BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 10-24

1 DECEMBER 1999

Operations

AIR FORCE CRITICAL INFRASTRUCTURE PROTECTION

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ USAF/SC (Lt Col David Warner)

Certified by: AF-CIO (Dr Lawrence Delaney)
Pages: 11
Distribution: F

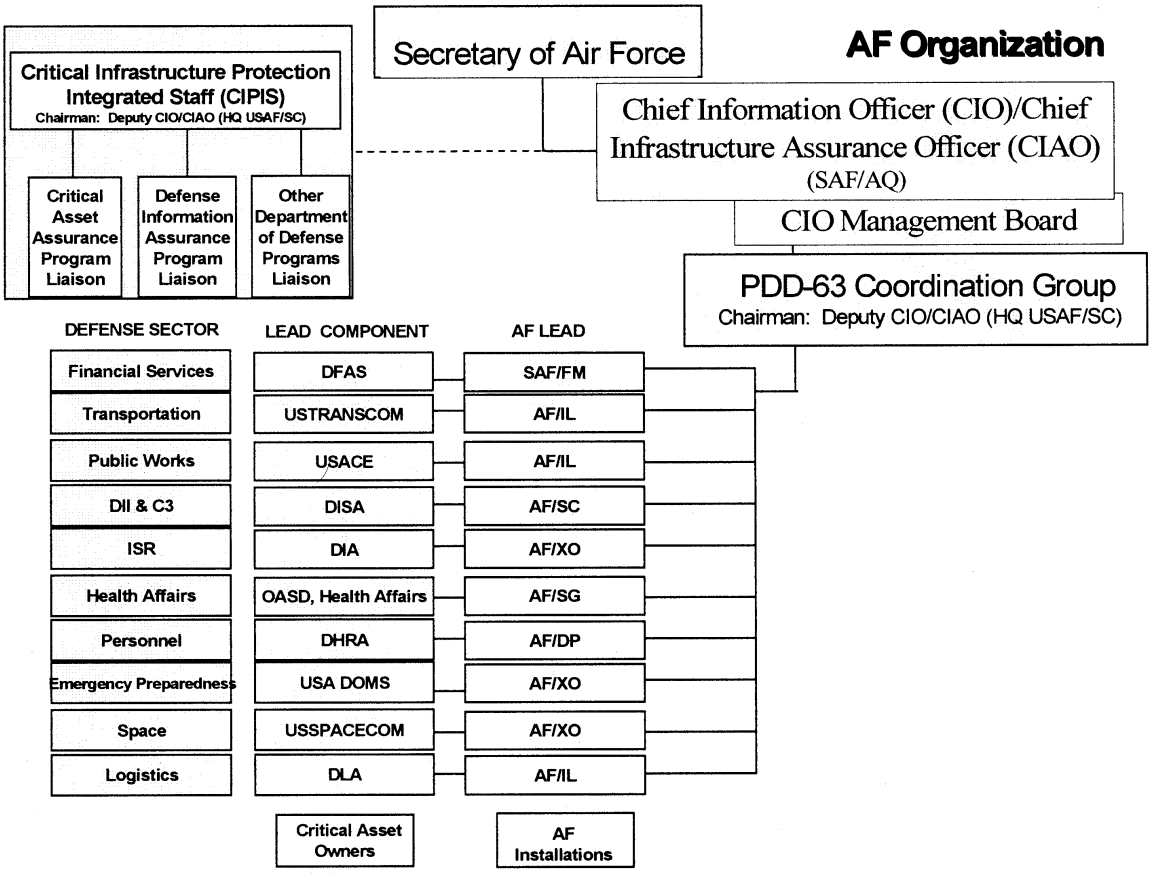
This directive establishes the Air Force Critical Infrastructure Protection Program (CIPP) policy. The program implements Department of Defense (DoD) Directive 5160.54, *Critical Asset Assurance Program (CAAP)*, January 20, 1998 and The Department of Defense *Critical Infrastructure Protection Plan (CIPP)*, November 18, 1998. These documents implement Presidential Decision Directive (PDD)/ National Security Council (NSC)-63, *Critical Infrastructure Protection*, May 22, 1998.

