enforcement activities.

D.2.2 Executive Office of the President, Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, The White House, Washington D.C., 3 April, 1984

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, E.O. 12472 established the Committee of Principals for the Federal government to coordinate with the National Security Telecommunications Advisory Committee consisting of industry representatives. DOD responsibilities include:

- 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.
- 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.

D.2.3 Executive Office of the President, Executive Order 12958, Classified National Security Information, The White House, Washington D.C., 17 Apr 95

Executive Order 12958 outlines a uniform system for classifying, safeguarding, and declassifying national security information, to include who may classify or declassify and under what circumstances. The purpose of the Order is to prevent unauthorized disclosure of national security information and to prevent over-classification. 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. The baseline period for review for declassification is set at 10 years with specific categories of allowed exceptions. “Information” is defined as any information or material, regardless of its physical form or

characteristics. The document also directs that each head of agency establish uniform procedures to ensure the integrity of classified information processed by information systems and to prevent unauthorized access to such systems and data. Assigned responsibilities and functions include:

- 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
 - Appoint a senior agency official to administer its information security program.

D.2.4 Executive Office of the President, Executive Order 13010, Critical Infrastructure Protection, The White House, Washington D.C., 15 July 1996

The purpose of Executive Order 13010 is 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. The order establishes:

The *President's Commission on Critical Infrastructure Protection* consists 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 Director of the Office of Management and Budget
The Secretary of Defense	The Director of the Federal Emergency Management Agency
The Attorney General	The Assistant to the President for National Security Affairs
The Secretary of Commerce	The Assistant to the Vice President for National Security Affairs
The Secretary of Transportation	
The Secretary of Energy	
The Director of Central Intelligence	

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.

Assigned responsibilities and functions include:

- 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
 - Shall 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.

D.2.5 Executive Office of the President, Executive Order 13011, Federal Information Technology, The White House, Washington D.C., 16 July 1996

The E.O. requires agencies to significantly improve IT acquisition and management by faithfully implementing the relevant provisions of the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996. Agencies are to refocus IT planning to more directly support their strategic mission, implement a budget-linked capital planning and investment process and rethink the way they do their work before investing in information technology to support the work (business process reengineering). Agencies are also to establish clear accountability for IT management by creating agency Chief Information Officers (CIO). The E.O. establishes three groups:

- The CIO Council to improve agency practices on such matters as the design, modernization, use sharing, and performance of agency information resources.
- The Government Information Technology Services Board to ensure continued implementation of the IT recommendations of the National Performance Review.
- The Information Technology Resources Board to provide independent assessments of specific IT systems proposed or under development and make recommendations to the agency and OMB.

Under the E.O., DOD is required to:

- Establish mission-based performance measurers for IT investments, aligned with agency performance plans prepared pursuant to the Government Performance and Results Act
- Establish agency-wide and project-level management structures and processes that will be responsible and accountable for managing and evaluating investments in IT with authority to terminate troubles IT systems
- Support appropriate training
- Support the interagency structure established by the order
- Select CIO's
- Structure major information systems into projects as narrow in scope and brief in duration as practical to reduce promote flexibility and interoperability, and better match mission requirements with current technology.

 **Other National Policy**

D.3 OTHER NATIONAL POLICY

D.3.1 Presidential/National Security Directives

D.3.1.1 PD/NSC 24, Telecommunications Protection Policy (U), 16 Nov 77 (Partially declassified/released on 18 Feb 94)

[Superseded and canceled by NSDD 145; which, in turn, was superseded by NSD 42. Excepted from cancellation are mandated ongoing telecommunications protection activities]

UNCLASSIFIED ABSTRACT: PD 24 established the NSC Special Coordinating Committee, which evolved to become the NSTISSC. The SECDEF is appointed the Executive Agent for classified and unclassified national security information. The Secretary of Commerce is appointed the Executive Agent government-derived unclassified information (except national security information) and for dealing with the commercial and private sector to enhance communications protection and privacy. It establishes national telecommunications policy requiring:

- Classified information be transmitted only by secure means
- Unclassified information that would be useful to an adversary should be protected during transmission
- Non-governmental information that would be useful to an adversary shall be identified and the private sector informed and encouraged to take appropriate measures
- Responsible agencies work with the FCC and common carriers to adopt system capabilities which protect the privacy of individual communications
- Private sector telecommunications carriers should be briefed (DoC lead) on the nature of the threat and appropriate government R&D information shall be made available.

DOD responsibilities include:

- The SECDEF shall act as the executive agent for communications security (COMSEC) to protect government-derived classified information and government-derived unclassified information, which relates to national security. Through the industrial security program, initiate new and improved personal and telecommunications security measures among Defense contractors.
- Revitalizing security training for US government personnel who use telephones and other means of communications for both unclassified and classified purposes.
- Executing all measures required to assure the security of DOD telecommunications and the control of compromising emanations.

D.3.1.2 PDD/NSC 29, Security Policy Coordination, 16 Sep 94

PDD 29 revised the security policy process based upon the greater diversity of threats to U.S. national security following the end of the Cold War. It recognizes a broader range of issues that affect national security, including economic issues and the proliferation of technologies from those used to create weapons of mass destruction to information

technology. PDD 29 created the Security Policy Board. This Board addresses a variety of security issues, including information systems security and risk management. 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. 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 Office of Management and Budget is represented on the Security Policy Board and Forum and the Overseas Security Policy Board. The Information Security Oversight Office has a representative on the Security Policy Forum.

DOD membership includes:

- Security Policy Board: The Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff.
- Security Policy Forum: Senior representatives from the Office of the Secretary of Defense, the Joint Chiefs of Staff, each military Department including the U.S. Coast Guard, the Defense Intelligence Agency (DIA), the National Security Agency (NSA) and the Defense Information Systems Agency/National Communications System.
- Overseas Security Policy Board: DIA and NSA.

D.3.1.3 PDD 39, Secret, U.S. Policy on Counterterrorism, 1996

UNCLASSIFIED ABSTRACT: PDD 39 directs measures to combat terrorism. These include reducing vulnerabilities to terrorism, deterring and responding to terrorist acts, and having capabilities to prevent and manage the consequences of terrorist use of nuclear, biological and chemical (NBC) weapons, including those of mass destruction. Specific efforts include reviewing the vulnerability of government facilities and critical national infrastructure. The Director, FEMA will ensure that the Federal Response Plan is adequate for consequence management activities in response to terrorist attacks against large U.S. populations.

[Source: NSC approved unclassified FEMA abstract. Requested and publicly released by Senator Nunn]

D.3.1.4 PDD 62, Combating Terrorism, 22 May 98

PDD-62 addresses the national problem of countering terrorism in all its varied forms. It highlights the growing range of unconventional threats faced by the Nation, including newer forms of more familiar chemical, radiological, and biological weapons as well as the emergence of "cyber-terrorism." The directive creates a new and more systematic approach to defending against them. The first step is to create within the Executive Office of the President a new National Coordinator (for Security, Infrastructure Protection and Counter-Terrorism). This official is responsible for coordinating the government and private partnership, which will assure the national and economic security as well as the well being of its citizenry.

The new National Coordinator for Security, Infrastructure Protection and Counter-Terrorism reports to the President through the National Security Advisor and when the NSC Principals Committee meets on security issues, serves as a full member of that Cabinet-level committee. This new "Security Czar" will coordinate with other presidential advisors in their area of expertise to address key infrastructure support issues, especially: the Director of the Office of Scientific Technology and Policy; and cabinet secretaries in their roles as lead agencies for various sectors. The full new national IA structure is shown in Exhibit D-1.

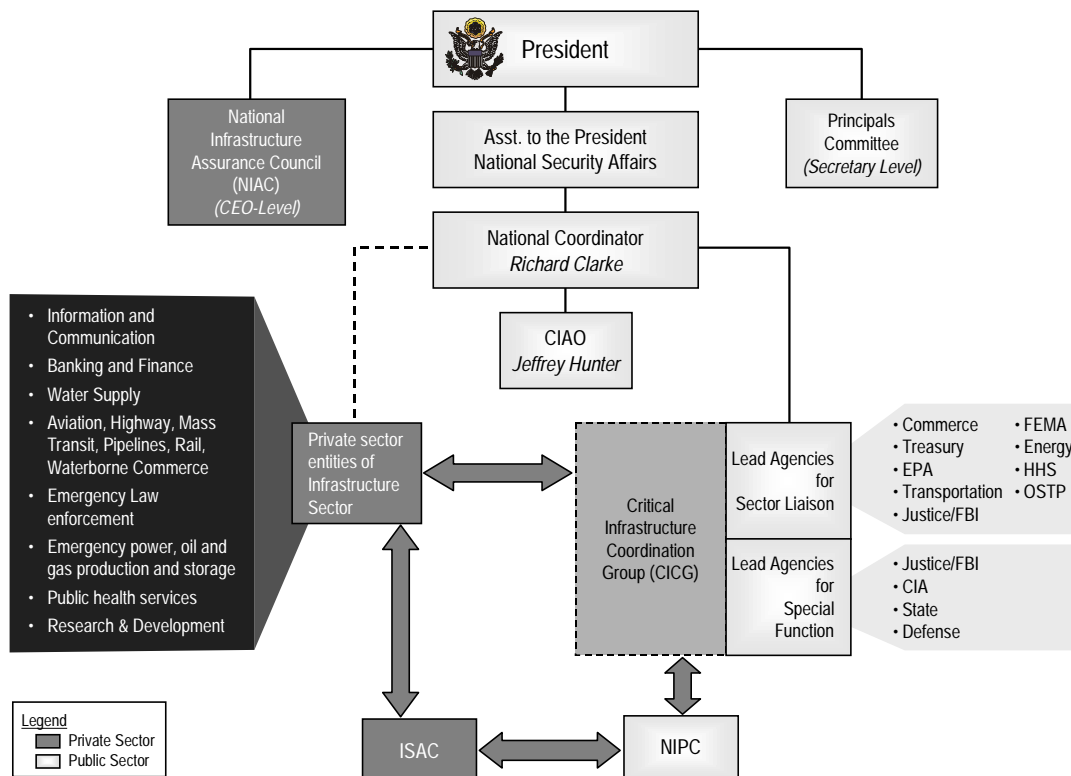


Exhibit D-1. National IA Structure

D.3.1.5 PDD 63, Protecting America's Critical Infrastructures, 22 May 98

PDD-63 focuses specifically on protecting the Nation's critical infrastructures from both physical and "cyber" attack. These attacks may come from foreign governments, foreign and domestic terrorist organizations, and foreign and domestic criminal organizations.

The National Coordinator oversees the efforts of the government in formulating the Federal Critical Infrastructure Protection (CIP) Plan and coordinating the National Plan for CIP with the private sector. The new national security structure for CIP brings together the efforts of the National Infrastructure Assurance Council, the Critical Infrastructure Coordination Group, the National Security Telecommunication Advisory Committee, the Manager of the National Communications System, and lead cabinet agencies for special functions and infrastructure industries. The infrastructure sectors and their respective federal lead agencies are:

<i>Infrastructure Sector</i>	<i>Lead Federal Agency</i>
<i>Banking and Finance</i>	<i>Department of Treasury</i>
<i>Transportation</i>	<i>Department of Transportation</i>
<i>Electric and Gas & Oil Pipelines</i>	<i>Department of Energy</i>
<i>Information/Communications</i>	<i>Departments of Commerce and Defense</i>
<i>Government Services</i>	<i>General Services Administration</i>
<i>Fire and Other Emergency Services</i>	<i>Federal Emergency Management Agency</i>
<i>Public Health Services</i>	<i>Department of Health and Human Services</i>
<i>Water Supplies</i>	<i>Environmental Protection Agency</i>

The proponents of special functions are:

<i>Special Function</i>	<i>Lead Federal Agency</i>
<i>Law Enforcement and Internal Security</i>	<i>Department of Justice</i>
<i>National Defense</i>	<i>Department of Defense</i>
<i>Intelligence</i>	<i>The Central Intelligence Agency</i>
<i>Foreign Affairs</i>	<i>Department of State</i>

The directive set up the Critical Infrastructure Assurance Office (CIAO) under the Department of Commerce and the National Infrastructure Protection Center (NIPC) under the sponsorship and guidance of the Federal Bureau of Investigation (FBI). Finally, because the Government has not received a Congressional mandate to regulate infrastructure industries, the directive lays out the framework for a *voluntary* Information Sharing and Analysis Center (ISAC), which will help to coordinate information and efforts toward addressed CIP issues.

D.3.1.6 NSD 42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 Jul 90

Issued, in part, to bring executive policy in-line with the Computer Security Act of 1987, this directive establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation. It establishes a mechanism for policy development and dissemination; and assigns responsibilities for its implementation. NSD 42 establishes the NSC Policy Coordinating Committee for National Security Telecommunications and Information Systems (NSTISSC). Except for ongoing telecommunications protection activities mandated by and pursuant to PDD 24 and NSDD-145, NSDD-145 is rescinded. [PD-24 was rescinded by NSDD 145]

Responsibilities

- The NSTISSC shall develop specific operating policies, procedures, guidelines, instructions, standards, and priorities as may be required to implement the directive; provide systems security guidance for national security systems to Executive departments and agencies; submit annually to the Executive Agent and evaluation of the security status of national security systems...; approve the release of cryptologic national security systems technical security material, information and techniques to foreign governments.
- The Executive Agent (SECDEF) shall: ensure the development of plans and programs to fulfill the objectives of the directive; procure and provide technical security material, assistance and services necessary to the accomplish the objectives of the directive; approve and provide minimum security standards and doctrine for systems subject to this directive; conduct research, etc.; operate or coordinate the efforts of U.S. government technical centers related to national security telecommunications and information systems security.
- The National Manager (DIRNSA) shall examine:
 - U.S. government national security systems and evaluate their vulnerability to foreign interception and exploitation;
 - Act as the U.S. government focal point for cryptography, telecommunications systems security, and information systems security for national security systems;
 - Review and approve standards, etc.;
 - Conduct foreign computer security and communications security liaison, including entering into agreements with foreign governments and with international and private organizations regarding national security systems (exception - intelligence);
 - Assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems; operate a central technical center to evaluate and certify the security of national security telecommunications and information systems;
 - Prescribe minimum standards, methods and procedures for protection;
 - Review and assess annually the programs and budgets of executive departments and agencies for national-security telecommunications systems security; coordinate with NIST in accordance with Computer Security Act of 1987.

- The Heads of Executive Departments and Agencies shall be responsible for achieving and maintaining secure national security systems within their departments or agencies; ensure policies, procedures, guidelines, etc. are implemented; provide appropriate information to the NSTISSC.
- The Director, OMB shall specify data to be provided during the annual budget review by executive departments and agencies on program budgets relating to security of their national security systems; consolidate and provide such data to the National Manager via the Executive Agent; review for consistency with this directive, and amend as appropriate, OMB policies and regulations which may pertain to the subject matter.

D.3.2 Office of Management and Budget

D.3.2.1 Office of Management and Budget, OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, Executive Office of the President, Publication Services, 9 Jul 90

OMB Bulletin 90-08 was incorporated, updated and superseded by Circular A-130, however, pending further guidance from NIST (a security planning FIPS), Agencies are to follow the guidance in 90-08 for completing the technical portions of their Security Plans as well as the guidance on technical security controls.

D.3.2.2 Office of Management and Budget, OMB Circular A-76, "Performance of Commercial Activities," Executive Office of the President, Publication Services, 4 Aug 83

This Circular establishes Federal policy regarding the performance of commercial activities. It is the policy of the United States Government to:

- **Achieve Economy and Enhance Productivity.** Competition enhances quality, economy, and productivity. Whenever commercial sector performance of a Government operated commercial activity is permissible, in accordance with this Circular and its Supplement, comparison of the cost of contracting and the cost of in-house performance shall be performed to determine who will do the work.
- **Retain Governmental Functions In-House.** Certain functions are inherently Governmental in nature, being so intimately related to the public interest as to mandate performance only by Federal employees. These functions are not in competition with the commercial sector. Therefore, these functions shall be performed by Government employees.
- **Rely on the Commercial Sector.** The Federal Government shall rely on commercially available sources to provide commercial products and services. In accordance with the provisions of this Circular, the Government shall not start or carry on any activity to provide a commercial product or service if the product or service can be procured more economically from a commercial source.

The critical definition for DOD implementation of this Circular, especially regarding IA, is that of Government performance of a commercial activity. It is "one which is operated by a Federal executive agency and which provides a product or service which could be obtained from a commercial source. A commercial activity is not a Governmental function."

The following activities are defined as commercial activities, which require a cost-benefit analysis and decision on outsourcing or other appropriate action.

- **Automatic Data Processing**
 - ADP services - batch processing, time-sharing, facility management, etc.
 - Programming and systems analysis, design, development, and simulation
 - Key punching, data entry, transmission, and teleprocessing services
 - Systems engineering and installation
 - Equipment installation, operation, and maintenance.
- **Security**
 - Guard and protective services
 - Systems engineering, installation, and maintenance of security systems and individual
 - Privacy systems
 - Forensic laboratories.
- **Special Studies and Analyses**
 - Cost benefit analyses
 - Statistical analyses
 - Scientific data studies
 - Regulatory studies
 - Defense, education, energy studies
 - Legal/litigation studies
 - Management studies.
- **Systems Engineering, Installation, Operation, Maintenance, and Testing**
 - Communications systems - voice, message, data, radio, wire, microwave, and satellite
 - Missile ranges
 - Satellite tracking and data acquisition
 - Radar detection and tracking
 - Television systems - studio and transmission equipment, distribution systems, receivers, antennas, etc.

D.3.2.3 Office of Management and Budget, Supplement to OMB Circular A-76, "Performance of Commercial Activities," Executive Office of the President, Publication Services, 8 Feb 96

As noted in the Vice President's Third Report of the National Performance Review, "Common Sense Government: Works Better and Costs Less," (September 1995), Americans want to "get their money's worth" and want a Government that is more businesslike and better managed. The reinvention of Government begins by focusing on core mission

competencies and service requirements. Thus, the reinvention process must consider a wide range of options, including: consolidation, restructuring or reengineering of activities, privatization options, make or buy decisions, the adoption of better business management practices, the development of joint ventures with the private sector, asset sales, the possible devolution of activities to State and local governments and the termination of obsolete services or programs. In the context of this larger reinvention effort, the scope of this Supplemental Handbook is limited to the conversion of recurring commercial activities to or from in-house, contract or ISSA performance. Circular A-76 is not designed to simply contract out. Rather, it is designed to: (1) balance the interests of the parties to a make or buy cost comparison, (2) provide a level playing field between public and private offerors to a competition, and (3) encourage competition and choice in the management and performance of commercial activities. It is designed to empower Federal managers to make sound and justifiable business decisions.

While the 1983 Circular establishes Federal policy for the performance of recurring commercial activities, this Supplement to the Circular replaces the Handbook issued with the 1983 Circular and provides updated guidance and procedures for determining whether recurring commercial activities should be operated under contract with commercial sources, in-house using Government facilities and personnel, or through interservice support agreements (ISSAs). The Revised Supplemental Handbook is an integral part of the 1983 Circular.

The Supplement to the Circular sets forth procedures for determining whether commercial activities should be performed under contract with commercial sources or in-house using Government facilities and personnel. A decision on the proper means of performing a commercial activity may omit a cost-benefit analysis under any of the following conditions.

National Defense

- The Secretary of Defense shall establish criteria for determining when Government performance of a commercial activity is required for national defense reasons. Such criteria shall be furnished to the Office of Federal Procurement Policy, OMB, upon request.
- Only the Secretary of Defense or his designee has the authority to exempt commercial activities for national defense reasons.

D.3.2.4 Office of Management and Budget, OMB Circular A-123, Management Accountability and Control, Executive Office of the President, Publication Services, 21 June 95

OMB Circular A-123 implements the Federal Managers' Financial Integrity Act (FMFIA). 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. Circular A-130 requires a review of security controls for each system whenever significant changes are made to a system, but at least every three years. If the review reveals that there is no assignment of security responsibility, no security plan, or no authorization to process for a system, consideration should be given to identifying a deficiency pursuant to OMB Circular 123 and the FMFIA.

D.3.2.5 Office of Management and Budget, OMB Circular A-130, Management of Federal Information Resources, Executive Office of the President, Publication Services, 8 Feb 96

This Circular establishes policy for the Management of Federal Information Resources. Appendix III (*Security of Federal Automated Information Resources*) reflects a major revision of procedures found in the previous circular. It incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives. Appendix III establishes a minimum set of management controls that are to be included in federal automated information security programs. These include assigning responsibility for security, developing a system security plan, screening and training individual users, assessing risk, planning for disasters and contingencies, and reviewing security safeguards at least every three years. It recognizes that all federal computer systems require some level of protection. It also requires agencies to clearly define responsibilities and expected behavior for all individuals with access to automated systems and to implement security incident response and reporting capabilities. Specific procedural and analytic guidance is provided for implementing Federal automated information security programs, assignment of agency responsibilities for security of automated information. Appendix III also links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123. DOD shall:

- Develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.
- Provide appropriate technical advice and assistance (including work products) to the Department of Commerce (DoC).
- Assist the DoC in evaluating the vulnerabilities of emerging information technologies.

As a Federal agency, DOD responsibilities under A-130 include:

- Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the paperwork Reduction Act (44 U.S.C. 3506)
- 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

- As part of the plan, establish a set of rules of behavior for individual users of each general support system. Rules should clearly delineate responsibilities of and expectations for all individuals with access to the he system. They should state the consequences of noncompliance.
 - » Review the Security Controls (at least every three years or when significant modifications are made to the system)
 - » 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)
 - » Ensure that a Management Official Authorizes in Writing the Use of the Application.

D.3.3 National Institute of Standards and Technology

D.3.3.1 National Institute of Standards and Technology (NIST), NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995

Referenced frequently in Appendix III, OMB Circular A-130, 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.