1. Military operations today are heavily dependent on globally (US and foreign, government and civilian) shared critical infrastructures (physical and cyber). Technological advances have interconnected these infrastructures, better enabling mission accomplishment anywhere in the world. While this connectivity better enables mission accomplishment, it also increases our vulnerability to human error, natural disasters, and physical or cyber attacks. For this reason, it is necessary to identify and protect mission-critical infrastructures. An infrastructure is critical when its damage or destruction would weaken national defense or economic security. Critical infrastructures include those physical assets and cyber systems essential to the minimum operations of the economy and government. This directive provides policy to protect Air Force critical infrastructures and to ensure a partnership with other government and civil agencies to protect critical national assets.

2. Presidential Decision Directive /National Security Council-63 (PDD/NSC-63) describes the tasks and goals, and their associated timelines for protecting our critical national infrastructures from physical and technical attacks and requires every department and agency to be responsible for and protect their own critical infrastructures. **Infrastructure assurance** and **information assurance** are PDD/NSC-63's key components. To protect these components every department or agency is required to appoint a Chief Information Office (CIO) with responsibility for Information Assurance and a Chief Infrastructure Assurance Officer (CIAO) with responsibility for all other aspects of protecting that department's critical infrastructure. The CIO may be appointed to fill both roles. Additionally, PDD/NSC-63 identifies critical infrastructures and appoints sector leads to: assess vulnerabilities of the sector to cyber or physical attack; to recommend a plan to eliminate the vulnerabilities; to propose a system to prevent attacks; and to develop a plan to alert, contain, and rebuff an attack in progress. The DoD-appointed sector leads will work in conjunction with the national Critical Infrastructure Protection (CIP) structure. USAF sector

leads are identified in figure 1 and described below. The Air Force sector leads will work with the DoD sector leads, and are responsible to the AF-CIO for PDD/NSC-63 implementation.

Figure 1. DoD, Lead Component, and Air Force Sector Leads.



3. The DoD Critical Infrastructure Protection Plan (CIPP) provides DoD implementation direction for PDD/NSC-63. The DoD approach to ensuring critical infrastructure protection incorporates six life-cycle phases. They are: Analysis and Assessment; Remediation; Indications and Warning; Response; Mitigation; and Reconstitution. The DoD will use the Critical Asset Assurance Program (CAAP) and the Defense-wide Information Assurance Program (DIAP) to implement CIP. The CAAP goal is to provide infrastructure assurance. The DIAP goal is to provide information assurance. The Air Force will support these life-cycle phases and programs and place particular emphasis on them as they relate to Air Expeditionary Forces (AEF) deployment. Critical physical infrastructure assets include physical facilities, equipment, and personnel, and critical cyber infrastructure assets may include information systems or command and control networks.

4. The Air Force will evaluate and use existing DoD and Air Force doctrine, plans, policies, instructions, and memoranda of agreement (MOA) as the basis for integrating PDD/NSC-63 tasks. Documents, which should reflect CIP implementation, are at attachment 1. Air Force sector leads will evaluate their functional documents to determine whether they adequately address CIP responsibilities and appropriately

update them. The evaluation will identify risks and vulnerabilities to the Air Force created by our reliance on other Service, government, or civil sector infrastructures (e.g., oil and gas pipelines or electricity). The evaluation should also identify tools to reduce the risks and vulnerabilities.

5. The following responsibilities and authorities are established:

5.1. The Air Force Chief Information Officer (AF-CIO) also serves as the Air Force Chief Infrastructure Assurance Officer (AF-CIAO) and is responsible for the Air Force's CIP implementation. In this capacity, AF-CIO, in conjunction with the CAAP, DIAP, and Air Force sector leads will:

5.1.1. Identify critical Air Force assets and infrastructure, with particular emphasis on assets supporting AEF deployment capabilities.

5.1.2. Determine potential impact to Air Force missions and operations resulting from degradation, loss, or compromise of critical assets and/or infrastructures.

5.1.3. Receive and approve functional area annual reports regarding Air Force PDD/NSC-63 and DoD CIPP implementation and report that status to the DoD-CIAO. Air Force sector leads will provide the annual report to the AF-CIAO by 1 Mar of each year.

5.2. The Assistant Secretary of the Air Force, Acquisition (SAF/AQ), who serves as the CIO and CIAO, is responsible for Air Force acquisition policy and procedures and will implement CIP initiatives during system acquisition. In this capacity, SAF/AQ will:

5.2.1. Establish policies and procedures to address assurance (both **infrastructure** and **information assurance**) and protection of critical systems and infrastructures during acquisition. Special consideration should be given to identifying vulnerabilities resulting from our reliance on other Service, government, or civil sector infrastructures (e.g., oil and gas pipelines or electricity) and the risk of their loss, damage or destruction to the Air Force mission. The goal is to reduce risks imposed by those vulnerabilities during system acquisition.

5.2.2. Adopt prudent business and operational planning practices to reduce the potential impact from loss or compromise of infrastructure services.

5.2.3. Establish policies and procedures to protect Air Force laboratories.

5.2.4. Develop a report on the acquisition community's implementation of PDD/NSC-63 and DoD CIPP by 1 Mar. This will be included in the annual report to the DoD-CIAO.

5.3. The Headquarters United States Air Force Director, Communications and Information (HQ USAF/SC) is responsible for **information assurance**. Additionally, HQ USAF/SC, as the deputy AF-CIO, serves as the Deputy CIAO. HQ USAF/SC is also the Air Force member to the DIAP Senior Steering Group and is the Air Force lead for the Defense Information Infrastructure (DII) and Command, Control, and Communications (C3) Defense Sector. In this capacity, HQ USAF/SC will:

5.3.1. Establish policies and procedures to guarantee the availability, integrity, non-repudiation, confidentiality, and authentication of all Air Force information and information systems.

5.3.2. Establish specific standards, network architectures, training, and certification requirements for network operators, managers, administrators, and users; prescribe procedures for information systems certification and accreditation.

5.3.3. Establish policy and procedures to protect Air Force-wide information systems and command, control, communications, computers, and intelligence (C4I) interfaces to weapon systems.

5.3.4. Establish policy and procedures to protect software applications and data engineering tools, methods, and processes to build and maintain command, control, intelligence, surveillance, and reconnaissance (C2ISR) systems.

5.3.5. Establish policy and procedures to ensure DII and Common Operating Environment (COE) compliance that facilitates interconnection and interoperability among networks.

5.3.6. Establish policy and procedures that enable the Air Force to marshal and coordinate the communications networks and systems in response to emergencies and hostilities. Special consideration should be given to identifying vulnerabilities resulting from our reliance on other Service, government, or civil communications networks and systems, and the risk of their loss, damage, or destruction to the Air Force mission with the goal of reducing risk.

5.3.7. Using the authority delegated by the Air Force Chief of Staff, invoke national security emergency preparedness telecommunications procedures when operational needs or emergency conditions require extraordinary response from the Defense Information Systems Agency and the telecommunications private sector.

5.3.8. Provide the AF-CIAO an annual report by 1 Mar of each year regarding HQ USAF/SC's implementation of PDD/NSC-63 and DoD CIPP.

5.4. The HQ USAF Deputy Chief of Staff, Installations and Logistics (HQ USAF/IL) has overall responsibility for **infrastructure assurance**. HQ USAF/IL is responsible for the Air Force CAAP and is the Air Force lead for the logistics, transportation, and public works defense sectors. Special consideration should be given to identifying vulnerabilities resulting from our reliance on other Service, government, or civil sector infrastructures (e.g., electricity, power, oil, natural gas, water, sewer, and emergency services) and the risk of their loss, damage or destruction to the Air Force mission. The goal is to reduce impacts imposed by those vulnerabilities. In this capacity, HQ USAF/IL will:

5.4.1. Establish policy and procedures to protect Air Force logistics activities, facilities, assets, infrastructures, and systems that support supply and services provisioning Air Force-wide. Logistics activities include material acquisition and development, storage, and distribution of supplies; maintenance of material and supplies; and final disposition of no longer needed materials.

5.4.2. Establish policy and procedures to protect Air Force transportation assets and facilities.

5.4.3. Establish policy and procedures to protect the Air Force infrastructure that makes up the public works defense sector (electric, power, oil and natural gas, water and sewer, and emergency services [fire, hazardous material handling, and aircraft recovery]), and the sector's distribution capability.

5.4.4. Provide the AF-CIAO an annual report by 1 Mar of each year regarding HQ USAF/IL's implementation of PDD/NSC-63 and DoD CIPP.

5.5. The HQ USAF Deputy Chief of Staff, Operations (HQ USAF/XO) is the Air Force lead for the emergency preparedness; space; and intelligence, surveillance, and reconnaissance (ISR) defense sectors. Additionally, HQ USAF/XO is responsible for integrating AF information operations and information warfare programs, including defensive counterinformation (DCI) across the spectrum of military operations. Special consideration should be given to identify vulnerabilities from our reli-

ance on other Service, government, or civil sector infrastructures (e.g., electricity and air traffic control), and the impact of their loss, damage or destruction to the Air Force mission. The goal is to reduce risks imposed by those vulnerabilities. In this capacity, HQ USAF/XO will:

5.5.1. Through Air Force Space Command (AFSPC), ensure the protection of Air Force space assets including launch (Eastern and Western launch ranges) and control systems.