D.3.3.2 National Institute of Standards and Technology (NIST), NIST Special Publication 800-13, Telecommunications Security Guidelines for Telecommunications Management Network, October 1995

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.

D.3.3.3 National Institute of Standards and Technology (NIST), Generally Accepted Principles and Practices for Security Information Technology Systems (Draft), 18 December 95

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.

D.3.4 National Security Telecommunications and Information Systems Security Committee

D.3.4.1 NCSC-1, National Policy For Safeguarding and Control of Communications Security Material, 16 Jan 81

Published by the National Communications Security Committee, this National Policy encourages the use of COMSEC materials and techniques and to safeguard and control COMSEC materials in a manner which assures their continued integrity, prevents access by unauthorized persons and controls the spread of COMSEC materials, techniques and technology when not in the best interests of the US or its allies. DOD responsibilities include:

- Each department or agency holding COMSEC keying material must establish a COMSEC Material Control System into which all COMSEC keying material must be placed.
- NSA will:
 - Prescribe minimum security standards for performance of Central Office of Record functions by Federal Department and Agencies
 - Establish procedures for reporting and evaluating communications security weaknesses
 - Establish doctrine and procedures to protect COMSEC information.

D.3.4.2 NCSC-5 w/ App 1 and 2, National Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments, 16 Jan 81

Published by the National Communications Security Committee, NCSC-5 establishes policy for the use of machine cryptosystems in high-risk environments. It requires that NSA promulgated factors for machine selection be considered, that workable plans be developed to protect, evacuate, or destroy COMSEC equipments and materials, that only the minimum amount of mission essential COMSEC material be located in the high risk environment, and that point-to-point keying material will be used. Appendix 1 is entitled *Guidelines for Identifying High Risk Environments (U)*. DOD responsibilities include:

- Identifying high-risk areas where machine cryptosystems may be used
- Applying the NSA criteria in the selection of machine cryptosystems
- Assuring that only the minimum amount of mission essential COMSEC material is located in high risk environments
- Assuring that workable plans are developed to protect, evacuate, or destroy COMSEC equipments and materials and notifying COMSEC authorities of loss, damage, capture, or compromise
- DIRNSA will coordinate in establishing standardized criteria for the identification of high-risk environments
- DIRNSA will establish and publish criteria for the selection of machine cryptosystems for use in high-risk environments. (Appendix 2 provides this criteria)
- DIRNSA will maintain oversight.

D.3.4.3 NCSC-11, National Policy for the Protection of Telecommunications Systems Handling Unclassified National Security-Related Information (U), 3 May 82

Requires all national security-related information to be protected commensurate with associated exploitation risks. Department and agency heads are responsible for deciding which of their transmittable unclassified information is national security related.

[Note: This Policy predates the Computer Security Act of 1987 and NSD 42, which brought administration policy in line with the CSA. The phrase “unclassified national security-related (UNS-R) information” is not in common use. Caution, therefore, should be used when quoting this “national policy”]

D.3.4.4 NCSC-8, Confidential, National Policy on Securing Voice Communications (U), 7 May 82

UNCLASSIFIED ABSTRACT: Not available.

D.3.4.5 NACAM - 83/1, Confidential, Advisory Memorandum on Protection of COMSEC Information Related to Foreign Governments and International Organizations (U), 10 Jun 83

UNCLASSIFIED ABSTRACT: NACAM-83/1 complements NCSC-6.

D.3.4.6 NCSC-2, National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources, 7 Jul 83

Published by the National Communications Security Committee, this National Policy states that COMSEC operations will normally be conducted by government personnel and limits the release of COMSEC material and information to nongovernmental sources. Nongovernment individuals granted access to classified COMSEC information must be U.S. citizens and must hold a final Government security clearance for the level of classification. All individuals granted access to COMSEC information must be briefed at least annually

regarding the unique nature of COMSEC information and their security responsibilities. DOD responsibilities include:

- Ensuring the requirements of the policy are met and determining that releases are in the best interests of the government
- Maintaining records of releases and notifying NSA
- Ensuring contractor performances meets established COMSEC standards and doctrine
- Incorporating policy criteria into all contracts. NSA will maintain a consolidated record of COMSEC contract and release notices, approve waivers from established physical security measures for the protection of COMSEC material, and provide assistance to other agency Heads.

D.3.4.7 NACAM - 84/1, Advisory Memorandum on Protection of Unclassified National Security-Related Telecommunications, 11 May 84

[Out of date advisory. UNS-R is no longer in use. Published in advance of NSDD-145 which was subsequently superseded.]

Published by the National Communications Security Committee, the advisory memorandum reminds that national security-related information of value to an adversary will be given protection commensurate with the associated risks of exploitation. The heads of departments and agencies are responsible for deciding which of their unclassified information intended for transmission is related to national security. The NACAM provides guidelines to identify telecommunications which contain unclassified national security-related (UNS-R) information that is useful to an adversary. The guidelines apply only to information which is being electrically transmitted.

D.3.4.8 NTISSP No 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems, 17 Jun 85

The *National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems* states that Government and Government contractor national security information that is transmitted over satellite circuits shall be protected from unauthorized intercept by approved techniques.

- *NTISSP No. 1* designates the National Security Agency as having primary responsibility for coordinating with the heads of departments or agencies to assess space systems telecommunication and command/control uplink function vulnerabilities and providing approved protection techniques and guidance.

D.3.4.9 NTISSP No 200, National Policy On Controlled Access Protection, 15 Jul 87

[This policy preceded the Computer Security Act of 1987 which assigns responsibility for sensitive unclassified information to DoC/NIST. A draft replacement is in coordination.]

Establishes a policy requiring that all automated information systems accessed by multiple users with varying levels of authorization to access classified or sensitive unclassified information provide automated Controlled Access Protection within five years. Controlled Access Protection is the C2 level of protection described in the Trusted Computer System Evaluation Criteria. Major characteristics include:

- Individual accountability through identification and authentication of each user
- Maintenance of audit trails of security-relevant events
- An ability to control a user's access to information according to the authorization the user has
- Preventing one user from obtaining another user's data.

Exceptions are authorized where the software or hardware security features are prohibitively costly, technically unsound, or may adversely impact operational requirements. Heads of departments are cautioned to continue to make progress toward reducing the circumstances that make the exception necessary.

D.3.4.10 NSTISSP No 100, Confidential, National Policy on Application of Communications Security to Command Destruct Systems (U), 17 Feb 88

UNCLASSIFIED ABSTRACT: Not available.

D.3.4.11 NTISSP No 3, FOUO, National Policy for Granting Access to US Classified Cryptographic Information, 19 Dec 88

Establishes a program governing access to U.S. classified cryptographic information for the purpose of preventing loss or unauthorized disclosure of U.S. classified cryptographic information. DOD responsibilities include:

- Implement policy
- Maintain capability to administer polygraph examinations
- Develop and maintain a cryptographic access briefing and certification
- Require reporting of unofficial foreign travel.

D.3.4.12 NSTISSD No 600, FOUO, Communications Security (COMSEC) Monitoring, 10 Apr 90

NSA is authorized to conduct COMSEC monitoring of government telecommunications systems to evaluate their vulnerability to hostile interception and exploitation. This directive establishes policy and basic procedures and assigns responsibilities for COMSEC monitoring operations. The policy precludes COMSEC monitoring for content or to produce foreign intelligence or counterintelligence. Users must be properly notified in advance that their use of monitored systems constitutes consent to monitoring for COMSEC purposes. Notification procedures are specified. The policy emphasizes legal constraints and requires Attorney General and legal counsel review. Public telecommunications, electronic surveillance, government telecommunications, contents, and nonpublic

communications are defined. Heads of departments and agencies shall develop procedures, provide for and conduct COMSEC monitoring operations and notify biennially the National Manager (DIRNSA) those organizations whose personnel and contractors that have been notified. DOD responsibilities include:

- The National Manager (DIRNSA) will:
 - Advise and assist other departments and agencies
 - Conduct COMSEC monitoring of government telecommunications IAW law and guidelines
 - Authorize and conduct emergency COMSEC monitoring of specific public telecommunications of the government prior to receiving certification when a delay may have serious impact upon national security interests or a threat to human life.

D.3.4.13 NSTISSP No 4, FOUO, National Policy on Electronic Keying, 16 Nov 92

Establishes a policy to reduce the operational and security vulnerabilities associate with the use of tangible keying materials through the development, dissemination and universal adoption of electronic keying methods.

- DOD departments and agencies will plan, program, fund, implement, and manage electronic keying programs.

D.3.4.14 NSTISSD No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals, 16 Nov 92

NSTISSD 501 establishes the requirement for federal departments and agencies to implement training programs for information systems security (INFOSEC) professionals. For the purposes of the directive, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during each phase of the life cycle.

D.3.4.15 NSTISSD No. 502, National Security Telecommunications and Automated Information Systems Security, 5 Feb 93

NSTISSD 502 delineates and clarifies the objectives, policies, procedures, standards, and terminology as set forth in NSD 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (See NSD 42, 5 Jul 90).

D.3.4.16 NSTISSD No. 500, FOUO, Information Systems Security (INFOSEC) Education, Training and Awareness, 25 Feb 93

Establishes a policy requiring Federal departments and agencies to develop and implement information systems security (INFOSEC) education, training and awareness programs for national security systems. The policy identifies the employee as the essential element of a successful protection program and requires an initial orientation, advanced education and

training commensurate with duties and responsibilities, and reinforcement activities. Key responsibilities include:

- Federal departments and agencies will implement education, training and awareness programs in accordance with National Manager guidelines, require contractors, to include contract specifications, to comply with the policy, and provide information copies of training materials to the National Manager.
- The National Manager (DIRNSA) will develop INFOSEC program guidelines, ensure that training materials are developed, collect and share information on INFOSEC programs, and develop and conduct or assist other federal departments and agencies in developing and conducting INFOSEC activities.

D.3.4.17 NSTISSD No. 501, National Training Program for Information Systems Security (INFOSEC) Professionals

Not available.

D.3.4.18 NSTISSP No. 5, FOUO, National Policy for Incident Response and Vulnerability Reporting for National Security Systems, 30 Aug 93

Establishes the policy requiring agencies and departments involved with national security systems to collaborate and cooperate with other appropriate organizations in the sharing of incident, vulnerability, threat, and countermeasures information concerning these systems. The objectives are to contain and minimize the impact of security incidents on national security systems and eliminate or minimize vulnerabilities among national security systems.

D.3.4.19 NSTISSD No. 503, FOUO, Incident Response and Vulnerability Reporting for National Security Systems, 30 Aug 93

This Directive establishes the National Security Information Systems Incident Program (NSISIP) to provide a strategy for responding to information systems security incidents and vulnerabilities among national security systems. National Security systems are as defined in NSD 42 which includes both classified systems and Title 10, section 2315 systems (Warner Exempt). The NSISIP puts in place a National Security Incident Response Center (NSIRC) whose primary purpose is to provide expert assistance in isolating, containing, and eliminating incidents that threaten the integrity, availability, or confidentiality of national security systems. A SIRC provides incident response service for its constituency at the agency level. The NSIRC responds to requests for SIRC for expert assistance in handling incidents that are beyond the technical capability or organizational scope. SIRCs also use the NSISIP to share information with the NSIRC about incidents that are likely to threaten the national security systems. DOD responsibilities include:

- The National Manager (DIRNSA) shall oversee the program
- Federal departments and agencies involved with national security systems will establish a Security Incident Response Capability (SIRC).

D.3.4.20 NSTISSP No. 300, FOUO, National Policy On Control of Compromising Emanations, 29 Nov 93

Establishes a policy requiring Federal departments and agencies, including contractors, to use TEMPEST countermeasures in proportion to the threat of exploitation and associated potential damage. Within the United States only the most critical information will be protected by implementation or countermeasures which entail cost. Departments and agencies are required to exchange technical information, coordinate and consolidate programs in order to obtain maximum effectiveness by the most economical means. Key responsibilities include:

- Heads of U.S. government departments and agencies: Manage a single compromising emanations control program. The program should include evaluations to determine the need for TEMPEST countermeasures, appointing a Certified TEMPEST Technical Authority (CTTA), providing the CTTA name to the TEMPEST Advisory Group, and forwarding any information to the National Manager related to the TEMPEST threat.
- The National Manager (DIRNSA) will certify the TEMPEST acceptability of cryptographic equipment, operate a National TEMPEST Information Center, encourage industry to voluntarily develop systems that satisfy TEMPEST standards, manage a CTTA training program, publish an annual assessment of the domestic and foreign TEMPEST threat, and provide guidance.
- The FBI will provide a list to the National Manager of the locations within the U.S. maintained by countries on the national Security Threat List of countries.
- The TEMPEST Advisory Group will recommend countermeasures that correlate with the threat and provide a forum for the exchange of TEMPEST information.

D.3.4.21 NSTISSI No. 7000, Confidential NOFORN, TEMPEST Countermeasures for Facilities (U), 29 Nov 93

UNCLASSIFIED ABSTRACT: Electronic and electromechanical information processing equipment can produce unintentional intelligence-bearing emanations, commonly known as TEMPEST. If intercepted and analyzed, these emanations may disclose information transmitted, received, handled, or otherwise processed by the equipment. NSTISSI 7000 establishes guidelines and procedures that shall be used by departments and agencies to determine the applicable TEMPEST countermeasures for national security systems.

D.3.4.22 NSTISSP No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems, 8 Apr 94

Establishes a policy requiring all departments and agencies to establish and implement programs that mandate the certification and accreditation of national security systems under their control. The C&A programs shall ensure that information processed, stored, or transmitted by national security systems is adequately protected with respect to requirements for confidentiality, integrity, and availability. National security systems, are as defined in the national INFOSEC Glossary, and include both classified systems and Title

10, section 2315 systems (Warner Exempt). The policy also defines accreditation, certification, and Designated Approving Authority.

D.3.4.23 NSTISSP No. 7, National Policy on Secure Electronic Messaging Services, 21 Feb 95

Establishes a policy requiring Federal government departments and agencies to establish and implement a program for secure government-wide interoperable electronic messaging service for the protection of information contained on national security systems. It defines electronic messaging services as those which, in addition to providing interpersonal messaging capability, meet specified functional, management and technical requirements and, taken together, yield a business-quality electronic mail service suitable for the conduct of official government business.

D.3.4.24 NSTISSI No. 4011, National Training Standard for Information Systems Security (INFOSEC) Professionals, 20 Jun 94

This instruction provides the minimum course content for the training of information systems security (INFOSEC) professionals in the disciplines of telecommunications security and automated information systems (AIS) security. NSTISSD 501 establishes the requirement for federal departments and agencies to implement training programs for INFOSEC professionals. As defined in NSTISSD 501, an INFOSEC professional is an individual who is responsible for the security oversight or management of national security systems during phases of the life cycle. That directive is being implemented in a synergistic environment among departments and agencies, which are committed to satisfying these INFOSEC education and training requirements in the most effective and efficient manner possible.

This instruction is the first in a series of minimum training and education standards, being developed to assist departments and agencies in meeting their responsibilities in these areas. It is available electronically at http://constitution.ncsc.mil/wws/nstissc/html/nstissc_library.html.

D.3.4.25 NSTISSI No. 4009, National Information Systems Security Glossary, August 1997

This NSTISSI defines INFOSEC related terms and acronyms. It is a complete revision of the glossary that the NSTISSC Glossary Working Group last issued as NSTISSI 4009 in 1992 and 1996. To remain useful, a glossary must be in a continuous state of coordination and review to keep pace with changes in information systems security terminology. It incorporates as new terms as they come into being and old terms fall into disuse or change meaning. Some terms from the previous version were deleted, others updated or added, and some are identified as candidates for deletion. It is available electronically at http://constitution.ncsc.mil/wws/nstissc/html/nstissc_library.html.

D.3.4.26 NSTISSI No. 4012, National Training Standard for Designated Approving Authority (DAA), August 1997

This instruction is the second in a series of minimum training and education standards, which are being developed to assist departments and agencies in meeting their responsibilities in these areas. This instruction provides the minimum course content for the training of information systems Designated Approving Authority (DAA). This standard uses the requirements for Job functions using competencies identified in:

- DoD 5200.28-M, Automated Data Processing Security Manual
- NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities For Automated Information Systems
- NCSC-TG-029, Version 1, Introduction to Certification and Accreditation
- NCSC-TG-005, Trusted Network Interpretation
- FIPS Publication 102, Guideline for Computer Security Certification and Accreditation.

As specified in the NSTISSI the INFOSEC functions of a DAA are:

- Granting final approval to operate an IS or network in a specified security mode.
- Reviewing the accreditation documentation to confirm that the residual risk is within acceptable limits.
- Verifying that each Information System complies with the IS security requirements, as reported by the Information Systems Security Officer (ISSO).
- Ensuring the establishment, administration, and coordination of security for systems that agency, service, or command personnel or contractors operate.
- Ensuring that the Program Manager (PM) defines the system security requirements for acquisitions.
- Assigning INFOSEC responsibilities to the individuals reporting directly to the DAA.
- Approving the classification level required for applications implemented in a network environment.
- Approving additional security services necessary to interconnect to external systems (e.g., encryption and non-repudiation).
- Reviewing the accreditation plan and signing the accreditation for the network and each IS.
- Defining the criticality and sensitivity levels of each IS.
- Reviewing the documentation to ensure each IS supports the security requirements as defined in the IS and network security programs.
- Allocating resources to achieve an acceptable level of security and to remedy security deficiencies.
- Establishing working groups, when necessary, to resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of conditions or agreements in Memoranda of Agreement (MOA).
- Ensuring that, when classified or sensitive but unclassified information is exchanged between logically connected components, the content of this communication is protected from unauthorized observation by acceptable means, such as cryptography, and Protected Distribution Systems (PDS).

A DAA, who is given a final report requesting approval to operate a hypothetical information system at a specified level of trust, should be able to analyze and judge the information for validity and reliability to ensure the hypothetical system will operate at the proposed level of trust. This judgement will be made based on system architecture, system security measures, system operations policy, system security management plan, and provisions for system operator and end user training. It is available electronically at http://constitution.ncsc.mil/www/nstissc/html/nstissc_library.html.

D.3.4.27 NSTISSI No. 4013, National Training Standard for System Administrators in Information Systems Security (INFOSEC), August 1997

This instruction is the third in a series of minimum training and education standards, which are being developed to assist departments and agencies in meeting their responsibilities in these areas. This instruction provides the minimum course content for the training of information systems administrators.

As specified in the NSTISSI the minimal INFOSEC performance standard for the job functions of system administrators includes:

- Working closely with the Information Systems Security Officer (ISSO) to ensure the Information System or network is used securely.
- Participating in the Information Systems Security incident reporting program.
- Assisting the ISSO in maintaining configuration control of the systems and applications software.
- Advising the ISSO of security anomalies or integrity loopholes.
- Administering, when applicable, user identification or authentication mechanism(s) of the IS or network.

A System Administrator, who is given various simulated scenarios and typical situations containing information systems security issues, should be able to describe and apply the appropriate actions to manage and administer the IS(s) in a secure manner. To be acceptable, the description must be in accordance with applicable INFOSEC regulations, policies, and guidelines. The NSTISSI gives a full and detailed list of performance items under competencies in each of the competency areas for the job functions. It is available electronically at http://constitution.ncsc.mil/www/nstissc/html/nstissc_library.html.

D.3.4.28 NSTISSI No. 4014, National Training Standard for Information Systems Security Officers (ISSO), August 1994

This instruction is the fourth in a series of minimum training and education standards, which are being developed to assist departments and agencies in meeting their responsibilities in these areas. This instruction provides the minimum course content for the training of information systems security officers. This standard uses the requirements for Job functions using competencies identified in:

- DoD 5200.28-M, Automated Data Processing Security Manual
- NCSC-TG-027, Version 1, A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems
- DCID 1-16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks.

The INFOSEC functions of an ISSO are:

- Maintaining a plan for site security improvements and progress towards meeting the accreditation.
- Ensuring the IS is operated, used, maintained, and disposed of in accordance with security policies and practices.
- Ensuring the IS is accredited and certified, if it processes sensitive information.
- Ensuring users and system support personnel have the required security clearances, authorization and need-to-know; are indoctrinated; and are familiar with internal security practices before access to the IS is granted.
- Enforcing security policies and safeguards on all personnel having access to the IS for which the ISSO is responsible.
- Ensuring audit trails are reviewed periodically (e.g., weekly, daily), and audit records are archived for future reference, if required.
- Initiating protective or corrective measures.
- Reporting security incidents in accordance with agency-specific policy, such as DOD 5200.1R, to the designated approving authority (DAA) when an IS is compromised.
- Reporting the security status of an IS, as required by the DAA.
- Evaluating known vulnerabilities to ascertain if additional safeguards are needed.

The Job performance objectives vary with the experience level of the ISSO.

At the ENTRY LEVEL: Given a series of hypothetical system security breaches, the ISSO should be able to identify system vulnerabilities and recommend security solutions required to return the systems to operational level of trust.

At the INTERMEDIATE LEVEL: Given a proposed new system architecture requirement, the ISSO should be able to investigate and document system security technology, policy and training requirements to assure system operation at a specified level of trust.

At the ADVANCED LEVEL: Given a proposed IS accreditation action, the ISSO should be able to analyze and evaluate the system security technology, policy, and training requirements in support of DAA approval to operate the system at a specified level of trust. This analysis will include a description of the management/technology team required to successfully complete the accreditation process.

The NSTISSI gives a full and detailed list of performance items under competencies in each of the competency areas for the job functions. It is available electronically at http://constitution.ncsc.mil/wws/nstissc/html/nstissc_library.html.

This page intentionally left blank.