5.5.2. Establish policy and procedures to protect Air Force assets and infrastructure supporting the development, production, and conduct of ISR activities, including intelligence production and fusion centers. Air Force ISR CIP efforts will be coordinated with national Intelligence Community CIO CIP efforts.

5.5.3. Establish policy and procedures to marshal and coordinate assets, facilities, capabilities, and systems needed to respond to hostilities and emergencies (including natural disasters and civil and domestic emergencies), in conjunction with other government and civil sectors.

5.5.4. Integrate DCI programs (e.g., Operational Security (OPSEC), Counter-intelligence, Electronic Protection) with CIP efforts; ensure Computer Network Defense (CND) capabilities support CIP efforts.

5.5.5. Ensure that requirements' documentation (Mission Needs Statement and Operational Requirements Documents) includes asset and infrastructure protection requirements.

5.5.6. Ensure force and facility protection.

5.5.7. Provide the AF-CIAO an annual report by 1 Mar of each year regarding HQ USAF/XO's implementation of PDD/NSC-63 and DoD CIPP.

5.6. The HQ USAF Deputy Chief of Staff, Personnel (HQ USAF/DP) is the Air Force lead for the personnel defense sector. Special consideration should be given to identify vulnerabilities resulting from our reliance on other Service, government, or civil sector infrastructures and the risk of their loss, damage, or destruction to the Air Force mission. The goal is to reduce risks imposed by those vulnerabilities. In this capacity, HQ USAF/DP will:

5.6.1. Establish policy and procedures to protect Air Force assets and systems supporting Air Force personnel.

5.6.2. Provide the AF-CIAO an annual report by 1 Mar of each year regarding HQ USAF/DP's implementation of PDD/NSC-63 and DoD CIPP.

5.7. The Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM) is the Air Force lead for the financial services defense sector. Special consideration should be given to identify vulnerabilities resulting from our reliance on other Service, government, or civil sector infrastructures (e.g., banks) and the risk of their loss, damage, or destruction to the Air Force mission. The goal is to reduce risks imposed by those vulnerabilities. In this capacity, SAF/FM will:

5.7.1. Establish policy and procedures to protect Air Force disbursing and pay operations.

5.7.2. Ensure the protection of Air Force financial servicing institutions.

5.7.3. Provide the AF-CIAO an annual report by 1 Mar of each year regarding SAF/FM's implementation of PDD/NSC-63 and DoD CIPP.

5.8. The Assistant Secretary of the Air Force for Manpower, Reserve Affairs, Installations, and Environment (SAF/MI) is responsible for civilian personnel, installations, health care, and facility policy

matters and provides policy oversight as prescribed in Air Force Policy Directive (AFPD) 90-1, Strategic Planning and Policy Formulation.

5.9. The HQ USAF Directorate of Test and Evaluation (HQ USAF/TE) will:

5.9.1. Establish policy and procedures to protect Air Force test and evaluation infrastructure, including test ranges with the exception of the Eastern and Western launch ranges.

5.9.2. Establish policy and procedures to protect physical and cyber data reduction, data analysis, and data communication systems used to support development and testing of new weapons technology and testing of existing legacy systems at our test ranges.

5.9.3. Provide the AF-CIAO an annual report by 1 Mar of each year regarding AF/TE's implementation of PDD/NSC-63 and DoD CIPP.

5.10. The Surgeon General of the Air Force (HQ USAF/SG) is the Air Force lead for the health affairs defense sector. Special consideration should be given to identify vulnerabilities resulting from our reliance on other Service, government, or civil sector infrastructures (e.g., hospitals) and the risk of their loss, damage or destruction to the Air Force mission. The goal is to reduce risks imposed by those vulnerabilities. In this capacity, SG will:

5.10.1. Establish policy and procedures to protect the Air Force's health care infrastructure, including information systems linking civil and other government facilities and health care networks to the Services and components.

5.10.2. Provide the AF-CIAO an annual report by 1 Mar of each year regarding HQ USAF/SG's implementation of PDD/NSC-63 and DoD CIPP.