Department of Defense

D.4 DEPARTMENT OF DEFENSE

D.4.1 DoDD TS-3600.1, Top Secret NOFORN, Information Warfare (U), 21 Dec 92

Superseded by DoDD S-3600.1.

D.4.2 DoDD S-3600.1 Secret NOFORN, Information Operations (U), 9 December 1996

UNCLASSIFIED ABSTRACT: On 9 December 1996, Deputy Secretary of Defense White signed out DoD Directive S-3600.1, *Information Operations*, updating DOD policy on Information Operations (IO) and Information Warfare (IW) and superseding DoD Directive TS-3600.1, *Information Warfare*, dated 21 December 1992.

The revised directive reflected the conceptual evolution as well as a general convergence in understanding and approach to IO within the DOD. This concept of IO is depicted in the Exhibit D-2 below.

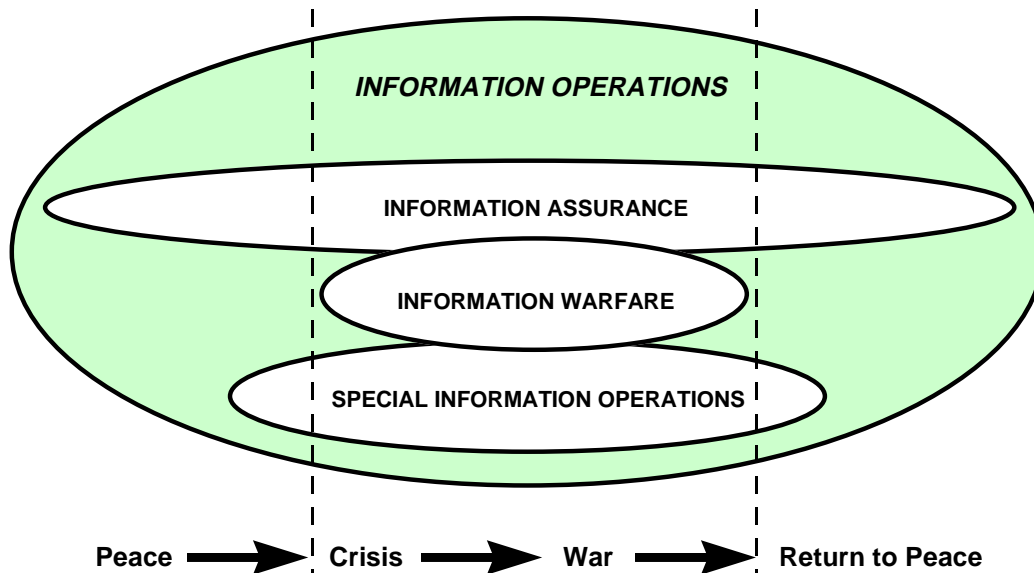


Exhibit D-2. Information Operations

The revised directive embraced IO, a term that already had a place in some Service doctrine, as an umbrella term inclusive of the universe of defensive and offensive information activities within the information environment. The concept also distinctly separated peacetime information operations and information warfare activities during crisis and war. Information Assurance (IA); encompassing what was previously peacetime defensive information warfare activities, would facilitate coordination with those outside of DOD, such as the civil agencies of the Federal government, industry and the public. At times, it had proven difficult to address *defensive information warfare* issues with those for whom *warfare* was not a normal part of their mission or culture. The adoption of IA reflects the recognition that IO is larger than DOD and that successful IO, particularly IA, depends upon the integration and cooperation of DOD, Federal, industry and public efforts. At the

same time, the concept of IA portrayed something much larger in scope than the classic information security and information systems security (INFOSEC) which have long been largely associated with the protection of national security information and systems.

D.4.3 DoDI 3600.2, Secret NOFORN, Information Warfare Security Guidance (U), 6 Aug 98

UNCLASSIFIED ABSTRACT: DoDI S-3600.2 has been issued to CINCs as guidance. When issued, it will supersede ASD(C3I) Memorandum, *Information Warfare Security Guidance*, dated 11 May 93. It establishes the minimum security classification of information related to Department of Defense information warfare activities.

D.4.4 DoDD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, 12 Nov 92

Promulgates policy for compatibility, interoperability, and integration of C3I systems in DOD. Establishes a long-term objective for a DOD-wide, global C3I plug-and-play infrastructure. Requires components to develop, acquire, and deploy C3I systems and equipment that meet essential operational needs of U.S. forces, that are compatible and interoperable with existing and planned C3I systems. Establishes that all C3I systems are considered to be for joint use and that interoperability and integration of C3I requirements must be established during the requirements validation process. ASD(C3I) is responsible for prescribing procedures to implement the policy. PSAs shall make appropriate recommendations during program and budget reviews. The CJCS will develop doctrinal and operational procedures to achieve compatibility and interoperability. Components will ensure that the policy is followed during the requirements validation process.

D.4.5 DoDI 4630.8, Procedures for Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, 18 Nov 92

Establishes procedures to implement policy for compatibility, interoperability, and integration of C3I systems in DOD promulgated in DoDD 4630.5. Assigns specific requirements and reviews of Mission Needs Statements (MNS) and Operational Requirements Documents (ORD). Includes COMSEC considerations.

D.4.6 DoDD 5000.1, Defense Acquisition, 15 Mar 96

DoDD 5000.1 reflects a major update of DOD acquisition policy; establishing guiding principles for all defense acquisition, from advanced fighter aircraft to the simplest combat helmet. The directive requires acquisition programs to be managed to optimize total system performance and minimize cost of ownership. The total system includes the following which are relevant to IA: how systems security procedures and practices are implemented; how the system will be able to respond to any affects unique to that

environment, such as Information Warfare; the operational and support infrastructure (including Command, Control, Communications, Computers and Intelligence).

D.4.7 DoD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information Systems (MAIS) Acquisition Programs, 15 Mar 96

DoD Regulation 5000.2-R specifies mandatory policies and procedures for major defense acquisition programs and major automated information system acquisition programs. It requires a C4I Support Plan but does not specifically call out information assurance considerations. It does identify “ensuring that information warfare risks have been assessed” as a software engineering principle and identifies INFOSEC as design consideration. A companion document, the *Defense Acquisition Deskbook* describes the discretionary information to which Program Managers and other participants in the defense acquisition process can turn for assistance in implementing guiding principles and mandatory procedures. The *Deskbook* does address security considerations.

D.4.8 DoDD 5105.19, *Defense Information Systems Agency*, 25 Jun 91

DoDD 5105.19 is the DISA charter. It assigns the following information assurance relevant responsibilities to the Director, DISA:

- Assist OSD and Chairman of the Joint Chiefs of Staff activities by assessing technology; recommend and conduct a program of research, development, test, and evaluation necessary to ensure that C3 systems remain capable of performing their assigned functions in threatened environments.
- Exercise operational direction and management control of the DCS through the DISA Operations Control Complex and Military Departments’ operations and maintenance commands.
- Coordinate information system security (communications security and computer security) interoperability requirements with cognizant DOD Components.
- Coordinate secure tactical C3 communications interoperability requirements with the National Security Agency (NSA) the Defense Intelligence Agency, the Military Departments, and the Chairman of the Joint Chiefs of Staff.
- In coordination with NSA/CSS and the MILDEPS and in accordance with DoDD C-5200.5 develop a tactical secure communications architecture as an integral part of the overall joint architecture including orderly and timely introduction of systems to satisfy interoperability requirements.

D.4.9 DoDD 5111.1, Under Secretary of Defense for Policy, 22 Mar 95

Summary

The Under Secretary of Defense Policy is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for all matters concerning the formulation of national security and defense policy and the integration and oversight of DOD policy and plans to achieve national security objectives.

Also has delegated authority to issue DOD Instructions, DOD Publications, and one-time directive-type memoranda, consistent with DoD 5025.1-M, that implement policy approved by the Secretary of Defense in assigned areas of responsibility.

Responsibilities

- Represents the Department of Defense, as directed, in matters involving the National Security Council (NSC), Department of State, and other Departments, Agencies, and interagency groups with responsibilities for national security policy.
- Serves as a member of the NSC Deputies Committee; serve as a member of the Deputies Committee for Crisis Management; and advises the Secretary of Defense on crisis prevention and management, including contingency planning for major areas of concern.
- Develops policy on the conduct of alliances and defense relationships with foreign governments, their military establishments, and international organizations; integrates and oversees plans and programs undertaken in conjunction with those alliances and defense relationships.
- Develops, coordinates, and oversees the implementation of international security strategy and policy; political-military policy on issues of DOD interest that relate to foreign governments and their defense establishments, to include arrangements for United States military facilities, access and operating rights, and status of forces; and policy on all matters relating to prisoners of war and missing in action.
- Develops, coordinates, and oversees the implementation of policy to reduce and counter the threat to the United States, its forces, and allies of weapons of mass destruction and other militarily significant technologies and force capabilities, to include counterproliferation policy, arms control policy, and security policy.
- Provides oversight of all DOD activities related to international technology transfer; develop, coordinate, and provides policy direction and overall management for the DOD Technology Security Program and policy related to international technology transfer, to include export controls, dual-use and munitions licensing, arms cooperation programs, and support for enforcement and intelligence systems.
- Develops policy guidance, provides overall supervision, and provides oversight of planning, programming, budgeting, and execution of special operations activities, including civil affairs and psychological operations, and of low-intensity conflict activities, including counterterrorism, support to insurgency, and contingency operations.

- Provides mid- and long-range policy planning on strategic security matters and emerging national security issues; develops and oversees the implementation of a comprehensive strategy toward Russia, Ukraine, and other newly independent states of Eurasia; plan and conduct net assessments and policy research activities and programs.
- Develops policy and provides oversight for emergency planning and preparedness, crisis management, defense mobilization in emergency situations, military support to civil authorities, civil defense, and continuity of operations and government.
- Develops policy and coordinates DOD participation in, and exercises staff supervision over, special activities, special access programs, sensitive support to non-DOD agencies, and the joint worldwide reconnaissance schedule.

D.4.10 DoDD 5137.1, Assistant Secretary of Defense for C3I, 12 Feb 92

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall have as his principal duty the overall supervision of C3I affairs of the Department of Defense. The ASD(C3I) is the principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for C3I, information management (IM), counter-intelligence (CI), and security countermeasures (SCM) matters, including warning, reconnaissance, and intelligence and intelligence-related activities conducted by the Department of Defense.

Responsibilities

- Exercises direction, authority, and control over: the Defense Information Systems Agency, the Defense Intelligence Agency, the Defense Mapping Agency, the Defense Investigative Service, the Defense Support Project Office, the Intelligence Program Support Group, the Defense Polygraph Institute, the DOD Security Institute, and the Defense Personnel Security Research Center.
- Exercises staff supervision over: the National Security Agency/Central Security Service, the Air Force and Navy Special Intelligence Programs, the Electromagnetic Compatibility Analysis Center, and the Defense Courier Service.
- Executive Agent for the National Communications System.
- Serves as the Department's senior IM official pursuant to Section 3506(b) of 44 U.S.C. (reference (c)); implements the Defense IM program, the Defense corporate IM initiative, and the principles of corporate IM throughout the Department of Defense; and ensures the proper integration of DOD computing, systems security, telecommunications, and IM activities.
- Serves as the Department's senior information security official pursuant to Section 5.3(a) of E.O. 12356.
- Serves as the principal DOD official responsible for establishing software policy and practices, but shall not be responsible for computer resources, both hardware and software, that are: physically part of, dedicated to, or essential in real time to the mission performance of weapon systems; used for weapon system specialized training, simulation, diagnostic test and maintenance, or calibration; or used for research and development of weapon systems.

- Establishes and implements IM policy, processes, programs, and standards to govern the development, acquisition, and operation of automated data processing (ADP) equipment by the Department of Defense, but shall not be responsible for ADP equipment that is an integral part of a weapon or weapon system, test support for a weapon or weapon system, or information technology basic research and development.
- Chairs the Major Automated Information System Review Council (MAISRC).
- Provides program management for the General Defense Intelligence Program, the Foreign Counterintelligence Program, and the Security and Investigative Activities Program.
- Serves as the principal DOD official responsible for preparing and defending the Department's C3I, CI, SCM, and IM programs before the Congress.
- Reviews and advises the Secretary of Defense on C3I, CI, SCM, and IM plans and programs; reviews and recommends requirements and priorities to ensure that DOD requirements are fully considered in the development of these plans and programs; monitors and evaluates the responsiveness of such programs to DOD requirements, particularly their readiness to support military operations.
- Provides guidance, and management and technical oversight for all C3I, CI, SCM, and IM projects, programs, and systems being acquired by, or for the use of, the Department of Defense and its Components.
- Oversees applicable training and career development programs to ensure that trained manpower is available to support DOD C3I, CI, SCM, and IM mission needs, including manpower requirements for projected systems.
- Assesses the responsiveness of intelligence products to DOD requirements.
- Promotes coordination, cooperation, and cross-Service management of joint C3I, IM, CI, and SCM programs to ensure essential interoperability is achieved within the Department of Defense and between the Department of Defense and other Federal Agencies and the civilian community.

Areas of Responsibility

- Strategic, theater, and tactical nuclear and conventional command and control
- Information networks
- C3I-related space systems
- Special technology and systems
- Telecommunications
- Identification, navigation, and position fixing systems
- Strategic C3 countermeasures
- Air traffic control and airspace management
- Surveillance, warning, and reconnaissance architectures
- North Atlantic Treaty Organization C3I architectures and systems
- Information systems security
- Intelligence programs, systems, and equipment
- National Communications System activities
- Radio frequency policy and management
- Mapping, charting, and geodesy

- Integration and/or interface of national and tactical C3I systems and programs
- C3I, IM, CI, and SCM career development, including DOD foreign language training
- Information management activities
- Counter-narcotics C3I activities
- C3I, IM, CI, and SCM technology programs and activities
- Counterintelligence operations and investigations policy and programs
- Defense investigative activities, to include personnel security investigations, unauthorized disclosures of classified information, and polygraph examinations
- Security countermeasures activities, to include physical security, personnel security, industrial security, and security classification and safeguards policy and programs
- Operations security and counter-imagery security
- Security-related research, including personnel security and polygraph activities
- Data and information systems standardization programs, including DOD-wide data administration.

D.4.11 DoDD 5160.54, Critical Assets Assurance Program (CAAP), 20 Jan 98 (re-issued)

This re-issued directive expanded the already existing “requirement to identify Critical Assets and assure their integrity, survivability, and capability to support vital DOD missions across the full range of military operations.”¹ This policy provides for an integrated infrastructure vulnerability assessment and assurance program using risk management principles.

It recognizes the need for accepting that it is impossible to defend against every possible attack. The directive acknowledges the need for “providing ... protection from all hazards, mitigating the effect of their loss or disruption; and planning for timely restoral or recovery.”² This reflects the DOD Defense in Depth strategy, which calls for “protect, detect, react.”

An important recognition in the directive is that critical DOD equipment, facilities, and services depend on the international and national infrastructures many of which are operated, maintained, and managed by other countries, other government agencies, and the private sector. It addresses the need for DOD officials to plan for emergency preparedness and provide assistance in case of natural disaster, physical or technical attack, or other emergencies.

This policy mandates an integrated asset and infrastructure vulnerability assessment and assurance program. The directive recognizes the need to work with other government bodies and private industry to provide for national security emergency preparedness. Accordingly, key responsibilities include:

¹ DODD 5160.54, January 20, 1998, para 1.3.

² DODD 5160.54, January 20, 1998, para 4.1.

- ASD(C3I) and the Under Secretary of Defense (USD) for Policy will:
 - Establish and support the Critical Infrastructure Protection Working Group (CIPWG), mentioned above. They will co-chair this working group.
- The Secretary of the Army will:
 - Serve as the DOD Executive Agent for the CAAP. The Executive Agent is to coordinate the program with the Services, DOD agencies, and other components.
- The Director, Defense Security Service (DSS)³ will:
 - Assist by conducting on-site surveys with vulnerability analyses of physical and technical threats.
- The Intelligence Community (CIA, DIA, NSA, DSS, and FBI) will:
 - Provide continuous analysis of hostile sources and support special operations to protect these Critical Assets.
- The Director, DISA will:
 - Provide for the assurance of the Defense Information Infrastructure (DII)
 - Coordinate with the Office of the Manager of the NCS to identify critical assets in the NII
 - Coordinate the activities of all DOD Computer Emergency Response Teams (CERTs) as well as interface with other CERT-related activities (such as the NIPC, the Carnegie Mellon University CERT/CC®, and the still-to-be-defined Information Sharing and Analysis Center).

D.4.12 DoDD 5200.1, DoD Information Security Program, 7 Jun 82 (Thru Change 2, 15 Apr 94)

Establishes a DOD Information Security Program for classified national security information. It is the policy of DOD to assure that information that warrants protection against unauthorized disclosure is properly classified and safeguarded as well as to facilitate the flow of unclassified information about DOD operations to the public. Heads of DOD components will:

- Designate a senior responsible official
- Ensure adequate funding and resources for oversight and education and training
- Address complaints and suggestions.

D.4.13 DoD 5200.1-R, Information Security Program Regulation, Jun 86 (Thru Change No 1, 27 Jun 88)

The purpose of this instruction is to govern the DOD Information Security program. It establishes a system for classification, downgrading, and declassification of information, sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations.

³ Formerly the Defense Investigative Service (DIS).

D.4.14 DoDD 5200.2, DoD Personnel Security Program, 6 May 92

Establishes the DOD Personnel Security Program (DoDPSP) and assigns overall policy, guidance and control responsibilities to the ASD(C3I).

[A complete revision of DoD 5200.2-R, DoD Personnel Security Program Regulation, which provides detailed guidance and implementing instructions for the DoDPSP, is underway.]

D.4.15 DoDD C-5200.5, Confidential, Communications Security (COMSEC) (U), 21 Apr 90

UNCLASSIFIED ABSTRACT: DoDD 5200.5 issues policy and assigns responsibilities for ensuring the security and protection of telecommunications systems that transmit classified and sensitive information. Sensitive information is defined as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of the Federal programs, or the privacy to which individuals are entitled under the Privacy Act but which has not been specifically authorized under the criteria established by executive order or act of Congress to be kept secret in the interest of nation defense or foreign policy. Key responsibilities include:

- ASD(C3I):
 - Responsible for overall coordination of COMSEC matters within DOD.
- USD(P):
 - Serves as the principal security policy advisor to the ASD(C3I)
 - Serve as the focal point for COMSEC concerns surfaced by the Defense Investigated Service.
- Chairman, Joint Chiefs of Staff:
 - Validate all joint military cryptography and COMSEC requirements
 - Validate joint operational requirements for secure communications between CINCs and other nations
 - Ensure the CINCs fully employ all appropriate COMSEC measures
 - Ensure joint programs include consideration of COMSEC techniques.
- Director, NSA:
 - Develop plans, policies, and procedures to ensure that technology and products are available to allow DOD Components to satisfy their COMSEC requirements.
 - Conduct and coordinate COMSEC assessment programs within the DOD. Disseminate assessment findings to DOD Components to include contractors, recommending appropriate countermeasures.

D.4.16 DoDD C-5200.19, Confidential, Control of Compromising Emanations (U), 16 May 95

UNCLASSIFIED ABSTRACT: Policies and responsibilities for the DOD-wide program to control compromising emanations (DOD TEMPEST Security Program). All DOD Components and their contractors shall apply TEMPEST countermeasures in proportion to

the threat of exploitation and the associated potential damage to the national security. Key responsibilities include:

- ASD(C3I) shall serve as the principal staff assistant to the Secretary of Defense for the DOD TEMPEST Security Program, its resources, and policy; ensure that the DOD TEMPEST policies are consistent with current national policy and the assessed threat; promulgate additional DOD TEMPEST guidelines to the DOD Components as necessary; monitor contractors for compliance.
- USD (P) (through Deputy USD (P)(PS)) shall serve as the principal international security programs policy advisor to the ASD(C3I); Review TEMPEST policies and plans that pertain to NATO.
- Director NSA shall apply TEMPEST suppression techniques and protective measures to cryptologic equipment and certify the TEMPEST acceptability of cryptologic equipment; operate National TEMPEST Information Center; encourage industry to develop equipment and systems that meet TEMPEST standards; fund, establish and manage a training program required for both the technical education of TEMPEST personnel and the specified training of CTTAs; publish annual assessment of the domestic and foreign TEMPEST threat; provide guidance to departments and agencies on the security classification and control of information pertaining to compromising emanations.
- Heads of the DOD Components shall plan, program, fund, implement and manage a single compromising emanations control program for national security systems to implement this directive and national policy from NSTISSC; evaluate to determine the need for TEMPEST countermeasures; submit promptly to the national manager and information related to the TEMPEST threat; appoint TEMPEST Decision Authorities.

D.4.17 DoDD 5200.28, Security Requirements for Automated Information Systems, 21 Mar 88

DoDD 5200.28 establishes mandatory, minimum AIS security requirements for AISs processing classified information (supplementing DoD 5200.1-R), sensitive unclassified information, and unclassified information and applies to all AISs including stand-alone, communications systems, and computer networks. Key responsibilities include:

- ASD(C3I):
 - Oversee implementation of directive
 - Develop overall AIS security policies and procedures in coordination with USD(P)
 - Promulgate instructions, standards, manuals and other issuance's.
- DUSD(P):
 - Continue to review, oversee, and formulate overall policies governing DOD security practices for information security, physical security, personnel security, and industrial security.
- Director, DSS:
 - Implement an AIS security program for DOD contractor AIS.
- Director, DISA:
 - Implement a program for the security of long-haul communications systems.