5.11. The major commands (MAJCOMs), direct reporting units (DRUs), and Air Force installation commanders are responsible for reviewing, supporting, and implementing DoD critical asset assurance requirements in accordance with DoD Directive 5160.54 and the DoD CIPP guidelines.

5.12. Air Force Computer Emergency Response Team (AFCERT), as the Joint Task Force-Computer Network Defense (JTF-CND) Air Force Forces (AFFOR), will provide AF operational capabilities for the conduct of CND in support of the JTF-CND-assigned mission. AFCERT will ensure the integration of CND operations with CIP efforts, with a focus on the cyber indications and warning, response, mitigation, and reconstitution phases of CIP.

5.13. Air Force Materiel Command (AFMC) will address assurance (including **information assurance**) and protection in the procurement of assets and infrastructure services. This will include commercial assets/services.

5.14. PDD/NSC-63 Coordination Group. This group will include representation from responsible functional areas, AFSPACE, and AFMC as listed above. The HQ USAF/SC, as the deputy AF-CIAO, will chair the PDD-63 coordination group. The Coordination Group will:

5.14.1. Determine how the Air Force will implement PDD/NSC-63 and the DoD CIPP requirements.

5.14.2. Make recommendations, through the CIO Management Board to the AF-CIO, regarding integration of Air Force issues with DoD implementation of PDD/NSC-63 and CIPP.

F. WHITTEN PETERS
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

PDD/NSC-63, *Protecting America's Critical Infrastructures*, May 22, 1998

Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988

DoD Directive S-3600.1, *Information Operations (IO)*(U), December , 199

DoD 0-2000-12H, *Protection of DoD Resources and Activities Against Acts of Terrorism and Political Turbulence*, Feb 93

DoD Directive 5160.54, *Critical Asset Assurance Program (CAAP)*, January 20, 1998

The Department of Defense Critical Infrastructure Protection Plan (CIPP), November 18, 1998

OSD Memo, "Management of the DoD Information Assurance Program (DIAP)," 30 Jan 98

Joint Pub 3-13, *Information Operations*, October 1998

CJCSI 3210.01A, *Information Operations Policy (U)*, November 1998

CJCSI 6510.01B CH-1, *Defensive Information Operations Implementation*, 2 August 98

AFDD 2-5, *Information Operations*

AFPD 10-20, *Air Force Defensive Counterinformation Operations*

AFI 31-210, *The Air Force Antiterrorism (AT) Program*

AFPD 32-10, *Installations and Facilities*

AFPD 32-40, *Disaster Preparedness*

AFI 32-1061, *Providing Utilities to US Air Force Installations*

AFH 32-4014V4, *USAF Ability to Survive and Operate Procedures in a Nuclear, Biological, and Chemical (NBC) Environment*

AFPD 33-2, *Information Protection*

AFI 33-115V1, *Network Management*

AFI 33-230, *Information Protection Assessment and Assistance Program*

Abbreviations and Acronyms

AEF—Air Expeditionary Forces

AF-CIO—Air Force Chief Information Officer

AFPD—Air Force Policy Directive

C2ISR—Command, Control, Intelligence, Surveillance, and Reconnaissance

C3—Command, Control, and Communications

C4I—Command, Control, Communications, Computers, and Intelligence

CAAP—Critical Asset Assurance Program

COE—Common Operating Environment

CIAO—Chief Infrastructure Assurance Officer

CIP—Critical Infrastructure Protection

CIPP—Critical Infrastructure Protection Plan

DIAP—Defense-wide Information Assurance Program

DII—Defense Information Infrastructure

DoD—Department of Defense

HQ USAF—Headquarters United States Air Force

HQ USAF/IL—Deputy Chief of Staff, Logistics

HQ USAF/DP—Deputy Chief of Staff, Personnel

HQ USAF/SC—Director, Communications and Information

HQ USAF/SG—Surgeon General of the Air Force

HQ USAF/TE—Directorate of Test and Evaluation

HQ USAF/XO—Deputy Chief of Staff, Operations

ISR—Intelligence, Surveillance, and Reconnaissance

JCS—Joint Chiefs of Staff

MAJCOM—Major Command

MOA—Memorandum of Agreement

NBC—Nuclear, Biological, and Chemical

OSD—Office of the Secretary of Defense

PDD/NSC—Presidential Decision Directive/National Security Council

SAF/AQ—Assistant Secretary of the Air Force, Acquisition

SAF/FM—Assistant Secretary of the Air Force, Financial Management and Comptroller

Terms

Analysis and Assessment Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Coordinated identification of DoD, national defense infrastructure, and international defense infrastructure critical assets, their system and infrastructure configuration and characteristics, and the interrelationships among infrastructure sectors; assessment of their vulnerabilities; quantification of the relationship between military plans and operations and critical assets/infrastructures; and assessment of the operational impact of loss or compromise.