- Director, DIA:
 - Implement a program for the security of contractor AISs that handle SCI except NSA/CSS.
- NSA/Central Security Service:
 - Implement an AIS security program for NSA/CSS and contractor AIS
 - As requested, provide communications and computer security assistance and advice to DOD components
 - Establish and maintain technical standards and criteria for evaluating and certifying trusted computer products
 - Review DoD 5200.28-STD yearly and recommend changes to ASD(C3I)
 - Train and certify DOD components in evaluation techniques and procedures
 - Evaluate computer products intended for use by DOD components or contractors as trusted computer products
 - Annually assess the overall AISs security posture and disseminate information on hostile threats
 - Operate a central technical center to provide technical assistance to evaluate and certify computer-based security features of AISs use in operational environments
 - Prescribe minimum security standards for safeguarding AISs classified and sensitive technical security material, techniques and procedures
 - Review and approve standards, techniques, systems, and equipment's for telecommunications and automated information systems security.
- The Joint Chiefs of Staff:
 - Implement an AIS security program for AISs that handle SIOP-ESI
 - Provide a source of education and training for managers in AIS security through the DOD Computer Institute of the national Defense University.
- Heads of DOD Components:
 - Implement overall AIS security programs
 - Ensure adequate funding and resources are programmed for staffing, training and supporting the AIS security program and for implementing AIS safeguards
 - Assign senior AIS policy officials as DAA
 - Establish and maintain an AIS security training and awareness program
 - Ensure periodic independent reviews of the security and protection of AISs
 - Support the Computer Security Technical Vulnerability Reporting Program.
- DAA's:
 - Review and approve security safeguards of AISs and issue accreditation statements
 - Ensure that all safeguards required, as stated in the accreditation documentation are implemented and maintained
 - Identify security deficiencies and, where deficiencies are serious enough to preclude accreditation, take action (e.g. allocate additional resources) to achieve an acceptable security level
 - Ensure a trained ISSO is named for each AIS
 - Require an AIS security education and training program
 - Ensure data ownership is established for each AIS.

- ISSOs:
 - Ensure the AIS is operated, used, maintained, in accordance with security policies and practices
 - Have the authority to enforce security policies and safeguards on all personnel having access to the AIS
 - Ensure users have the required personnel security clearances, authorization, and need-to-know, have been indoctrinated and are familiar with internal security practices
 - Ensure audit trails are reviewed periodically
 - Begin protective or corrective measures if a security problem exists
 - Report security incidents
 - Report the security status of the AIS as required to the DAA
 - Evaluate known vulnerabilities to ascertain if additional safeguards are needed
 - Maintain a plan for system security improvements and progress toward meeting accreditation.

*A new edition of the DoDD 5200.28, is currently in coordination at the C/S/A level with publication still pending. The final version may be published under the “5200.28” label or as a new proposed series “8500” which will cover Information Assurance. This directive will ultimately determine the scope and direction for other instructions and manuals that serve as implementing publications.

D.4.18 DoD 5200.28-M, ADP Security Manual; Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating - Secure Resource-Sharing ADP Systems, Jan 73 (Thru Change 1, June 25, 1979)

The techniques, methodologies, and procedures in the ADP Security Manual represent an approved method of securing a remotely accessed resource-sharing computer system in a multilevel security mode. The objective of the manual is to provide guidelines and establish techniques and procedures, which can be used to:

- Implement secure resource-sharing ADP systems so that with reasonable dependability, deliberate or inadvertent access to classified material by unauthorized personnel or the unauthorized manipulation of the computer and its associated peripheral devices, which could lead to the compromise of classified information, can be prevented.
- Develop, acquire, and establish methodologies, techniques, standards, and procedures for the design, analysis, testing, evaluation, and approval of the security features for resource-sharing ADP systems.
- Establish methodologies, techniques, and procedures for the physical protection of ADP Systems and components.
- Prescribe standards, criteria, and specifications for deactivating secure ADP Systems and the sanitization of system components for disposition or utilization in unsecured environments.

**D.4.19 DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria,
26 Dec 85**

The purpose of the Orange Book is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities of the DOD Components. It is mandatory for use by all DOD Components in carrying out ADP technical security evaluation activities applicable to the processing and storage of classified and other sensitive DOD information and applications.

D.4.20 DODD 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97

The DITSCAP was developed to establish a standardized process, set of activities, general task descriptions, and management structure to verify, validate, implement, and maintain the security posture of the DII throughout the system life cycle. This process aligns itself with the program strategy and integrates its activities into the system life cycle to ensure that a new or modified IT system meets accreditation requirements and continues to maintain accredited security posture.

A standard process is a series of activities consistently performed to bring about accreditation. The sets of activities, which define the process, are specified forms of supervised actions called process activities. Process activities provide an effective method for determining and maintaining the security posture of an IT.

The DITSCAP focuses on protecting the DII by presenting an infrastructure-centric approach for certification and accreditation. The DITSCAP protects IT systems commensurate with their value to DOD. An acceptable level of residual risk is based on the relationship of the threat to the system and the information processed; to the information system's mission, environment, and architecture; and its security confidentiality, integrity, availability, authenticity and non-repudiation objectives. The DITSCAP fundamentally verifies and validates the IT system's functions, attributes, and mechanisms to meet these objectives. It is oriented to establish, verify, and validate a degree of confidence to meet the objectives, i.e., system-wide assurances.

Key responsibilities include:

- ASD(C3I):
 - Oversee and review implementation of this Instruction
 - Review, oversee, and formulate overall policies that govern DOD security practices and programs to implement the DITSCAP as the standard DOD process for conducting IT Certification and Accreditation (C&A)
 - Promulgate standards, establish support and training, and manage the transition to the DITSCAP

- Conduct an annual assessment and/or review of the DITSCAP and consider proposed changes
- Ensure that each designated approving authority (DAA) implements and maintains the DITSCAP for security C&A of DOD Component and DOD contractor IT and networks under their jurisdiction.
- OSD Principal Staff Assistants and the Chairman of the Joint Chiefs of Staff, in respective areas of responsibility, shall ensure DOD Component compliance with the DITSCAP.
- Director, DISA:
 - Maintain DITSCAP procedural information in support of security C&A of DOD Component and DOD contractor IT systems and networks
 - In coordination with the National Security Agency (NSA), implement, operate, and maintain an on-line information assurance support environment (IASE)
 - In coordination with NSA, provide assistance such as information system security engineering, security solutions, and security guidance to the DOD Components in the use of DITSCAP through the IASE
 - Provide DITSCAP training for the DOD Components
 - Support the annual review of the DITSCAP.
- Heads of the DOD Components:
 - Implement the DITSCAP for security C&A of DOD Component and DOD contractor IT systems and networks in accordance with DoD Directive 5200.28, P. L. 100-235 (1987), OMB Circular A-130, DCID 1/16, DoD Directive 5220.22, the NISPOM, and Chairman of the Joint Chiefs of Staff S3231.01.
 - Provide assistance, and support to their respective Service or Agency constituents, in the implementation of the DITSCAP.
 - Assign responsibility to implement the standard C&A process to DAA responsible for accrediting each IT and network under their jurisdiction.
 - Support the annual review of the DITSCAP.

D.4.21 DoDD 5205.2, DOD Operations Security Program, 7 Jul 83

Establishes a DOD OPSEC Program and requires components to establish programs. Applies to both classified and unclassified information. The DUSD(P) is responsible for policy and oversight. The Joint Staff is tasked to establish OPSEC requirements for CINCs.

D.4.22 DoDD 5215.1, Computer Security Evaluation Center, 25 Oct 82

Establishes the DOD Computer Security Evaluation Center (CSEC) in NSA to encourage the easy availability of trusted computer systems. The USDR&E, in coordination with the DUSD(P) and the ASD(Comptroller), is responsible for policy and oversight.

D.4.23 DoDI 5215.2, Computer Security Technical Vulnerability Reporting Program, 2 Sep 86

Establishes a Computer Security Technical Vulnerability Reporting Program (CSTVRP) under the direction of NSA and procedures for DOD Component reporting, collection and analysis of all demonstrable and repeatable technical vulnerabilities of AISs. The ASD(C3I) is responsible for staff supervision and oversight.

[A revision, which includes incident and vulnerability reporting, is in draft.]

D.4.24 DoDD 5220.22, DOD Industrial Security Program, 8 Dec 91

Assigns overall responsibility for the Defense Industrial Security Program (DISP) and ensures that classified information released to industry is properly safeguarded. The DUSD (Policy Review) is responsible for policy and oversight. DSS administers the DISP.

D.4.25 DoDD 5240.11, Damage Assessments, 23 Dec 91

Establishes policy for reporting, review and analysis of comprehensive damage assessments of both the compromise of U.S. classified intelligence (sources and methods) and non-Intelligence U.S. classified defense information resulting from unauthorized disclosure and establishes the DOD Damage Assessment Committee. The DASD(CI) will chair the DODDAC, provide oversight and formulate policy. The USD(A), USD(P), General Counsel, Joint Staff, MILDEPS, DIRNSA, and DIA will appoint a representative to sit on the DODDAC. DOD Components will establish damage assessment procedures and reporting procedures in accordance with this directive.

D.4.26 DoDD 7740.1, DoD Information Resources Management Program, 20 Jun 83

Implements the Paperwork Reduction Act of 1980, by establishing the DOD Information Resources Management Program to promote coordinated and integrated information management functions. Procedures are designed to, among others, support DOD operations and decision-making with information that sufficiently meets the need in terms of availability, accuracy, timeliness, and general quality. The ASD(Comptroller) is responsible for coordination, policy and oversight.

D.4.27 DoDD 8000.1, Defense Information Management (IM) Program, 27 Oct 92

Establishes policy for implementation of the Defense Information Management (IM) Program, which governs the continuing evolution, and improvements of IM. IM includes the functional process improvement program, information resources management, and supporting information technology and services throughout the DOD. Specific policy includes, among others, that security, integrity, and survivability of information are basic to the DOD mission and shall be an integral part of all functional processes. Where possible and cost-effective, a centrally managed infrastructure for computing, communications, information security, and systems security shall be used. Security of information,

commensurate with the risk and magnitude of harm resulting from loss, misuse, or unauthorized access to or modification of the information, shall be an integral part of all IS designs. The user shall apply risk analysis to validate IS designs. The ASD(C3I) is the Principal Staff Assistant for the DOD IM Program.

D.4.28 Office of the Secretary of Defense, National Industrial Security Program (NISP) Operating Manual (NISPOM), undated (January 1995 Baseline)

Assigns overall responsibility for the Defense Industrial Security Program (DISP) and ensures that classified information released to industry is properly safeguarded. The DUSD(Policy Review) is responsible for policy and oversight. DSS administers the DISP. The Manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The Manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including Restricted Data, Formerly Restricted Data, intelligence sources and methods information, Sensitive Compartmented Information, and Special Access Program information. The Secretary of Defense is the Executive Agent for NISP. The Director, Information Security Oversight Office (ISOO) is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

[The NISPOM replaces DoD 5220.22-M and DoD 5220.22-M-Sup, the DOD Industrial Security Manual for Safeguarding Classified Information, dated January 1991]

D.4.29 Defense Science Board (DSB), Report of the Defense Science Board Task Force on Information Warfare - Defense, November 1996

The Defense Science Board Task Force on Information Warfare (Defense) was directed to “focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence.” This meant an assessment of the state of DOD readiness of what is called today the Defensive Information Operations component of Information Assurance. Specifically, the Task Force was asked to:

- Identify the information users of national interest who can be attacked through the shared elements of the national information infrastructure.
- Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities.
- Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the national information infrastructure and the information users of national interest.
- Identify the indications and warning, tactical warning and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize

attacks on the national information infrastructure and/or attacks on the information users of national interest.

- Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability.
- Provide specific guidelines for implementation of the Task Force's recommendations.

The Task Force observed that:

- The Intelligence community must step up to the IW challenge: by asking relevant questions; by recognizing that traditional methods are not effective, that key commercial technologies have lethal possibilities, that they are ubiquitous and relatively simple "business" processes are complex, HUMINT is still extremely important, and required skill sets are much broader and deeper in educational level.
- DOD lacks a common vocabulary: The Task Force could not find or derive a useful IW taxonomy; The Task Force proposed a standard vocabulary for IW-D readiness assessment and reporting and for threat warning.
- Resources are focused on classified content and systems.
- It is easy to make the IW-D problem too hard by focusing too broadly or on solving political or social problems before addressing IW-D.
- Acquisition policy and practices pose dilemmas as current practices trade off security, but the Policy is clear.
- Cascading effects have occurred, are difficult to predict - infrastructure robustness untested and recovery is uncertain.
- Area and perimeter defenses are not sufficient: resiliency and repairability are critical; and information domains are essential.
- Easy technical solutions are not apparent.
- Encryption is useful, but it's not a panacea, as it doesn't protect against denial of service attacks. Access control and identification and authentication are many times more effective than encryption in "raising the bar." There is a great need for promoting information security in the private sector.
- Local processes procedures and mechanisms must not be under or depend on centralized control.
- However, much more can be done:
 - Awareness, training and education and clarity of organizational responsibility and accountability are seen as yielding the largest short-term improvements.
 - DOD is not applying the knowledge it already has.
- And, DOD must start now!

The Task Force made 13 key recommendations, which it considered to be imperatives – and which they had made pointing out for three years previously.

1. Designate an accountable IW focal point.
2. Organize for IW-D.
3. Increase awareness.
4. Assess infrastructure dependencies and vulnerabilities.

5. Define threat conditions and responses.
6. Assess IW-D readiness.
7. "Raise the bar" (with high-payoff, low-cost items).
8. Establish a minimum essential information infrastructure.
9. Focus the R&D.
10. Staff for success.
11. Identify and resolve the legal issues.
12. Participate fully in critical infrastructure protection.
13. Provide the resources.



Joint Staff

D.5 JOINT STAFF

D.5.1 CJCSI 3210.01A, Secret, Joint Information Operations Policy (U), 5 Nov 98

UNCLASSIFIED ABSTRACT: CJCSI 3210.01A provides guidance and assigns responsibilities for information operations. Key responsibilities include:

- J-2:
 - Ensure combatant commands and Joint Staff receive intelligence support to assist planning and execution of IO
 - Coordinate development of joint doctrine, strategy and policy for IO intelligence support
 - Coordinate the development of effective indications and warning methods to identify potential IO Threats.
- J-3:
 - Provide the focal point for IO at the Joint Staff to include, policy and strategy development, validation of requirements and programs, IO JWCA, budget reviews and assessments, technology development, and security
 - Ensure activities and capabilities are fully integrated into IO deliberate and crisis planning
 - Coordinate with Services, combatant commands, Defense agencies and Joint Staff to develop IO doctrine.
- J-5:
 - Ensure employed activities and capabilities to conduct IO are fully integrated into deliberate and crisis plans and planning processes, and joint exercises consistent with DOD policy
 - Coordinate IO policy and strategy development.
- J-6:
 - Coordinate IA policy and strategy development, validation of defensive capability requirements and programs for IA, budget reviews and assessments, and technology development
 - Ensure IA is integrated into deliberate and crisis plans and planning processes.
- J-7:
 - Refine IO doctrine through joint training events and exercises including conditions that stress our forces and their information systems and capabilities in realistic scenarios
 - Ensure IO is incorporated into joint professional military education curriculums and to Universal Joint Task List (UJTL)
 - Update the Joint Operations Planning and Execution System (JOPES) to reflect deliberate IO planning.
- Joint Task Force - Computer Network Defense (JTF-CND):
 - Coordinate and direct appropriate DOD actions to stop attack, contain damage, restore functionality, and provide feedback to user community
 - Develop contingency plans, tactics, techniques, and procedures to defend DOD computer networks

- Monitor Computer Emergency Response Team (CERT) Alerts, Warnings and Advisories, and provide input to and monitor Indications and Warning (I&W) reporting.
- National Security Agency (NSA):
 - Provide INFOSEC technology, products, and services to help protect against hostile CAN efforts
 - Conduct vulnerability and threat analysis to support information protection and the defense and protection of US and friendly information system.
- Defense Intelligence Agency (DIA):
 - Manage Defense Intelligence Community production to support the full range of DOD IO
 - Oversee DOD intelligence requirements in support of IO
 - Provide indications and warning of foreign IO (including CNA), with the assistance of DISA and other government and non-government agencies.
- Joint Command and Control Warfare Center (JC2WC):
 - Provide augmentation support to CINC staffs
 - In concert with the Services, assist in the integration of IO opposition force activities (Red Teaming) conducted in the joint exercise arena.
- Joint Warfighting Center (JWFC):
 - Coordinate and assist the Joint Staff, Services, and combatant commanders in developing joint IO doctrine
 - Ensure modeling and simulation efforts are coordinated to eliminate duplication of effort and help focus on the development of systems that fulfill combatant command and Service IO training and exercise requirements.
- Joint COMSEC Monitoring Activity (JCMA):
 - Provide COMSEC monitoring and analysis support.
- Joint Spectrum Center (JSC):
 - Provide locational and technical characteristics about friendly force C2 systems
 - Provide assistance in development of the joint restricted frequency (JFRL) for deconfliction purposes

Provide unclassified C4 area studies about regional C4 infrastructure.

D.5.2 CJCSI 6510.01B, Defensive Information Operations, 30 Jun 97 (Through Change 1, 26 Aug 98)

CJCSI 6510.01B provides implementing guidance and supplemental joint policy for defensive information operations. CJCS specific policy guidance requires that information, information-based processes and information systems (such as command, control, communications, and computer (C4) systems, weapon systems, and infrastructure systems, etc.) used by US military forces will be protected relative to:

- The value of the information contained therein
- The risks associated with the compromise of or loss of access to the information.

The most significant addition in Change 1 was the result of several lessons learned from Solar Sunrise – the need for an effective and efficient incident and vulnerability reporting system. The new reporting structure has four levels: Global, Regional, Service and Local. All Services’ local control centers (whether in operational locations – OPLOCs, Intelligence, C4 or Law Enforcement facilities at bases, camps, posts, and stations will report upward through either or both of the two functional/command chains (see Exhibit D-3):

- DISA Regional Operations and Security Centers (ROSCs), many of which are collocated with warfighting CINCs.
- Service/Regional CERTs or CIRTs, some of which are collocated with Service staffs.

Both of these levels will report upward to the DISA Global Operations and Security Center (GOSC). These reports are consistent with the traditional network management process for reporting network outages. This reporting process augments other operational reporting through the chain of command, such as OPREPs.

At the global level the GOSC will notify and coordinate with the Joint Staff, the NSA National Security Operations Center (NSOC) Information Protection Cell (IPC), and the (FBI) National Infrastructure Protection Center (NIPC, mentioned earlier). The GOSC will assure analysis and correlation of event and incident data as well as assist coordination at all levels. Detection, analysis, and correlation can originate in manual or automated tools, such as the JIDS.

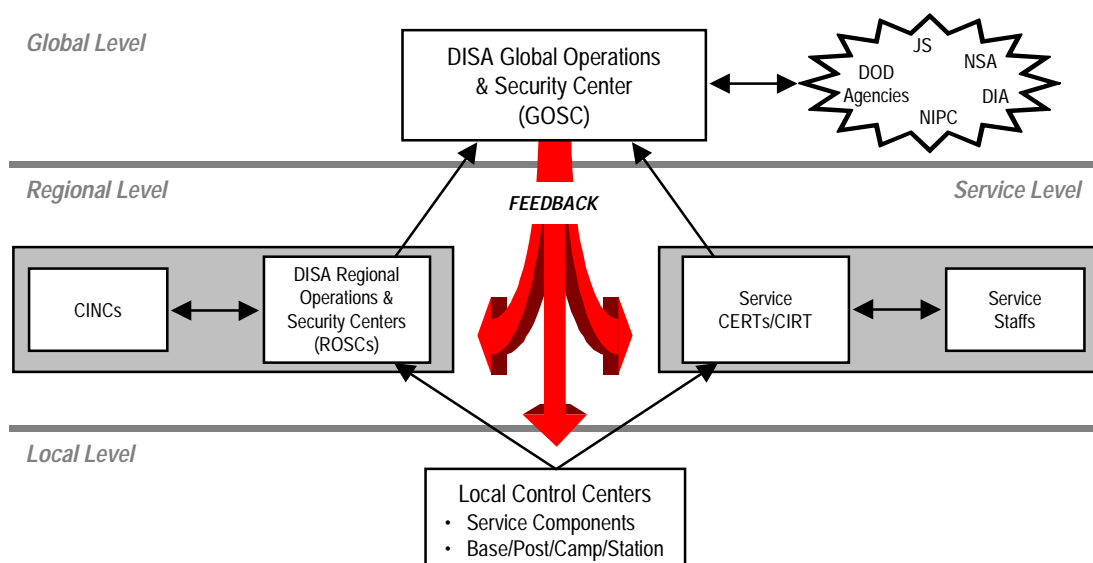


Exhibit D-3. Incident Reporting Structure

The military coordination chain will ensure notification of all military organizations which need the pertinent information. The Joint Staff will provide briefings to National Command Authorities through the Chairman’s role as military advisor. The NIPC will provide mutual threat assessments, warnings and indications, vulnerability advisories, and law enforcement investigations and response liaison to the FBI.

While the upward transmission of vulnerability and incident information is traditional to military operations, the reverse flow is equally important. Through the Information Assurance Vulnerability Alert (IAVA) process, the DISA GOSC, specifically the Automated System Security Incident Support Team (ASSIST) will implement a comprehensive distribution for alerts and countermeasures. The publication of a secure Website for this information will require acknowledgement of receipt within a nominal 5-day period. Then every local control center will assess the impact of their alert, and report compliance through normal command chain within a nominal 30-day period.

D.5.3 Joint Pub 3-13, Joint Doctrine for Information Operations, 9 Oct 98

The Joint Staff published Joint Pub 3-13, *Joint Doctrine for Information Operations*, to codify for the Warfighter how IO will serve as an integral part of all military operations. Its relationship to other operations is clarified in its links to the Crisis Action Planning Process, the Joint Operations Planning and Execution System, and Annexes C and K of the Joint OPOD/ CONPLAN/OPLAN of any Joint Force. There are several concepts, which while perhaps not totally new, constitute a maturing trend in operational doctrine.

First, JP 3-13 formalizes the close ties between information and the management of violence through physical assets. Throughout the publication, there is a strong and constant emphasis on the relationship of IO to military missions and objectives – the Warfighter. In Chapter II, General Gordon Sullivan, former Army Chief of Staff, recognized the role of information in crisis and war before the Joint Vision 2010 made it a formal doctrine. He noted that in the 21st century, “Information is the currency of victory on the Battlefield.”

Second, it addresses more directly the issues of offensive IO as an adjunct of defensive IO. Early drafts of 3-13 did prepare the way for introduction of this idea by addressing the notions of Information Warfare (IW) although most of the prior discussions were as an extension of C2W, EW, and jamming (mostly communications oriented). With so much of crisis and warfare decision-making depending on information systems and networks, the time was right to advance the concept of computer network attacks (CNA) as a legitimate means of warfare. Although US military forces temper the means of warfare with considerations of the laws of armed conflict, domestic and international law, national treaties, and rules of engagement, various real and potential adversaries of the US have made clear their intention to use all means, including CNA.

Third, there is a full chapter detailing the IO organization, a typical Joint Information Operations (Response) Cell. In many ways it parallels the classic notion of a Crisis Action Team or a Battle Staff. The Cell is normally headed up by an IO officer from J-3 with supporting representatives of: the J-2, J-4, J-5, J-6, J-7 functions; the Public Affairs Office, the Staff judge Advocate (for legal questions); Civil Affairs; Electronic Warfare, Joint PSYOPS Task Forces, Joint Special Operation Task Forces, Special Technical Operations, and other traditional C2W players.



Other

D.6 OTHER

D.6.1 DCID 1/16, Secret, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U), Jul 88

DCI Directive 1/16 establishes long-term goals and near-term requirements intended to improve the security of U.S. intelligence processed in automated information systems and networks with respect to its possible compromise because of:

- Penetration by hostile intelligence services
- Penetration by otherwise legitimate users who gain access to data or processes for which they are not authorized
- Inadequate security design, implementation, or operation.

The directive also assigns policy execution roles and responsibilities, and establishes a procedural framework within which they are to be implemented.

D.6.2 DCID 1/16, FOUO, Security Policy on Intelligence and DOD SAP Information in Information Systems: Policy, Draft Five, November 1997

This unclassified draft version compiles into one volume a wealth of information for securing Intelligence and DOD Special Access Program (SAP) information in information systems. It is a much-needed modernization of the older directive. This directive is applicable to all government organizations, their commercial contractors, and Allied governments, which process, store, or communicate U.S. Intelligence and DOD SAP information. Of great benefit is its unclassified form which makes it much easier for more people to use its guidance for a foundation of any unclassified (but sensitive) information security program. It defines roles and responsibilities for the Principal Accrediting Authority (PAA), the Data Owner, the Data Custodian, the Designated Approving Authority (DAA), the Designated Approving Authority Representative (DAAR), the Information System Security Manager (ISSM), the Information System Security Officer (ISSO), privileged users, and general users. The directive has chapters on:

- Requirements and implementation methods for risk management
- Security of interconnected systems with special treatment of
 - Interface management
 - Web security (especially mobile code – Java, Javascript and ActiveX.)
 - E-mail
 - Collaborative computing
 - Period processing
 - Embedded , data acquisition, and special purpose systems
 - Tactical or deployable systems
 - Group authenticators

- Special/Administrative security requirements
 - Administrative security
 - Environmental security
 - Physical security
 - Personnel security
 - Foreign national access
- Certification and accreditation procedures.

It also has several sections defining security features and assurances to provide confidentiality, integrity, and availability. It is generally much broader, although in a few places a little briefer, than most DOD security publications.

Appendix E **Acronyms**

APPENDIX E
LIST OF ACRONYMS

This page intentionally left blank.

ADP	Automated Data Processing
AECA	Arms Export Control Act
AES	Advanced Encryption Standard
AFC4A	Air Force C4 Agency
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigation
AFPD	Air Force Policy Directive
AIMS	Automated Infrastructure Management System
AIS	Automated Information Systems
ALECs	Alternate Local Exchange Carriers
AMIDS	Audit Monitoring and Intrusion Detection System
ANSI	American National Standards Institute
AO	Area of Operations
AOL	America On Line
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
APII	Asia Pacific Information Infrastructure
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASEAN	Association of Southeast Asian Nations
ASIMS	Automated Security Incident Measuring System
ASSIST	Automated System Security Incident Support Team
ATD	Advanced Technology Demonstration
ATM	Asynchronous Transfer Mode
B,C,P,Ss	Bases, Camps, Ports and Stations
BETSI	Bellcore's Trusted Software Integrity System
BIS	Bank for International Settlements
BM/C2	Battle Management/Command and Control
BXA	Bureau of Export Administration
C&A	Certification and Accreditation
C&A WG	Certification and Accreditation Working Group
C/S/A	CINCs/Services/Agencies
C2	Command and Control

C2W	Command and Control Warfare
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CA	Certification Authority
CAAP	Critical Asset Assurance Program
CAC	Commander of the Combined Arms Command
CAP	Connection Approval Program
CCL	Commerce Control List
CEC	Cooperative Engagement Capability
CERT®	Computer Emergency Response Team
CERT®/CC	CERT/Coordination Center
CFJO	Concept for Future Joint Operations
CFR	Code of Federal Regulations
CI	Counterintelligence
CIA	Central Intelligence Agency
CIAC	Computer Incident Advisory Capability
CIAO	Critical Infrastructures Assurance Office
CIM	Corporate Information Management
CINC	Commander In Chief
CINCLANTFLT	Commander in Chief, U.S. Atlantic Fleet
CINCPACFLT	Commander in Chief, U.S. Pacific Fleet
CINCUSNAVEUR	Commander in Chief, U.S. Naval Force Europe
CIO	Central Imagery Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
CIRT	Computer Incident Response Team
CISA	C4I Integration Support Activity
CITAC	Computer Investigation and Infrastructure Threat Assessment Center
CITEL	Inter-American Telecommunications Commission
CIWE	Center for Information Warfare Excellence
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joints Chiefs of Staff Instruction
CLECs	Competitive Local Exchange Carriers

CMDS	Computer Misuse Detection System
CMS	Community Management Staff
CMUSNAVCENT	Commander, U.S. Naval Forces Central Command
CNA	Computer Network Attack
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COP	Common Operational Picture
COTS	Commercial Off-the-Shelf
CSA	Computer Security Act
CSA	Chief of Staff U.S. Army
CSAAS	Combat Support Agency Assessment System
CSIR	Computer (and Network) Security Incident Response
CSPAR	CINCs Preparedness Assessment Report
CSSOs	Computer Systems Security Officers
DAA	Designated Approving Authority
DARO	Defense Airborne Reconnaissance Office
DARPA	Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary of Defense
DBS	Direct Broadcast Satellite
DCI	Director of Central Intelligence
DDPO	Defense Dissemination Program Office
DDR&E	Director, Defense Research and Engineering
DEFCON	Defense Condition
DES	Digital Encryption Standard
DFAS	Defense Finance and Accounting Service
DG	Directorate General
DG	Defense Guidance
DIA	Defense Intelligence Agency
DIACCS	Defense IA Command and Control System
DIAMOND	Defense Intrusion Analysis & Monitoring Desk
DIAP	Defense Information Assurance Program
DIDS	Distributed Intrusions Detection System
DII	Defense Information Infrastructure

DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISCO	Domestic-International Satellite Consideration Order
DISN	Defense Information Systems Network
DITSCAP	DoD IT Security Certification and Accreditation Process
DITSWG	Defense Information Technology Security Working Group
DMA	Defense Mapping Agency
DMC	Defense MegaCenter
DMS	Defense Messaging System
DNS	Domain Name Servers
DoC	Department of Commerce
DoD	Department of Defense
DoDD	Department of Defense Directive
DoE	Department of Energy
DoN	Department of the Navy
DoS	Department of State
DOT	Department of Transportation
DPG	Defense Program Guidance
DSB	Defense Science Board
DSCS	Defense Satellite Communications Systems
DTAP	Defense Technology Area Plan
DTH	Direct-to-Home
EAA	Export Administration Act
EAR	Export Administration Regulation
EAS	Emergency Alert System
EBS	Emergency Broadcast System
EC	Electronic Combat
EC/EDI	Electronic Commerce/Electronic Data Interchange
ECOSOC	Economic and Social Council
ECPA	Electronic Communications Privacy Act
EDI	Electronic Data Interchange
EFF	Electronic Freedom Frontier
EFOIA	Electronic Freedom of Information Act
EOP	Executive Office of the President
EP	Electronic Protection

EPA	Environmental Protection Agency
ETA	Education, Training and Awareness
ETAPWG	Education, Training, Awareness and Professionalization Working Group
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEDCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FIPS PUB	Federal Information Processing Standard Publication
FIRST	Forum of Incident Response and Security Teams
FIWC	Fleet Information Warfare Center
FM	Field Manual
FOIA	Freedom of Information Act
FS	Federal Standard (also FED-STD)
FSO	Field Security Office
FTC	Federal Trade Commission
FTS	Federal Telecommunications Service
G7	Group of Seven Nations
GAO	General Accounting Office
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GENIE	Global Networked Information Exchange
GETS	Government Emergency Telecommunications Service
GIE	Global Information Environment
GII	Global Information Infrastructure
GITS	Government Information Technology Services
GMITS	Guidelines for the Management of IT Security
GOSC	Global Operations and Security Center
GOTS	Government Off-the-Shelf
GPRA	Government Performance and Results Act

GSA	General Services Administration
GSII	Government Services Information Infrastructure
HQMC	Headquarters, Marine Corps
HTML	Hypertext Markup Language
HUMINT	Human intelligence
I&W	Indications and Warning
IA	Information Assurance
IAD	Information Assurance Document
IADB	Inter-American Development Bank
IAG	Information Assurance Group
IAPWG	Information Assurance Policy Working Group
IATAC	Information Assurance Technology Analysis Center
IAVA	Information Assurance Vulnerability Alert
IBRD	International Bank for Reconstruction and Development
IC	Intelligence Community
IC/EXCOM	Intelligence Community Executive Committee
ICSID	International Centre for Settlement of Investment Disputes
IDA	International Development Association
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
IEEPA	International Economic Emergency Powers Act
IETF	Internet Engineering Task Force
IFC	International Finance Corporation
ILECS	Incumbent Local Exchange Carriers
IMS	Integrated Management System
INFOCONs	Information Operations Conditions
INFOSEC	Information Systems Security
INFOSYS	Information Systems
INMARSAT	International Maritime Satellite Organization
INMS	Integrated Network Management System
INTELSAT	International Telecommunications Satellite Organization
IO	Information Operations
IOC	Initial Operating Capability
IOTC	Information Operations Technical Center

IP	Internet Protocol
IPMO	INFOSEC Program Management Office
IPR	Internet Protocol Router
IPSec	Internet Protocol Security
IPT	Integrated Product Team
IPTF	Infrastructure Protection Task Force
IPTF-PoA	Information Protection Task Force Plan of Action
IRC	INFOSEC Research Council
IRM	Information Resource Management
IRS	Incident Reporting Structure
IRT	Incident Response Team
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITMRA	Information Technology Management Reform Act
ITR	Information Technology Resources
ITU	International Telecommunication Union
IW	Information Warfare
IW-D	Information Warfare - Defensive
IXCs	Interexchange Carriers
JCCC	Joint Communications Control Center
JDIICS	Joint DII Control Systems
JIC	Joint Intelligence Center
JID	Joint Intrusion Detection
JIEO	Joint Interoperability Engineering Organization
JIT	Just-in-Time
JIWG	Joint IA Operations Working Group
JPO STC	Joint Program Office for Special Technical Countermeasures
JTA	Joint Technical Architecture
JTF	Joint Task Force
JTF-CND	Joint Task Force-Computer Network Defense
JTTP	Joint Tactics, Techniques, and Procedures
JV-2010	Joint Vision 2010

JWID	Joint Warrior Interoperability Demonstration
JWSTP	Joint Warfighting Science and Technology Plan
KMI	Key Management Infrastructure
L2F	Layer Two Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
LCC	Local Control Center
LDCs	Least Developed Countries
LEA	Law Enforcement Agency
LEC	Local Exchange Carrier
LOAC	Law of Armed Conflict
MAISRC	Major Automated Information System Review Council
MAN	Metropolitan Area Network
MARIS	Maritime Information Systems Project
MCDES	Malicious Code Detection and Eradication System
MCEB	Military Communications Electronic Board
MHz	Megahertz
MIE	Military Information Environment
MIGA	Multilateral Investment Guarantee Agency
MIT	Massachusetts Institute of Technology
MLS WG	Multilevel Security Working Group
NACC	North Atlantic Cooperation Council
NACIC	National Counterintelligence Center
NAFTA	North American Free Trade Agreement
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NAVCIRT	Naval Computer Incident Response Team
NCA	National Command Authority
NCIS	Naval Criminal Investigative Service
NCS	National Communications System
NCSA	National Center for Supercomputing Applications
NCSA	National Computer Security Association

NCSC	National Computer Security Center
NDU	National Defense University
NIAC	National Infrastructure Assurance Council
NIC	National Intelligence Council
NID	Network Intrusion Detector
NIE	National Intelligence Estimate
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency
NIPRNET	Unclassified (but Sensitive) Internet Protocol Routing Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NITB	National INFOSEC Technical Baseline
NIWA	Naval Information Warfare Activity
NMCC	National Military Command Center
NOC	Network Operating Centers
NOSC	Network Operation Security Center
NRC	National Research Center
NRIC	Network Reliability and Interoperability Council
NRO	National Reconnaissance Office
NRT	Near-Real-Time
NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSD	National Security Directive
NSIRC	National Security Incident Response Center
NSOC	National Security Operations Center
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NTIA	National Telecommunications and Information Administration
OAS	Organization of American States
OASD(C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)

OCI	Offensive Counter Information
OCONUS	Outside the Continental United States
OECD	Organization for Economic Cooperation and Development
OEEC	Organisation for European Economic Co-operation
OET	Office of Engineering & Technology
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
OPSEC	Operations Security
ORNL	Oak Ridge National Laboratory
OSD	Office of the Secretary of Defense
OSD/JS	Office of the Secretary of Defense/Joint Staff
OSE	Open Systems Environment
OUSD(P)	Office of the Under Secretary of Defense (Policy)
PCC	Permanent Consultative Committees
PCCIP	President's Commission on Critical Infrastructure protection
PCS	Personal Communications Service
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKE	Public Key Encryption
POSIX	Portable Operating System for Information Exchange
PPBS	Planning, Program, and Budgeting System
PPTP	Point-to-Point Tunneling Protocol
PRA	Paperwork Reduction Act
PSN	Public Switched Network
PSYOP	Psychological Operations
QDR	Quadrennial Defense Review
R&D	Research and Development
RBOCs	Regional Bell Operating Companies
RCC	Regional Control Center
RCC PAC	RCC Pacific
RCERTs	Regional Computer Emergency Response Teams
RDT&E	Research, Development, Test and Evaluation

RII	Relevant Information and Intelligence
ROSC	Regional Operations and Security Center
S&T	Science and Technology
S/A	Services/Agencies
SABI	Secret and Below Interoperability
SABI WG	Secret and Below Interoperability Working Group
SAIC	Science Applications International Corporation
SATAN	Systems Administrators' Tool for Assessing Networks
SBU	Sensitive-But-Unclassified
SCI	Sensitive Compartmented Information
SECDEF	Secretary of Defense
SEI	Software Engineering Institute
SET	Secure Encrypted Transaction
SIO	Special Information Operations
SIPRNET	Secret Internet Protocol Routing Network
SNET	Southern New England Telephone Company
SORTS	Status of Resources and Training System
SPB	Security Policy Board
SSAA	Systems Security Authorization Agreement
STIGs	Security Technical Implementation Guides
TAFIM	Technical Architecture Framework for Information Management
THREATCON	Threat Condition
TRANSEC	Transmission Security
TRIPS	Trade-Related Aspects of Intellectual Property Rights
U.S.C.	U.S. Code
UCMJ	Uniform Code of Military Justice
UNCITRAL	United Nations Conference on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNISTE	UN International Symposium on Trade Efficiency
URL	Uniform Resource Locator (also Universal Resource Locator)
US	United States
USACOM	U.S. Atlantic Command

USD	Undersecretary of Defense for Policy
USSS	United States Secret Service
VAAP	Vulnerability and Assessment Program
VAS	Vulnerability Assessment System
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WEU	Western European Union
WIPO	World Intellectual Property Organization
WTO	World Trade Organization
Y2K	Year 2000

Appendix F Glossary

APPENDIX F
GLOSSARY

This page intentionally left blank.

NOTE: The source of a definition is shown in brackets. Multiple definitions and their sources are shown where there is significant variance between definitions.

Access Control – Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NSTISSI 4009, 1996]

Accountability – 1. (COMSEC) Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information; 2. (Information Systems) Property that allows auditing of information system activities to be traced to persons or processes that may then be held responsible for their actions. [NSTISSI 4009, 1996]

Accreditation – Formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NSTISSI 4009, 1999]

Advanced Intelligent Network (AIN) – A proposed intelligent-network (IN) architecture that includes both IN/1+ and IN/2 concepts. [Federal Standard 1037C]

Application Program Interface (API) – A formalized set of software calls and routines that can be referenced by an application program in order to access supporting network services. [Federal Standard 1037C]

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 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 – The intentional act of attempting to bypass security controls on an Automated Information System. [JIWG Proposed Common Terminology]

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. [Joint Pub 1-02, 1994]

Audit – Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NSTISSI No. 4009, 1999]

Authenticate – To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission. [NSTISSI 4009, 1996]

Automated Information System Security – Measures and controls that protect AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions, characteristics and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computer, and terminal facilities; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the AIS and for the data and information contained in the AIS. It includes the totality of security safeguards needed to provide an acceptable protection level for AIS and for data handled by AIS. [NCSC TG-004]

Automated Systems Security Incident Support Team (ASSIST) – An integrated DOD operational response capability for handling information systems security incidents, attacks and threats to DOD-interest automated telecommunications systems. ASSIST provides telephonic, on-line, and on-site support 24 hours a day, 7 days a week, 52 weeks a year. [http://www.fas.org/irp/congress/1996_hr/s960605a.htm]

Availability – Ensuring that data transmission or computing processing systems are not denied to authorized users. [CJCSI 6510.01B, 1997]

Availability of Services – Timely, reliable access to data and information services for authorized users. [NSTISSI 4009, 1996]

Banking and Finance – The retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support entities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loans and other financial instruments. [IPTF-PoA, 1996]

Biometrics – Automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristics. [NSTISSI No. 4009, 1999]

Certification – Comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NSTISSI No. 4009, 1999]

Certification Authority (CA) – Third level of the Public Key Infrastructure (PKI) Certification Management Authority responsible for issuing and revoking user certificates, and exacting compliance to the PKI policy as defined by the parent Policy Creation Authority (PCA). [NSTISSI No. 4009, 1999]

Certificate Authority Workstation (CAW) – Commercial-off-the-shelf (COTS) workstation with a trusted operating system and special purpose application software that is used to issue certificates. [NSTISSI No. 4009, 1999]

Code of Federal Regulations – A codification of the Federal Register wherein all regulations and amendments thereto, in force, are codified and brought together by subject. [<http://call.army.mil/call/thesaur/index.htm>]

Clandestine Operation – An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. [Joint Pub 1-02, 1994]

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, 1995]

Client-Server Architecture – Any network-based software system that uses client software to request a specific service, and corresponding server software to provide the service from another computer on the network. [FS -1037C, 1966]

Combatant Command – A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. [JP 1-02]

Command and Control-Protect (C2-Protect) – The maintenance of effective C2 of own forces by turning to friendly advantage or negating adversary efforts to deny information to, to influence, to degrade, or to destroy the friendly C2 system; C2-protect can be offensive or defensive in nature; offensive C2-protect uses the five elements of C2W to reduce the adversary's ability to conduct C2-attack; defensive C2-protect reduces friendly C2 vulnerabilities to adversary C2-attack by employment of adequate physical, electronic, and intelligence protection. [Field Manual 100-6 (adapted from CJCSI 3210.03), 1996]

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. 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. [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.*

Command, Control, Communications, and Computer (C4) Systems – Integrated systems of doctrine, procedures, organizational structures, personnel, equipment, facilities, and communications designed to support a commander's exercise of command and control, through all phases of the operational continuum. [JP-02]

Commercial-off-the-shelf (COTS) – An item of hardware or software that has been produced by a contractor and is available for general purchase. Such items are at the unit level or higher. Further, such items must have meaningful reliability, maintainability, and logistics historical data. [DISA, *TAFIM*, 1997]

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, emission security, and physical security of COMSEC material. [NSTISSI 4009, 1996]

Computer Crime – Fraud, embezzlement, unauthorized access, and other crimes committed with the aid of or directly involving an AIS. [USAF Manual 33-270]

Computer Intrusion – An incident of unauthorized access to data or an Automated Information System. [JIWG]

Computer Security – Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated. [NSTISSI No. 4009, 1999]

Concept of Operations (CONOP) – Document detailing the method, act, process, or effect of using an IS. [NSTISSI No. 4009, 1999]

Confidentiality – Assurance that information is not disclosed to unauthorized entities, or processes. [NSTISSI 4009, 1996]

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, 1994]