Computer Network Defense—Measures taken to protect and defend information, computers and networks from disruption, denial, degradation, or destruction (CJCSI 6510.01B, *Defensive Information Operations Implementation*).

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 (5160.54, *Critical Asset Assurance Program (CAAP)*).

Critical Asset Assurance Program (CAAP)—Established by DoD Directive 5160.54 to implement the requirements of Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, November 18, 1988, and to improve DoD's mission readiness by accounting for dependencies on assets and infrastructure in the deliberate and crisis action planning process.

Cyber—A prefix used to describe a person, thing, or idea made possible as part of the computer and information age.

Cyberspace—The on-line, non-physical terrain created by the world of computer networks and systems.

Defense Sector Leads—Single focal point for planning and coordination of assurance activities within each sector. Air Force sector leads will coordinate with the DoD sector leads. See Figure 1.

Defensive Counterinformation (DCI)—Activities which are conducted to protect and defend friendly information and information systems.

Defense-Wide Information Assurance Program (DIAP)—Provides for the integrated planning, coordination, and oversight of DoD's Information Assurance Program to assure the availability, integrity, authentication, confidentiality, and non-repudiation of the DoD's mission-essential and mission-support information and reliability of the Defense Information Infrastructure.

Incident Response Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Coordinated third party (not owner/operator) emergency (e.g., medical, fire, hazardous, or explosive material handling), law enforcement, investigation, defense, or other crisis management service aimed at the source or cause of the incident.

Indications and Warning Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Tactical indications through the implementation of sector monitoring and reporting, strategic indications through intelligence community support, and warning in conjunction with the National Infrastructure Protection Center (NIPC) in concert with existing DoD and national capabilities.

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 (DoD Directive S-3600.1, *Information Operations (IO)*(U), December 9, 1996).

Infrastructure—A 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, the smooth functioning of government at all levels, or society as a whole (5160.54, *Critical Asset Assurance Program* (CAAP)).

Infrastructure Assurance—Operations that protect and defend 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, the smooth functioning of government at all levels, or society as a whole.

Mitigation Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Pre-planned and coordinated operator reactions to infrastructure warning and/or incidents designed to reduce or minimize impacts; support and complement emergency, investigatory, and crisis management response; and facilitate reconstitution.

Network —1. An organization of stations capable of intercommunication but not necessarily on the same channel. 2. Two or more interrelated circuits. 3. A combination of switches, terminals, and circuits that serve a given purpose. 4. A combination of terminals and circuits in which transmission facilities interconnect the user stations directly (that is, there are no switching, control, or processing centers). 5. A combination of circuits and terminals serviced by a single switching or processing center. 6. A combination of information transfer resources devoted to the interconnection of three or more distinct devices, systems, or gateways. 7. Two or more systems connected by a communications medium. (AFDIR 33-121, Compendium of Communication and Information Terminology).

Public Works—Public works includes four distinct physical infrastructure sectors: electric power, oil and natural gas, water and sewer, and emergency services (fire, medical, hazardous material handling, etc.). This defense infrastructure sector is composed of networks and systems, principally for the distribution of the associated commodities. The generation, production, and transport of these commodities for and to DoD are primarily the function of their respective national infrastructures. The US Army Corp of Engineers is responsible for coordinating the assurance of activities of this defense infrastructure sector (DoD CIPP).

Reconstitution Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Owner/operator-directed restoration of critical assets and/or infrastructure.

Remediation Life Cycle Phase—The term used in the DoD CIPP which refers to the period during which the following occurs: Deliberate precautionary measures undertaken to improve the reliability, availability, survivability, etc., of critical assets and/or infrastructures, e.g., emergency planning for load shedding, graceful degradation and priority restoration; increased awareness, training, and education; changes in business practices or operating procedures, asset hardening or design improvements, and system level changes such as physical diversity, deception, redundancy and backups.

System—Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions (Joint Pub 1-02, *DoD Dictionary of Military Terms*).