Cookie – A message given to a Web browser (such as Netscape) by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. When entering a Web site using cookies, a user may be asked to fill out a form providing such information as name and interests. This information is packaged into a cookie and sent to the Web browser which stores it for later use. The next time the user goes to the same Web

site, the browser will send the cookie to the Web server. The server can use this information to present with custom Web pages. So, for example, instead of seeing just a generic welcome page, users might see a welcome page with their own name on it. The name cookie derives from UNIX objects called magic cookies. These are tokens that are attached to a user or program and change depending on the areas entered by the user or program. Cookies are also sometimes called persistent cookies because they typically stay in the browser for long periods of time. [*PC Webopaedia*, 1997]

Correlation – The process which associates and combines data on a single entity or subject from independent observations, in order to improve the reliability or credibility of the information. [JIWG Proposed Common Terminology]

Covert Action – An operation that is so planned and executed as to conceal the identity or permit plausible denial by the sponsor. [USC 50 § 413b]

Critical Asset – Any facility, equipment, service, or resource considered essential to DOD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration. Critical assets may be DOD assets or other government or private assets, (e.g., Industrial or Infrastructure Critical Assets), domestic or foreign, whose disruption or loss would render DOD Critical Assets ineffective or otherwise seriously disrupt DOD operations. Critical assets include both traditional "physical" facilities or equipment, non-physical assets (such as software systems) or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks). [DODD 5160.54, Jan. 1998]

Critical Infrastructures – Certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include 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. [Executive Order 13010]

Cryptography – Art of science concerning the principles, means, and methods for rendering plain information unintelligible and of restoring encrypted information to intelligible form. [NSTISSI 4009, 1996]

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. [Joint Pub 1-02, 1994]

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, 1995]

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. [Joint Pub 1-02, 1994]

Data Encryption Standard (DES) – Cryptographic algorithm, designed for the protection of unclassified data and published by the National Institute of Standards and Technology in Federal Information Processing Standard (FIPS) Publication 46. [NSTISSI No. 4009, 1999]

Defense in Depth – 1. The siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver his reserve. [JP1-02] 2. The security approach, whereby each system on the network is secured to the greatest possible degree. May be used in conjunction with firewalls.
[<http://www.thewall.com/glossary.htm>]

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 Switched Network – Component of the Defense Communications System that handles Department of Defense voice, data, and video communications.
[<http://call.army.mil/call/thesaur/index.htm>]

Defensive Counterinformation – Actions protecting our military information functions from the adversary. [Air Force, *Cornerstones of Information Warfare*, 1995]

Defensive Information Operations – The defensive IO process integrates and coordinates policies and procedures, operations, personnel, and technology to protect information and to defend information systems. Defensive IO are conducted through information assurance, physical security, operations security, counter deception, counter psychological operations, counter intelligence, electronic protect, and special information operations. Defensive IO objectives ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems for their own purposes. [CJCSI 6510.01B, 1997]

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 an information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services. [CJCSI 6211.02, 1993]

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]

Discretionary Access Control (DAC) – Means of restricting access to objects based on the identity and need-to-know of users and/or groups to which the object belongs. Controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (directly or indirectly) to any other subject. See mandatory access control. [NSTISSI No. 4009, 1999]

Domain Name Servers – Servers that retain the addresses and routing information for TCP/IP LAN users. [Federal Standard 1037C]

Electrical Power Systems – The generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system. [IPTF-PoA, 1996]

Electronic Data Interchange – The sending, transmission, reception, and interchange of information and data relating to business transactions via electronic means. EDI is analogous to EFT (Electronics Funds Transfer) but it is more complicated to establish standards for EDI, as each organization typically has its own document formats, its own ordering and invoice practices. Establishing an EDI service involves devising a standard format for each type of transaction that suits all participants. EDI has developed from pioneer work initially in the United Kingdom and later the rest of Europe and the USA. [<http://call.army.mil/call/thesaur/index.htm>]

Electronic Warfare (EW) – 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]

Emergency Services – The medical, police, fire and rescue systems and personnel that are called upon when an individual or community is responding to a public health or safety incident where speed and efficiency are necessary. [IPTF-PoA, 1996]

Encryption – Process of transforming data into an unintelligible form to conceal its meaning. [USAF Manual 33-270]

Event – any suspicious pre-assessed activity. [JIWG Proposed Common Terminology]

Firewall – A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. [*PC Webopaedia*, 1997]

Fraud (Computer) – Computer-related crimes involving deliberate misrepresentation or alteration of data to get something of value, usually for monetary gain. A computer system must have been involved in the preparation or cover-up of the act, or series of acts, through improper manipulation of input or output data, applications programs, data files, computer operations, communications, or computer hardware, software, or firmware. [USAF Manual 33-270]

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). [Joint Pub 1-02, 1994]

Gas and Oil Production, Storage and Transportation – The holding facilities for natural gas, crude and refined petroleum, and petroleum-derived fuels, the refining and processing facilities for these fuels and the pipelines, ships, trucks, and rail systems that transport these commodities from their source to systems that are dependent upon gas and oil in one of their useful forms. [IPTF-PoA, 1996, 1996]

Global Information Infrastructure (GII) – Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services. [CJCSI 6510.01B, 1997]

Government Services Information Infrastructure (GSII) – The U.S. Government information infrastructure portion of the National Information Infrastructure (NII) used to link people to government and its services. Sometimes referred to as Government Information Technology Services (GITS). [GITS document, Chapter A-15]

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, 1996]

Human Intelligence – A category of intelligence derived from information collected and provided by human sources. [<http://call.army.mil/call/thesaur/index.html>]

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 bankcard. [CJCSI 6510.01B, 1997]

Imagery – Collectively, the representation of objects reproduced electronically or by optical means on file, electronic display devices, or other media. [Joint Pub 1-02, 1994]

Incident – An assessed event of attempted entry, unauthorized entry, and/or an information attack on a AIS. It includes unauthorized probing, browsing; disruption, or denial of service; altered or destroyed input, processing, storage, or output of information; or changes to system hardware, firmware, or software characteristics with or without the users knowledge, instruction or intent (e.g., malicious logic). [JIWG Proposed Common Terminology]

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 U.S. 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. [Joint Pub 1-02, 1994]

Indicator – An action specific, generalized or theoretical, that an adversary might be expected to take in preparation for an aggressive act. [JIWG Proposed Common Terminology]

Information – 1. Facts, data, or instructions in any medium or form. [DoDD S-3600.1, 1996]; 2. The meaning that a human assigns to data by means of the known conventions used in their representation. [Joint Pub 1-02, Mar 94]; 3. Any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. [DISA, *TAFIM*, 1997; OMB Circ A-130, 1996]

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. [DoDD S-3600.1, 1996]

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, 1995]

Information Operations (IO) – Actions taken to affect adversary information and ISs while defending one's own information and ISs. [NSTISSI No. 4009, 1999]

Information Security – The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [FS -1037C, 1996]

Information Superiority – That degree of dominance in the information domain which permits the conduct of operations without effective opposition. [DoDD S-3600.1, 1996]

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, 1996]

Information Systems Security – 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 (includes those measures necessary to detect, document, and counter such threats). [NSTISSI 4009, 1996]

Information Warfare (IW) – Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. [DoDD S-3600.1, 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, *Report: Options*]

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, *Report: Options*]

Integrity – Absolute verification that data has not been modified in transmission or during computer processing. [CJCSI 6510.01B, 1997]

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. [Joint Pub 1-02, 1994]

Interoperability – The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. [Joint Pub 1-02, 1994]

Java – A high-level, object-oriented programming language similar to C++, but simplified to eliminate language features that cause common programming errors. Java source code files (files with a java extension) are compiled into a format called bytecode (files with a .class extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as Java Virtual Machines (VMs), exist for most operating systems, including UNIX, the Macintosh OS, and Windows. Bytecode can also be converted directly into machine language instructions by a just-in-time compiler (JIT). Small Java applications, called Java applets, can be downloaded from a Web server and run on a computer by a Java-compatible Web browser, such as Netscape Navigator or Microsoft Internet Explorer. Microsoft has stated that it intends to include a Java interpreter in future versions of Windows, which will enable users to execute Java applets directly from the operating system. [PC Webopaedia, 1997]

Legacy Systems – Systems that are candidates for phase-out, upgrade, or replacement. Generally, legacy systems are in this category because they do not comply with data standards or other standards. Legacy system workloads must be converted, transitioned, or phased out (eliminated). Such systems may or may not operate in a legacy environment. [TAFIM, 1997]

Local Area Network (LAN) – A data communications system that lies within a limited spatial area, has a specific user group, has a specific topology, and is not a public switched telecommunications network, but may be connected to one. (Note: LANs are usually restricted to relatively small areas, such as rooms, buildings, ships, and aircraft. An interconnection of LANs within a limited geographical area, such as a military base, is commonly referred to as a campus area network. An interconnection of LANs over a city-wide geographical area is commonly called a metropolitan area network (MAN). An interconnection of LANs over large geographical areas, such as nationwide, is commonly called a wide area network (WAN). LANs are not subject to public telecommunications regulations. [FS -1037C, 1996]

Logic Bomb – Resident computer program triggering an unauthorized act when particular states of an IS are realized. [NSTISSI No. 4009, 1999]

Malicious Logic – Hardware, software, or firmware that is intentionally included into an information system for an unauthorized purpose (e.g., virus & Trojan horse). [JIWG Proposed Common Terminology]

Mandatory Access Control (MAC) – Means of restricting access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. See discretionary access control. [NSTISSI No. 4009, 1999]

Middleware – Software that connects two otherwise separate applications. For example, there are a number of middleware products that link a database system to a Web server. This allows users to request data from the database using forms displayed on a Web

browser, and it enables the Web server to return dynamic Web pages based on the user's requests and profile. The term middleware is used to describe separate products that serve as the glue between two applications. It is, therefore, distinct from import and export features that may be built into one of the applications. Middleware is sometimes called plumbing because it connects two sides of an application and passes data between them. In a three-tier architecture, middleware occupies the middle tier. [*PC Webopaedia*, 1997]

Multiple Security Level/Multilevel Security (MLS) – Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization. [NSTISSI No. 4009, 1999]

National Information Infrastructure (NII) – 1. The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the national information infrastructure. [Joint Pub 3-13, Draft, 1997]. 2. 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. [IITF, *NII Security: The Federal Role*, 1995]

National Security Systems – Those telecommunications and information systems operated by the U.S. 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]

Offensive Information Operations – The integrated use of assigned and supporting capabilities and processes, mutually supported by intelligence, to affect information and information systems to achieve or promote specific objectives. These capabilities and processes include, but are not limited to, operations security, military deception, psychological operations, electronic warfare, and physical destruction. [Joint Pub 3-13, Draft, Jul 1997]

Open System – 1. 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. [PCCIP]; 2. A system with characteristics that comply with specified, publicly maintained, readily available standards and that therefore can be connected to other systems that comply with these same standards. [FS -1037C, 1996]

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. [TAFIM, 1997]

Operations Security (OPSEC) – OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by adversary intelligence systems, (b) 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, and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [Joint Pub 1-02, 1994]

Penetration Testing – Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. [NSTISSI No. 4009, 1999]

POSIX – Acronym for portable operating system interface for computer environments. A Federal Information Processing Standard Publication (FIPS PUB 151-1) for a vendor-independent interface between an operating system and an application program, including operating system interfaces and source code functions. IEEE Standard 1003.1-1988 was adopted by reference and published as FIPS PUB 151-1. [FS -1037C, 1966]

Public Key Encryption – Also known as asymmetric key encryption. Relies on two keys, one public and one known only to its owner. Most on the market today are based on the RSA algorithm. These tend to be much slower than private key ciphers and normally require significantly longer keys to provide the same level of security. [<http://io.datasys.swri.edu/freeburg/glossary.html#W>]

Public Key Infrastructure (PKI) – Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. [NSTISSI No. 4009, 1999]

Public Switched Network (PSN) – Any common carrier network that provides circuit switching among public users. Note: The term is usually applied to public switched telephone networks, but it could be applied more generally to other switched networks, e.g., packet-switched public data networks. [Federal Standard 1037C]

Precedence –A designation assigned to a message by the originator to indicate to communications personnel the relative order of handling and to the addressee the order in which the message is to be noted. [Joint Pub 1-02, 1994]

Protocol – 1. Set of rules and formats, semantic and syntactic, that permits entities to exchange information. [NSTISSI 4009, 1996]; 2. A formal set of conventions governing the format and control of interaction among communicating functional units. Protocols may govern portions of a network, types of service, or administrative procedures. For example, a data link protocol is the specification of methods whereby data communications over a data link are performed in terms of the particular transmission mode, control procedures, and recovery procedures. In layered communications system architecture, a formal set of procedures that are adopted to facilitate functional interoperation within the layered hierarchy. [FS -1037C, 1996]

Psychological Operations (PSYOP) – Planned operations 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 U.S. 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]

Readiness – Ability of forces, units, and weapon systems to deliver the designed output. [<http://call.army.mil/call/thesaur/index.htm>]

Reliability – 1. The ability of an item to perform a required function under stated conditions for a specified period of time. 2. The probability that a functional unit will perform its required function for a specified interval under stated conditions. 3. The continuous availability of communication services to the general public and emergency response activities in particular, during normal operating conditions and under emergency circumstances with minimal disruption. [Federal Standard 1037C]

Risk – The probability that a particular threat will exploit a particular vulnerability of the system. [NSA, NCSC *Glossary*, 1988]

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*, 1988]

Risk Assessment – Process of analyzing threats to and vulnerabilities of an information system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective counter-measures. Synonymous with risk analysis. [NSTISSI No. 4009, 1996]

Risk Management – The total process of identifying, measurement, controlling, and minimization of security risks in information systems to a level commensurate with the value of the assets protected. [NSTISSI No. 4009, 1996]

Security Management – In network management, the set of functions: (1) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences, and (b) that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges. [Federal Standard 1037C]

Security Measures (Metrics) – Elements of software, firmware, hardware, or procedures that are included in a system for the satisfaction of security specifications. [NCSC TG-004]

Security Policies – A set of rules and procedures regulating the use of information including its processing, storage, distribution, and presentation (Working Group 3N102). [Joint Technical Committee/Subcommittee 27/N734]

Security Test and Evaluation – An examination and analysis of the security safeguards of a system as they have been applied in an operational environment to determine the security posture of the system. [NCSC Glossary, 1988]

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, 1996]

Sniffers – Software tool for auditing and identifying network traffic packets. [NSTISSI No. 4009, 1999]

Social Engineering – A deception technique utilized by hackers to derive information or data about a particular system or operation. [PCCIP, *Hacker Primer*, 1997]

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: (a) country of origin – country or countries initiating hostilities, (b) event type and size – identification of the type of event and determination of the size and number of weapons, (c) country under attack – determined by observing trajectory of an object and predicting impact point, and (d) event time – time the hostile event occurred. [Joint Pub 1-02, 1994]

Technical Architecture – A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformal system satisfies a specified set of requirements. [<http://call.army.mil/cal/thesaur/index.htm>]

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]

Telecommunications – 1. Preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electro-mechanical, electro-optical, or electronic means. [NSTISSI 4009, 1996]; 2. Any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. [Joint Pub 1-02, 1994]

Threat – Any circumstance or event with the potential to cause harm to an AIS in the form of destruction, disclosure, modification of data, or denial of service. [JIWG Proposed Common Terminology]

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 cryptanalysis. [NSTISSI 4009, 1996]

Transportation – The aviation, rail, highway, and aquatic vehicles, conduits, and support systems by which people and goods are moved from a point-of-origin to a destination point in order to support and complete matters of commerce, government operations, and personal affairs. [IPTF-PoA, 1996]

Trashing – Hacker term for physically entering the trash containers at a target site in hopes of finding valuable information such as passwords, system documentation, or employee personal information to be used for social engineering attacks. [PCCIP, *Hacker Primer*, 1997]

Trojan Horse Software – Program containing hidden code allowing the unauthorized collection, falsification, or destruction of information. [NSTISSI No. 4009, 1999]

Trustworthy Systems – Systems that employ sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information. [TNI]

Verifiability/Verification – The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). This process may or may not be automated. [NCSC TG-004]

Virtual Network – 1. A network that provides virtual circuits and that is established by using the facilities of a real network [FS -1037C, 1996]; 2. A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable one to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. [*PC Webopaedia*, 1997]

Virus – Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence. [NSTISSI 4009, 1996]

Vulnerability Analysis – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [USAF Manual 33-270]

Vulnerability Assessment – Systematic examination of an IS or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. [NSTISSI No. 4009, 1999]

Water Supply Systems – The sources of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration and cleaning systems, the pipelines, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with waste water and fire fighting. [IPTF-PoA, 1996]

Web Server – A computer that delivers (serves up) Web pages. Every Web server has an IP address and possibly a domain name. For example, if you enter the URL, <http://www.sandybay.com/index.html>, in your browser, this sends a request to the server whose domain name is sandybay.com. The server then fetches the page named index.html and sends it to your browser. Any computer can be turned into a Web server by installing server software and connecting the machine to the Internet. There are many Web server software applications, including public domain software from NCSA and commercial packages from Microsoft, Netscape and others. [*PC Webopaedia*, 1997]

Wide Area Network (WAN) – Computer network that services a large area. WANs typically span large areas (i.e., states, countries, and continents) and are owned by multiple organizations. [USAF Manual 33-270]

Wiretaps – An unauthorized device, such as a computer terminal, to a communications circuit to gain access to data by generating false messages or control signals, or by altering legitimate users' communications. [USAF Manual 33-270]

This page intentionally left blank.

APPENDIX G
INDEX

This page intentionally left blank.

A

Accreditation · 1-4, 3-12, 3-14, A-11, A-72, A-76, A-80, A-84, A-218, D-7, D-8, D-41, D-43, D-45, D-57, D-58, D-59, D-70, E-3, E-6, F-3, F-4

Acquisition Support and Product Development · A-11, A-15

Administrator of the Economics and Statistics Administration · A-108

Advanced Encryption Standard · A-112, E-3

Advanced Technology Program · A-112

AFIWC Plans Office · A-60

Air Force C4 Agency · E-3

Air Force Information Warfare Center · A-3, A-52, A-57, E-3

Air Force Office of Special Investigation · 2-8, A-52, C-11, E-3

Air Force Reserve · 5-7

Air Intelligence Agency · A-53

Air National Guard · 5-7

America OnLine · 2-10

American National Standards Institute · 4-11, E-3

Analysis and Warning Section · A-155

Analysis Support Division · A-60

Antiterrorism Act · A-159

Application Programming Interface · 4-3, E-3

Architecture and Integration · A-67

Army National Guard · 5-7

Army Reserve · 5-7

ASD C3I · 5-1, A-9, B-35, B-36

Assessments and Emergency Response Division · A-58

Asymmetric · 2-12, 4-5, 4-6, F-15

Asynchronous Transfer Mode · 4-3, E-3

Attack and Incident Mitigation · A-112

Audit · A-62, A-171, A-233, A-234, B-31, C-37, D-34, D-38, D-45, D-58, E-3, F-3, F-17

Authentication · 3-3, 4-3, 4-5, 4-6, 4-7, 4-11, A-67, A-76, A-80, A-138, A-213, B-21, C-38, D-38, D-44, D-63, F-11

Automated Information Systems Security · D-7, D-39

Automated Infrastructure Management System · A-75, E-3

Automated Security Incident Measurement · A-54

Automated Security Incident Measuring System · E-3

Automated Systems Security Incident Support Team · F-4

Availability · 1-3, 2-3, 3-1, 3-14, 4-2, 4-3, A-52, A-81, A-108, A-117, A-133, A-186, A-213, B-21, C-7, C-9, C-37, D-16, D-40, D-41, D-59, D-60, D-61, D-70, F-4, F-6, F-11, F-16

B

Baldrige National Quality Program · A-112

Bilateral Information Operations Steering Group · A-9

Biometrics · A-79, F-4

Bureau of Alcohol, Tobacco and Firearms · A-170

Bureau of Census · A-108

Bureau of Diplomatic Security · A-159, A-161

Bureau of Economic Analysis · A-108

Bureau of Engraving and Printing · A-171

Bureau of Export Administration · 2-12, A-107, A-108, C-33, C-35, C-36, C-38, E-3

Bureau of Intelligence and Research · A-160

Bureau of Public Debt · A-170, B-15

C

C2 Networks Division · A-58

C2W Analysis Division · A-60

C2W Information Directorate · A-58

C2W Integrated Analysis Division · A-58

C2W Operations Division (OSJ) · A-60

C4 Database System (CDS) · A-62

C4I Integration Support Activity · A-8, E-4

Capability Analysis Division · A-60

Cellular Priority Access Service · B-21

Cellular Priority Service · B-21

Central Intelligence Agency · 3-7, A-4, A-175, B-20, B-26, C-27, C-29, D-21, D-28, E-4

Certificate Authority Workstations · A-77

Certification · 1-4, 3-12, 3-14, 4-6, 5-5, A-11, A-24, A-54, A-67, A-70, A-72, A-73, A-80, A-84, A-138, A-161, A-218, C-18, C-19, D-7, D-8, D-12, D-38, D-39, D-41, D-43, D-59, D-70, E-3, E-4, E-6, F-4

Certification and Accreditation Working Group · A-11, E-3

Certification Authority · E-4, F-4

Chief Engineer · A-71

Chief Information Officer · 1-1, 2-15, 3-7, 3-15, 4-12, A-7, A-27, A-32, A-37, A-51, A-107,

A-109, A-111, A-121, A-124, A-159, A-163,
 A-166, A-193, A-197, A-200, A-203, A-217,
 A-221, B-7, C-31, C-32, D-15, D-23, E-4
 Chief Information Officers Council · 2-15
 Chief of Naval Education and Training · A-38
 Chief, Assessment and Certification Division ·
 A-161
 CJCSI 3210.01 · A-23, A-24, D-9, D-65
 CJCSI 6510.01B · 3-10, D-9, D-66, F-4, F-8, F-10,
 F-11, F-12
 Classified Information Systems Security
 Program · A-122
 Coalition Communications and Electronics
 Board · 1-4
 Coalition Vulnerability Assessment Team · A-74
 Code of Federal Regulations · 2-11, C-33, E-4, F-5
 Combatant Commands · 5-8, A-76, A-83, A-84
 Command and Control Warfare · A-23, A-31,
 A-38, A-48, A-58, A-60, D-66, E-4, F-5
 Command, Control, Communications, and
 Computer · E-4, F-6
 Commander in Chief, U.S. Atlantic Fleet · A-41,
 E-4
 Commander in Chief, U.S. Naval Force Europe ·
 A-41, E-4
 Commander in Chief, U.S. Pacific Fleet · A-41,
 E-4
 Commander of the Combined Arms Command ·
 A-32, E-4
 Commander, U.S. Naval Forces Central
 Command · A-41, E-5
 Commerce Control List · A-107, C-33, E-4
 Commercial Off-the-Shelf · 4-9, A-75, E-5
 Committees of the House of Representative · A-4
 Committees of the Senate · A-4
 Common Operating Environment · 4-3, A-74,
 E-5
 Common Operational Picture · 4-3, E-5
 Communications Act · A-103, C-3, C-9, C-21,
 D-5, D-11, D-14
 Communications and Information Infrastructure
 Assurance Program · A-117, A-118
 Communications Assistance for Law
 Enforcement Act · C-3, C-14, C-15, D-12
 Communications Decency Act · D-14
 Communications Resource Information Sharing
 · B-23
 Computer (and Network) Security Incident
 Response · A-204, E-5
 Computer Crime · 2-1, 2-2, 2-3, 2-6, 2-7, 2-8,
 A-149, A-150, A-151, A-152, A-171, A-172, B-9,
 C-6, C-11, C-12, C-13, C-14, F-6
 Computer Crime and Intellectual Property · 2-1,
 2-6, A-149
 Computer Emergency Response Teams · 3-13,
 A-72, D-54, E-12
 Computer Fraud and Abuse Act · 2-2, 2-3, 2-4,
 2-5, 2-7, C-3, C-6, D-16
 Computer Incident Advisory Capability · A-73,
 A-121, A-125, A-129, E-4
 Computer Incident Response Team · A-38, A-42,
 A-48, E-4, E-10
 Computer Investigations and Operations Section
 · A-156
 Computer Network Attack · 3-3, 3-9, 3-18, 5-3,
 A-22, A-23, A-79, D-68, E-5
 Computer Security · A-42, A-52, A-54, A-58,
 A-62, A-97, A-98, A-111, A-112, A-113, A-124,
 A-125, A-129, A-138, A-150, A-199, A-200,
 A-217, A-218, A-233, B-3, B-13, B-35, C-3, C-5,
 C-6, C-15, C-32, D-5, D-6, D-9, D-12, D-13,
 D-14, D-29, D-33, D-34, D-36, D-37, D-43,
 D-49, D-57, D-60, D-61, E-5, E-10, E-11, F-6,
 F-17
 Computer Security Act · A-98, A-112, B-13, C-3,
 C-5, C-6, C-15, C-32, D-5, D-12, D-13, D-14,
 D-29, D-33, D-36, D-37, E-5, F-17
 Computer Security Awareness · A-218
 Computer Security Division · A-111, A-112
 Computer Security Engineering Team · A-58
 Computer Security Enhancement Act · C-3, C-5
 Computer Security Organization · A-129
 Computer Security Resource Clearinghouse ·
 A-113
 Computer Security Technology Center · A-129
 Computer System Security and Privacy
 Advisory Board · A-112, C-6, C-15, C-17, D-12
 Computer Systems Security Officers · A-62,
 A-150, E-5
 Concept of Operations · A-178, E-5, F-6
 Concepts and Requirements Division · A-58
 Confidentiality · 3-10, 4-2, 4-3, 4-5, 4-11, A-80,
 A-186, C-8, C-37, D-14, D-16, D-17, D-40,
 D-41, D-59, D-70, F-6, F-11
 Connection Approval · A-72, A-73, E-4
 Connection Approval Process · A-73
 Contingency Operations · A-71, B-21, D-50
 Council of Colonels · A-32
 Counter-Intelligence · A-7, A-32, A-57, D-51
 Countermeasure Engineering Team · A-58
 Countermeasures Division · A-58
 Counter-Terrorism Program Coordination Team
 · A-177
 Critical Asset Assurance Program · 3-1, 3-12, 5-8,
 A-10, A-51, E-4

Critical Assets · 3-12, 3-13, A-10, D-8, D-53, D-54, F-7
Critical Infrastructure Assurance Office · 3-7, 5-6, A-9, A-107, A-121, A-163, B-3, B-5, D-28
Critical Infrastructure Assurance Officer · A-121, A-163
Critical Infrastructure Coordination Group · 3-7, A-93, D-28
Critical Infrastructure Program · A-24
Critical Infrastructure Protection · 1-1, 1-3, 3-1, 3-2, 3-5, 3-7, 3-13, 5-6, A-7, A-9, A-10, A-12, A-41, A-47, A-51, A-65, A-79, A-80, A-83, A-93, A-95, A-97, A-101, A-104, A-107, A-111, A-113, A-117, A-121, A-133, A-137, A-141, A-145, A-149, A-155, A-163, A-165, A-169, A-175, A-177, A-197, A-203, A-217, A-221, A-233, B-5, B-6, B-19, B-25, B-29, B-31, B-32, B-43, B-47, B-48, C-3, C-11, C-28, C-29, D-5, D-21, D-28, D-54, E-4
Critical Infrastructure Protection Working Group · 3-13, A-10, D-54, E-4
critical Infrastructures · 1-1, 1-2, 1-3, 3-1, 3-5, 3-6, 5-6, 5-8, A-104, A-142, A-155, A-156, A-212, B-5, B-7, B-48, C-28, C-29, C-30, D-5, D-21, D-22, D-23, D-28, E-4, F-7
Critical Infrastructures Assurance Office · 5-6, E-4
Critical Protection Working Group · A-9
Critical Technologies Group · A-175
Critical Vulnerabilities · A-71
Crypto-Control · 4-6
Current Operations Division · A-60

D

DARPA Information Assurance Program · A-66
DARPA Information Systems Office · A-66
DARPA Information Technology Office · A-65
Data Encryption Standard · A-112, F-8
Data Systems Research and Development · A-137
DCID 1/16 · D-9, D-60, D-69
DDCI for Community Management · A-9
Dedicated Hardware · A-186
Defense Advanced Research Projects Agency · A-3, A-65, E-5
Defense Courier Service · A-8, D-51
Defense Finance and Accounting Service · 4-11, E-5
Defense Goal Security Architecture · 4-10
Defense IA Command and Control System · A-75, E-5

Defense In Depth · A-71, A-72
Defense Information Assurance Program · 3-7, 4-12, A-10, E-5
Defense Information Infrastructure · 3-8, 3-13, 4-3, 5-2, 5-5, A-10, A-67, A-69, A-138, D-16, D-54, E-5, F-8
Defense Information System Network · 4-3
Defense Information Systems Agency · 5-5, A-3, A-8, A-69, A-79, B-14, B-36, D-8, D-26, D-49, D-51, E-6
Defense Information Technology Security Certification and Accreditation Process · 3-12, D-59
Defense Information Technology Security Working Group · 1-4, E-6
Defense Intelligence Agency · 5-2, A-3, A-8, A-21, A-83, B-36, D-26, D-49, D-51, D-66, E-5
Defense Intrusion Analysis & Monitoring Desk · A-70, E-5
Defense Investigative Service · 3-13, A-8, D-51, D-54
Defense Logistics Agency · 4-11, A-199
Defense Megacenters · A-75
Defense Messaging System · E-6
Defense Personnel Security Research Center · A-8, D-51
Defense Planning, Program, and Budgeting System · 5-4
Defense Polygraph Institute · A-8, D-51
Defense Program Guidance · 3-5, E-6
Defense Reform Initiative · A-76
Defense Satellite Communications Systems · E-6
Defense Science Board · 3-2, A-109, D-9, D-62, E-6
Defense Security Service · 3-13, D-54
Defense Support Project Office · A-8, D-51
Defensive Information Warfare Branch · A-38
Department of Commerce · 2-12, 3-4, 3-7, A-3, A-88, A-107, A-109, A-111, A-113, B-5, B-7, B-8, B-9, B-13, B-19, C-15, C-29, C-32, C-33, C-35, C-36, C-38, D-21, D-28, D-33, E-6
Department of Health and Human Services · 3-7, A-3, A-145, B-19, D-28
Department of Justice · 2-1, 2-7, 2-8, 2-9, 2-11, 3-4, 3-7, A-3, A-149, A-178, B-9, B-14, B-19, C-15, C-18, C-29, D-21, D-22, D-28
Department of State · 3-4, 3-7, A-3, A-117, A-137, A-138, A-159, A-160, A-221, B-15, B-19, C-24, C-32, C-33, D-28, D-50, E-6
Department of the Air Force · A-3, A-31, A-51, C-11
Department of the Army · A-3, A-31, A-32
Department of the Energy · A-3

Department of the Navy · A-3, A-31, A-37, E-6
Department of the Treasury · A-3, A-169, A-171,
B-15, B-19, C-29, D-21
Department of Transportation · 3-7, A-3, A-163,
B-8, B-15, B-19, C-29, D-21, D-28, E-6
Deputy Assistant Secretary of Defense · 5-1, E-5
Deputy Director for Community Intelligence ·
A-9
Detect · 3-10, 3-13, 3-17, 4-2, 4-4, 5-7, A-12, A-48,
A-66, A-67, A-70, A-71, A-130, A-134, A-155,
C-23, C-30, D-23, D-53, D-62, F-11, F-12
Detection · 1-4, 3-8, 3-11, 3-12, 4-2, 4-4, A-15,
A-25, A-42, A-48, A-62, A-67, A-70, A-75,
A-76, A-80, A-81, A-89, A-130, A-149, A-205,
C-12, D-31, D-67, E-3, E-5, E-9, E-10, F-11
Digital Encryption Standard · E-5
Director, Land Information Warfare Activity ·
A-3
Director, National Security Agency · 3-8, 5-5,
A-112, B-36, E-6
Director, Space, Information Warfare, Command
and Control · A-37
Directorate for Intelligence · A-21, A-83
Directorate for Operations, Readiness, and
Mobilization · A-32
Discretionary Access Control · A-114, F-9
Distributed Intrusion Detection System · A-62
DOD Security Institute · A-8, D-51
Domain Name Servers · 4-3, E-6, F-9
Domestic Preparedness Program · A-177, A-179
Dynamic Routing · A-186

E

Economic Espionage Act · C-3, C-7, D-5, D-16
Education, Training, and Awareness · 4-5, A-73
Education, Training, Awareness, and
Professionalization Working Group · A-11
Electronic Combat · A-59, A-60, E-6
Electronic Commerce Program Management
Office · A-199
Electronic Communications Privacy Act · 2-10,
C-3, C-17, D-5, D-12, E-6
Electronic Data Interchange · E-6, F-9
Electronic Freedom Frontier · 3-15, E-6
Electronic Freedom of Information · C-3, C-5, E-6
Electronic Warfare Integrated Reprogramming ·
A-59
Emergency Alert System · A-182, A-186, E-6
Emergency Broadcast System · A-182, C-27, E-6
Encryption · 1-4, 2-1, 2-12, 2-13, 3-1, 3-15, 3-16,
3-17, 4-1, 4-2, 4-3, 4-6, 4-9, 4-11, A-67, A-75,

A-79, A-109, A-112, A-113, A-138, C-3, C-6,
C-13, C-33, C-35, C-38, D-43, D-63, E-3, E-5,
E-12, F-8, F-9, F-15, F-19
Encryption Key Recovery · A-113
Encryption Licensing Arrangements · 2-13
Encryption Policy · 3-16, C-35
End-User Identification · 4-3
Engineering Information Division · A-58
Environmental Protection Agency · 3-7, A-4,
A-177, B-14, B-26, D-28, E-7
Executive Committee for Information
Management · A-125
Executive Office of the President · 3-6, A-3,
A-104, B-14, B-20, C-29, C-32, D-5, D-19, D-20,
D-21, D-22, D-23, D-27, D-30, D-31, D-32,
D-33, E-6
Executive Order 12333 · C-3, C-23, D-5, D-19
Executive Order 12472 · A-98, B-19, C-3, C-25,
D-5, D-19
Executive Order 12958 · C-3, C-27, C-31, D-5,
D-20, F-5, F-7, F-11
Executive Order 13010 · 1-1, C-3, C-28, D-5,
D-21, F-7
Executive Order 13011 · C-3, C-31, C-32, D-5,
D-23
Export Administration Regulations · 2-12, A-107,
C-33
Export of Encryption · 2-12, 3-1, C-3, C-35

F

Federal Acquisition Streamlining Act · 4-10
Federal Aviation Administration · 2-8, 2-11, B-8,
B-15
Federal Bureau of Investigation · 3-7, A-149,
A-150, A-178, B-9, B-14, B-36, C-15, C-18,
C-24, C-29, D-21, D-22, D-28, E-7
Federal Communications Commission · 2-11,
A-4, A-117, A-150, A-181, A-229, B-14, B-20,
B-31, B-37, B-39, C-9, C-10, C-13, C-21, C-22,
C-27, D-11, E-7
Federal Computer Incident Response Capability
· A-197, A-199, E-7
Federal Emergency Management Agency · 3-7,
A-4, A-104, A-178, A-182, A-185, B-14, B-20,
B-36, C-27, C-29, D-21, D-22, D-28, E-7
Federal Guidelines for Searching and Seizing
Computers · 2-6
Federal Information Systems Support Program ·
A-198
Federal Law Enforcement Training Center ·
A-170

Federal Public Key Infrastructure Steering Committee · A-199
Federal Reserve Information Technology · A-190
Federal Reserve System · A-4, A-171, A-189, B-14, B-20
Federal Response Plan · A-104, A-145, D-26
Federal Systems Integration and Management Center · A-198
Federal Trade Commission · A-4, A-193, E-7
Field Security Operations · A-70
Financial Crimes Enforcement Network · A-170, B-15
Firewalls · 1-4, 3-3, 3-12, 4-1, 4-2, 4-3, 4-5, A-67, A-76, A-79, A-80, A-81, A-114, A-186, A-198, A-213, F-8, F-10
Fleet Information Warfare Center · A-3, A-38, A-41, E-7
Foreign Counterintelligence Program · A-8, D-52
Foreign Intelligence Surveillance Act · A-150, A-151, C-3, C-17, C-18, D-5, D-11, D-19
Forum of Incident Response and Security Teams · A-130, A-205, E-7
Fraud · 2-2, 2-3, 2-4, 2-5, 2-7, A-53, A-150, A-159, A-170, A-172, A-183, C-3, C-6, C-14, C-37, D-13, D-16, F-6, F-10
Functional Evaluating and Integration Team · 5-4
Functional Infrastructures · A-10

G

General Accounting Office · A-4, A-123, A-233, B-14, C-5, E-7
General Defense Intelligence Program · A-8, D-52
General Services Administration · 3-7, A-4, A-197, B-8, B-14, B-20, B-36, C-16, C-27, C-32, D-28, E-8
Global Combat Support System · A-74, E-7
Global Command and Control System · 4-9, E-7
Global Networked Information Exchange · E-7
Global Operations and Security Center · 3-11, 4-4, A-70, D-67, E-7
Government Computers · C-14, D-17
Government Emergency Telecommunications Service · B-20, E-7
Government Information Technology Services Board · A-98, D-23
Government Performance and Results Act · D-5, D-13, D-24, E-7

H

Hackers · 2-1, 3-2, 3-9, A-72, A-79, A-172, F-10, F-17
Headquarters, Marine Corps · A-47, E-8
High Assurance Guard · A-77
High Confidence Computing · A-66
High Confidence Networking · A-66
House Committee on Government Operations · A-112
House of Representatives · 3-4, 5-6, A-4, A-229, B-14, C-5, C-16
Human intelligence · E-8
Human Resources · A-11, A-15, B-44

I

IA Policy Working Group · A-11
IA Vulnerability Alerting · A-70
Incident Reporting Structure · 3-11, D-67, E-9
Industrial College of the Armed Forces · A-28
Information Assurance · 1-1, 1-2, 1-3, 1-4, 1-5, 2-1, 2-2, 2-7, 2-11, 3-1, 3-4, 3-7, 3-8, 3-11, 3-12, 4-3, 4-7, 4-12, 5-4, 5-5, 5-7, 5-8, A-3, A-7, A-8, A-9, A-10, A-11, A-12, A-15, A-19, A-21, A-23, A-24, A-27, A-31, A-37, A-41, A-47, A-48, A-51, A-53, A-54, A-57, A-65, A-66, A-67, A-69, A-70, A-71, A-73, A-76, A-79, A-80, A-87, A-93, A-95, A-97, A-101, A-107, A-111, A-113, A-117, A-121, A-129, A-130, A-133, A-137, A-138, A-141, A-142, A-145, A-149, A-159, A-163, A-165, A-169, A-177, A-181, A-185, A-189, A-197, A-198, A-203, A-211, A-217, A-221, A-225, A-226, A-229, A-230, A-231, A-233, B-7, B-8, B-9, B-13, B-19, B-25, B-29, B-30, B-35, B-39, B-43, B-47, D-3, D-47, D-49, D-58, D-60, D-62, D-68, E-5, E-8, F-8, F-11
Information Assurance Chief Executive Engineer · A-71
Information Assurance Engineering Support Organization · A-69, A-71
Information Assurance Group · A-3, A-11, A-19, E-8
Information Assurance Support Environment · A-73
Information Assurance Technology Analysis Center · A-3, A-79, E-8
Information Assurance Vulnerability Alert · 3-11, D-68, E-8
Information Infrastructure Group · B-30

Information Management · 4-8, 4-11, 4-12, A-7, A-98, A-123, A-124, A-125, A-138, A-149, A-151, A-165, A-166, A-193, A-217, A-233, C-20, C-31, D-9, D-11, D-14, D-15, D-51, D-61, E-4, E-13

Information Operations · 1-1, 3-1, 3-8, 3-10, 3-12, 5-1, 5-2, 5-5, 5-7, 5-8, A-7, A-9, A-11, A-12, A-15, A-21, A-22, A-23, A-27, A-31, A-32, A-35, A-37, A-41, A-45, A-47, A-48, A-51, A-52, A-53, A-54, A-57, A-58, A-61, A-65, A-70, A-72, A-75, A-76, A-79, A-80, A-83, A-84, A-87, A-93, A-95, A-97, A-101, A-111, A-129, A-133, A-137, A-141, A-159, A-165, A-169, A-175, A-185, A-189, A-193, A-203, A-217, A-221, B-19, B-25, B-29, B-35, B-43, D-8, D-9, D-47, D-62, D-65, D-66, D-68, E-8, E-13, F-8, F-11, F-14

Information Operations Conditions · 3-12, E-8

Information Operations Security Classification Guidance · A-9

Information Operations Technology Center · A-9, A-61

Information Protect Operations Decision Support System · A-62

Information Resources Management College · A-27

Information Sharing and Analysis Centers · 3-7, A-93

Information Strategies Concentration Program · A-27, A-28

Information Systems Concepts Division · A-59

Information Systems Directorate · A-57, A-59

Information Systems Security · 5-5, A-10, A-12, A-38, A-87, A-89, A-118, A-122, A-145, A-163, A-169, A-199, A-205, B-3, B-35, B-37, B-47, B-48, C-24, D-7, D-8, D-16, D-26, D-29, D-35, D-39, D-40, D-42, D-43, D-44, D-48, D-57, E-8, E-11, F-4, F-12

Information Technology · 1-2, 1-4, 3-4, 3-5, 3-7, 3-12, 3-14, 3-15, 4-8, 5-4, A-8, A-9, A-65, A-73, A-74, A-98, A-111, A-112, A-113, A-114, A-123, A-124, A-126, A-129, A-163, A-172, A-185, A-189, A-190, A-197, A-198, A-199, A-200, A-203, A-204, A-205, A-217, C-3, C-8, C-20, C-31, C-32, D-5, D-6, D-8, D-11, D-15, D-23, D-26, D-35, D-52, D-59, D-61, E-6, E-7, E-9, F-10, F-15

Information Technology Laboratory · A-111, A-112

Information Technology Management Reform Act · 3-14, 4-8, A-112, C-31, D-15, D-23, E-9

Information Technology Resources Board · D-23

Information Warfare · 3-1, 3-9, 4-4, 5-2, A-3, A-24, A-25, A-27, A-28, A-32, A-35, A-37, A-38, A-41, A-42, A-45, A-51, A-52, A-53, A-57, A-60, A-61, A-70, A-79, A-80, A-83, A-84, A-175, A-198, B-7, B-9, D-8, D-9, D-47, D-48, D-49, D-62, D-63, D-68, E-3, E-4, E-7, E-9, E-11, F-8, F-12

Information Warfare Support Division · A-60

Information Warfare Team · A-175

Information Warfare/Command and Control Warfare Division · A-38

INFOSEC Program Management Office · A-69, E-9

Infrastructure Management Division · A-57, A-59

Infrastructure Protection Task Force · C-29, C-30, D-22, D-23, E-9

Inspector General · A-75, A-159, A-171, A-194, B-15

Institute of Telecommunications Sciences at Boulder, CO · A-118

Integrated Product Team · A-11, E-9

Integration and Standards Division · A-58

Integrity · 2-3, 2-8, 2-14, 3-10, 3-12, 4-2, 4-3, 4-11, A-80, A-186, A-190, A-198, A-204, C-7, C-28, C-37, D-14, D-16, D-21, D-32, D-35, D-40, D-41, D-44, D-53, D-59, D-61, D-70, E-3, F-3, F-6, F-11, F-12, F-18

Intelligence Application and Production Division · A-60

Intentional Damage · C-14, D-17

Interdepartment Radio Advisory Committee · A-118

Internal Revenue Service · 2-11, A-171, B-15

International Monetary Fund · A-169

International Trade Administration · A-108, A-118

Internet · 1-1, 1-3, 2-1, 2-2, 2-7, 2-9, 2-10, 2-12, 3-9, 3-14, 3-17, 4-3, A-72, A-73, A-75, A-109, A-112, A-113, A-114, A-125, A-186, A-194, A-212, A-221, A-222, B-21, B-31, B-32, C-5, C-9, C-31, C-32, C-33, C-35, C-36, C-38, E-8, E-9, E-11, E-13, F-10, F-13, F-14, F-19

Internet Protocol Router · 4-3, A-73, A-75, E-9

Internet Protocol Security · A-113, E-9

Intrusion Detection Devices · 4-4

Intrusion Detection Tools · 1-4, A-76, A-80, A-81

J

J-2 · 3-10, A-21, A-23, D-65, D-68
 J-3 · 3-10, A-22, A-23, D-65, D-66, D-68

J-6 · 3-10, A-22, A-24, D-65, D-68
Joint DII Control Systems · A-70, E-9
Joint Doctrine for Information Operations · 3-1,
3-8, A-23, D-9, D-68
Joint IA Tools Working Group · A-11
Joint Interoperability Engineering Organization ·
A-74, E-9
Joint Intrusion Detection · E-9
Joint Publication 3-13 · A-23
Joint Security Commission · A-11, B-47
Joint Staff · 3-1, 3-8, 3-11, 3-12, 4-7, 4-8, 5-2, 5-4,
5-5, A-3, A-9, A-21, A-22, A-23, A-24, A-31,
A-74, A-80, A-88, B-20, D-3, D-60, D-61, D-65,
D-66, D-67, D-68, E-12
Joint Task Force-Computer Network Defense ·
E-9
Joint Technical Architecture · 4-10, E-9
Joint Vision 2010 · 3-17, 4-1, 4-8, 4-12, A-76, D-68,
E-9
Joint Warrior Interoperability Demonstration ·
1-4, A-74, E-10
Joint Web Risk Assessment Cell · 5-7
JTF Organization · 5-3
Justice Management Division · A-149

L

Lawrence Livermore National Laboratory · A-3,
A-122, A-125, A-129
Library Services Division · A-59
Local Area Network · 4-4, 5-8, A-138, A-205,
E-10, F-13
Local Emergency Planning Committees · A-177
Local Registration Authority · A-77
Logic Bombs · A-75
Logistics Division · A-59
Los Alamos National Laboratory · A-3, A-122,
A-133
Loudoun v. Board of Trustees of Loudoun
County Library · 2-10

M

Major Automated Information System Review
Council · A-8, D-52, E-10
Major Commands · A-31, A-53, A-54, A-62
Management Reform Memorandum (MRM) #16
· 4-7
Manager of the National Communications
System · 3-7, D-28
Mandatory Access Control · A-114, F-9, F-13

Manufacturing Extension Partnership · A-112
Marine Corps Combat Development Command
· A-48
Marine Corps Reserve · 5-7
Measurement and Standards Laboratories ·
A-112
Military Communications Electronics Board ·
3-12
Mission Critical · 4-2, 4-7, 4-12, 5-3
Mission Support Directorate · A-59
Mission Support Programs Division · A-59
Mobile Agent Security · A-113
Multilevel Security Working Group · A-11, E-10
Multiple Security Level · A-71, A-77, F-14
Multiple Security Levels · A-77

N

NASA Automated Systems Incident Response
Capability · A-205
National Aeronautic and Space Administration ·
2-8
National Aeronautics and Space Administration
· A-4, A-203, B-20, B-26, E-10
National Command Authority · A-22, E-10
National Communications System · 3-7, A-103,
A-104, B-3, B-7, B-19, B-31, B-36, C-10, C-11,
C-21, C-25, C-26, D-19, D-20, D-26, D-28,
D-51, D-52, E-10, E-12
National Defense Authorization Act · C-3, C-10,
D-5, D-15, D-16
National Defense University · A-27, A-28, E-11
National Disaster Medical System · A-145
National Economic Council · A-3, A-93, A-95,
B-6
National IA Structure · 3-6, D-27
National Imagery and Mapping Agency · A-8,
B-37, E-11
National Industrial Security Program · D-62,
E-11
National Information Infrastructure · 3-18,
A-103, C-6, D-5, D-15, E-11, F-10, F-14
National Infrastructure Assurance Council · 3-7,
B-5, D-28, E-11
National Infrastructure Protection Act · D-16
National Infrastructure Protection Center · 3-5,
3-7, 3-11, 5-6, A-3, A-31, A-155, B-6, B-22,
B-32, D-28, D-67
National Institute for Standards and Technology
· 3-3, A-108, A-199
National Intelligence Council · A-4, A-207, E-11
National Intelligence Estimates · A-208

National Intelligence Officers · A-207
National Oceanic and Atmospheric Administration · A-108
National Research Council · A-4, A-211
National Science and Technology Council · A-101, A-104, B-3, B-10, B-25, B-43, E-11
National Security Advisor · 3-6, 3-16, A-103, D-27
National Security Agency · 3-3, 3-8, 5-5, A-3, A-8, A-87, A-112, A-113, A-138, A-199, B-14, B-20, B-35, B-36, C-16, C-17, C-23, C-29, D-12, D-19, D-21, D-26, D-37, D-49, D-51, D-60, D-66, E-6, E-11
National Security and International Affairs Division · A-102, A-103, A-233
National Security Council · 3-4, A-3, A-95, A-104, A-159, B-7, B-19, C-23, C-24, C-26, D-20, D-21, D-50
National Security Incident Response Center · A-89, D-40, E-11
National Security Information · C-3, C-14, C-24, C-27, C-31, D-5, D-20, D-40, F-5
National Security Operations Center · 3-11, D-67, E-11
National Security Policy · 4-12
National Security Telecommunications Advisory Committee · A-103, A-104, B-3, B-19, B-29, B-32, C-25, D-20, E-11
National Technical Information Service · A-108, B-13
National Telecommunications and Information Administration · A-3, A-108, A-117, B-20, E-11
National War College · A-28
National Warning System · A-186
NATO Command Control Consultation Board · 1-4
Naval Computer Incident Response Team · E-10
Naval Criminal Investigative Service · 2-8, E-10
Naval Doctrine Command · A-38
Naval Information Warfare Activity · A-3, A-38, A-42, A-45, E-11
Naval Reserve · 5-7
Near-Real-Time · A-23, A-62, A-87, E-11
Network Intrusion Detection · A-130
Network Intrusion Device Monitoring · A-42
Network Management Information Center · A-124
Network Operating Centers · A-42, E-11
Network Operation Security Center · A-53, E-11
Network Reliability · A-181, A-183, B-3, B-39, E-11
Network Reliability and Interoperability Council · A-181, B-3, B-39, E-11

Next Generation Information Infrastructure · A-66, A-67
Next Generation Internet · A-109
No Electronic Theft Act · 2-2, 2-5, 2-7
Non-Repudiation · 4-2, 4-5, 4-6, 4-7, 4-11, A-80, D-43, D-59, F-11
North Atlantic Treaty Organization · D-52, E-10
NSD 42 · B-35, D-5, D-25, D-29, D-36, D-39, D-40

O

Oak Ridge National Laboratory · A-3, A-122, A-137, E-12
Offensive Counter Information · E-12
Office of Architecture, Standards, and Information Security · A-123
Office of Critical Infrastructure Protection · A-10, A-12, A-121
Office of Information and Privacy · A-149
Office of Information and Technology Management · A-193
Office of Information Management · A-165, A-166
Office of Information Security Technology · A-161
Office of Information Technology Integration · A-197
Office of Information, Records, and Resource Management · A-123
Office of Intelligence Policy and Review · A-150
Office of Management and Budget · 2-15, 3-14, A-3, A-73, A-97, A-112, A-199, B-7, B-9, B-19, B-26, B-36, C-16, C-17, C-20, C-21, C-22, C-26, C-28, C-29, D-6, D-11, D-20, D-22, D-26, D-30, D-31, D-32, D-33, E-12
Office of Naval Intelligence · A-38
Office of Non Proliferation and National Security · A-121
Office of Operations, Engineering, and Customer Service · A-124
Office of Planning, Policy, and Mission Analysis · A-123
Office of Safeguards and Security · A-121, A-122, A-125, A-141
Office of Science and Technology Policy · A-3, A-101, B-19, B-25, B-31, B-43, C-26, D-20
Office of Special Investigation · 2-8, A-52, A-150, C-11, E-3
Office of Spectrum Management · A-117, A-118
Office of the Comptroller of the Currency · A-171, B-15

Office of the Secretary of Defense · A-21, A-31,
D-9, D-26, D-62, E-12
Office of Thrift Supervision · A-171, B-15
Omega Engineering Corporation · 2-11
Omnibus Diplomatic Security · A-159
On-Line Survey · A-43, A-58, A-61
Open Network Architecture · A-182
Operation Solar Sunrise · 5-2, 5-9, 5-10
Operational Architecture · 4-9, 4-10, A-10
Operational Impact · A-39, A-70
Operational Locations · 3-10, D-67
Operational Monitoring · A-11
Operational Policy · A-11
Operational Readiness · 3-8, 3-18, A-12, A-16,
A-87
Operations Support Directorate · A-57, A-59
Overarching Integrated Project Team · 4-12

P

Pacific Northwest National Laboratory · A-3,
A-122, A-141
Paperwork Reduction Acts · D-13
Password Trafficking · C-14
PD/NSC 24 · D-5, D-25
PDD 39 · D-5, D-26
PDD 62 · 3-5, D-5, D-27
PDD/NSC 29 · D-5, D-25
Penetration Testing · A-80, A-112, A-138, A-171,
F-15
Policy · 1-1, 1-2, 1-4, 1-5, 2-7, 2-9, 2-10, 2-12, 2-13,
2-14, 2-15, 3-1, 3-2, 3-5, 3-6, 3-8, 3-9, 3-10, 3-12,
3-13, 3-14, 3-15, 3-16, 3-17, 4-12, 5-1, 5-4, 5-7,
A-3, A-7, A-9, A-11, A-12, A-15, A-19, A-21,
A-22, A-23, A-24, A-31, A-32, A-37, A-47,
A-52, A-53, A-67, A-69, A-70, A-72, A-73,
A-77, A-93, A-95, A-97, A-98, A-101, A-102,
A-103, A-104, A-107, A-108, A-113, A-117,
A-118, A-122, A-123, A-124, A-125, A-149,
A-150, A-151, A-159, A-160, A-161, A-163,
A-166, A-169, A-170, A-171, A-172, A-178,
A-185, A-189, A-190, A-193, A-197, A-199,
A-200, A-203, A-204, A-205, A-211, A-213,
A-217, B-3, B-6, B-7, B-14, B-19, B-20, B-22,
B-25, B-26, B-29, B-31, B-35, B-36, B-37, B-43,
B-44, B-47, B-48, C-10, C-20, C-21, C-22, C-23,
C-24, C-25, C-26, C-27, C-28, C-30, C-35, D-3,
D-5, D-6, D-7, D-8, D-9, D-13, D-14, D-15,
D-16, D-20, D-21, D-22, D-25, D-26, D-27,
D-29, D-30, D-32, D-33, D-35, D-36, D-37,
D-38, D-39, D-40, D-41, D-42, D-44, D-45,
D-47, D-48, D-50, D-51, D-52, D-53, D-54,

D-55, D-56, D-57, D-59, D-60, D-61, D-62,
D-63, D-65, D-66, D-69, E-3, E-8, E-12, E-13,
E-14, F-3, F-4, F-17, F-18
Presidential Decision Directive (PDD) 63 · B-5
Privacy Act · 2-10, A-98, A-149, A-225, A-230,
C-3, C-17, C-20, D-5, D-11, D-12, D-55, E-6,
F-17
Probabilistic Risk Assessments · 3-3
Program and Development Team · 5-4
Program Objective Memorandums · 3-5, 3-8
Protect · 1-3, 2-10, 3-3, 3-5, 3-10, 3-13, 3-17, 4-1,
4-2, 4-3, 4-4, 4-12, 5-2, 5-3, 5-6, 5-10, A-12,
A-23, A-32, A-38, A-41, A-42, A-48, A-57,
A-60, A-62, A-69, A-71, A-72, A-75, A-89,
A-104, A-113, A-122, A-142, A-186, A-198, B-8,
C-11, C-15, C-20, C-23, C-30, D-11, D-17, D-19,
D-22, D-25, D-35, D-36, D-53, D-54, D-62,
D-63, D-66, F-3, F-4, F-8, F-11, F-18
Protected Computer · 2-2, C-7, D-17
Protected Enclave · 4-4
Protection · 1-1, 1-2, 1-3, 1-5, 2-3, 2-12, 2-14, 3-1,
3-2, 3-3, 3-5, 3-6, 3-7, 3-11, 3-12, 3-13, 3-18, 4-2,
5-1, 5-5, 5-6, 5-8, A-3, A-4, A-7, A-8, A-9, A-10,
A-12, A-15, A-19, A-31, A-32, A-35, A-39,
A-41, A-47, A-51, A-52, A-53, A-54, A-62,
A-65, A-71, A-72, A-79, A-80, A-83, A-87,
A-88, A-93, A-95, A-97, A-98, A-101, A-102,
A-103, A-104, A-107, A-109, A-111, A-112,
A-113, A-114, A-117, A-118, A-121, A-122,
A-129, A-133, A-137, A-138, A-141, A-145,
A-149, A-151, A-155, A-156, A-160, A-163,
A-165, A-169, A-170, A-175, A-177, A-193,
A-197, A-198, A-203, A-204, A-205, A-217,
A-221, A-226, A-230, A-233, B-5, B-6, B-7, B-9,
B-10, B-14, B-19, B-22, B-25, B-26, B-29, B-30,
B-31, B-32, B-43, B-47, B-48, C-3, C-6, C-7,
C-11, C-20, C-23, C-26, C-28, C-29, C-30, D-5,
D-6, D-7, D-9, D-13, D-15, D-16, D-20, D-21,
D-22, D-23, D-25, D-27, D-28, D-29, D-33,
D-35, D-36, D-37, D-38, D-39, D-42, D-45,
D-48, D-53, D-54, D-55, D-57, D-58, D-62,
D-64, D-66, D-67, D-69, E-4, E-6, E-7, E-9, E-12,
F-4, F-5, F-7, F-8, F-9, F-11, F-12, F-18
Public Key Encryption · 4-2, 4-6, 4-9, 4-11, E-12,
F-15
Public Key Infrastructure · 4-1, 4-7, 4-11, 4-12,
A-25, A-73, A-76, A-80, A-114, A-199, F-4,
F-15
Public Switched Network · E-12, F-15

Q

Quadrennial Defense Review · 3-5, 4-11, E-12

R

React · 3-13, 3-17, A-12, A-48, A-71, A-198, D-53
Readiness · 3-8, 3-12, 3-18, 5-4, A-10, A-11, A-12,
A-15, A-16, A-22, A-24, A-32, A-51, A-70,
A-75, A-87, A-88, A-118, A-160, B-20, B-32,
B-40, C-22, D-15, D-52, D-62, D-63, D-64, F-12,
F-16

Real-time Intrusion Detection and Response ·
A-130

Red Team · 1-2, A-12, A-24, A-67, A-80, D-66

Regional Computer Emergency Response Teams
· A-72, E-12

Reliability · 4-2, A-111, A-122, A-124, A-181,
A-182, A-183, B-3, B-21, B-39, B-40, D-44, E-11,
F-6, F-7, F-12, F-16

Reprogramming Division · A-60

Research and Technology · A-11, A-15, A-122

Response · 1-1, 1-2, 1-3, 2-5, 2-7, 3-5, 3-11, 3-13,
4-3, 5-4, 5-6, A-15, A-22, A-35, A-38, A-42,
A-48, A-52, A-58, A-61, A-62, A-67, A-72,
A-75, A-87, A-89, A-98, A-104, A-113, A-129,
A-130, A-134, A-145, A-146, A-151, A-160,
A-177, A-178, A-185, A-186, A-197, A-199,
A-205, B-6, B-20, B-21, B-30, B-48, D-7, D-16,
D-26, D-33, D-40, D-54, D-66, D-67, D-68, E-4,
E-5, E-7, E-9, E-11, F-4, F-16

Risk Analysis · A-74, A-98, A-102, A-198, D-62,
F-16

Risk Assessment · 1-4, 3-3, 5-7, A-138, A-205,
A-218, B-9, B-30, F-16

Role Based Access Control · A-114

S

School of Information Warfare and Strategy ·
A-3, A-27

Scientific and Technical Information · A-79

Secret and Below Interoperability · 3-12, A-11,
A-73, A-77, E-13

Secret and Below Interoperability Working
Group · A-11, E-13

Secret Internet Protocol Routing Network · E-13

Secure Electronic Transactions · 2-13, 4-10

Secure Protocols · 4-2, 4-3

Secure Sockets Layer · 4-9, 4-11

Secured Operating Systems · 4-5

Security and Information Operations · 5-1, A-11
Security and Investigative Activities Program ·
A-8, D-52

Security Countermeasures · A-7, D-51

Security Management · A-11, A-15, A-67, A-70,
A-76, A-130, A-203, A-204, A-234, B-8, D-44,
F-17

Security Management Tools · A-70

Security Metrics · 5-5

Security Policies · 1-4, A-21, A-52, A-80, B-48,
C-36, C-37, D-26, D-45, D-56, D-58, F-17

Security Readiness Reviews · A-70

Security Technical Implementation Guides ·
A-76, E-13

Security Test and Evaluation · A-77, A-80, F-17

Senior IO Review Committee · A-32

Sensitive Information · 5-7, A-67, A-112, A-122,
A-151, A-183, B-33, C-15, C-16, C-17, D-6,
D-12, D-13, D-30, D-45, D-55, F-17

Sensitive-But-Unclassified · E-13

Situation Awareness/Response · 4-3

Situational Awareness · A-72, A-75

Sniffers · F-17

Space and Naval Warfare Systems Command ·
A-38

State Emergency Response Commissions · A-177

Statistical Process Control · A-61

Strategic Information Management · A-123

Switched Network · A-181, A-186, B-20, E-12,
F-8, F-14, F-15

Symmetric · 4-6

Systems Analysis Directorate · A-60

Systems Architecture · 4-9, 4-10, A-66

T

Tactics, Techniques, and Procedures · A-42,
A-83, D-65, E-9

Technical Architecture · 4-8, 4-9, 4-10, 4-12, E-9,
E-13, F-18

Technical Threat Analysis · A-38, A-45

Technology Administration · A-108

Telecommunications Act · A-182, B-21, B-31,
B-39, C-3, C-8, C-9, D-5, D-11, D-14

Telecommunications and Information
Infrastructure Assistance Program · A-117

Telecommunications Electric Service Priority ·
B-22

Telecommunications Service Priority · B-22

Theater Deployable Communications · A-54

Threats · 1-1, 3-1, 3-2, 3-4, 3-5, 3-13, 4-1, 5-5, 5-6,
5-7, A-24, A-32, A-39, A-52, A-89, A-95, A-103,

A-113, A-134, A-142, A-150, A-152, A-155,
A-156, A-207, A-209, B-6, B-33, B-48, C-23,
C-30, D-17, D-19, D-22, D-23, D-25, D-27,
D-29, D-54, D-57, D-62, D-65, F-4, F-12, F-16
Top Secret · A-137, C-27, C-31, D-8, D-47
Traditional Security · A-73, A-76
Training, Administration, and Outreach Section
· A-155
Transnational Warfare Group · 5-2, A-83
Transportation Administrative Service Center ·
A-163
Trojan Horse software · A-75
Trustworthiness · 4-2, A-211, A-212, A-213,
A-214, C-36, C-37
Trustworthy Systems · A-213, F-18

U

U.S. and Foreign Commercial Service · A-108
U.S. Department of Commerce Bureau of Export
Administration · C-33
U.S. Department of Health and Human Services,
Office of Emergency Preparedness · A-145
U.S. Navy · 2-10, 2-11
U.S. Secret Service · 2-3, B-15
U.S. Security Policy Board · B-47
U.S. v. Hilton · 2-10
U.S. v. LaMacchia · 2-5, 2-7
U.S. v. Machado · 2-9
Under Secretary of Defense · 3-13, A-9, A-12,
D-8, D-9, D-50, D-54, E-12
Uniform Code of Military Justice · C-3, C-11,
D-12, E-13
Unintentional Damage · C-14
United States Coast Guard · A-3, A-165
United States Customs Service · A-170

United States Information Agency · A-4, A-221,
B-20
United States Marine Corps · A-3, A-47, B-36
United States Secret Service · A-170, E-14
Urofsky v. Allen · 2-10
US Security Policy · A-11

V

Verifiability · 4-2, F-18
Violent Crime Control and Law Enforcement
Act · C-3, C-13
Virus · 3-12, A-62, A-70, A-80, A-156, A-194,
F-13, F-19
Virus Detection and Eradication · A-70
Vulnerability Analysis · A-42, A-60, A-72, A-74,
A-80, A-81, A-138, F-19
Vulnerability Analysis Division · A-60
Vulnerability and Assessment Program · E-14
Vulnerability Assessment · 1-2, 3-12, 3-13, A-24,
A-74, A-75, A-80, A-88, B-8, B-9, D-53, E-14,
F-19
Vulnerability Assessment Software · A-75
Vulnerability Awareness · B-8
Vulnerability Compliance and Tracking System ·
A-72

W

Wide Area Network · 4-3, A-124, E-14, F-19
Wiretaps · A-151, C-12, C-15, F-19

Y

Year 2000 · A-163, A-234, B-32, B-39, B-40, C-32,
E-14

This page intentionally left blank.