BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE POLICY DIRECTIVE 10-24

28 APRIL 2006

Operations

AIR FORCE CRITICAL INFRASTRUCTURE PROGRAM (CIP)

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: HQ USAF/A3/5 (Lt Col Jon Dix)

Certified by: HQ USAF/A3/5
(Lt Gen Carrol H. Chandler)

Supersedes AFPD 10-24, 1 December 1999

Pages: 11
Distribution: F

This directive establishes policy for the Air Force Critical Infrastructure Program (CIP) and supports the implementation of Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection,* December 17, 2003 and DoDD 3020.40, *Defense Critical Infrastructure Program*, 19 August 2005.

SUMMARY OF REVISIONS

This publication has been substantially revised and must be completely reviewed. Major changes include recent publication changes, HQ USAF realignment, and renaming the program from Air Force Critical Infrastructure Protection to Air Force Critical Infrastructure Program. This publication changes AF CIP implementation responsibilities from the Air Force Chief Information Officer to the HQ USAF Deputy Chief of Staff, Air, Space and Information Operations, Plans and Requirements (AF/A3/5). In addition, this publication revises and creates the roles and responsibilities of Headquarters Air Force, Major Commands, Field Operating Agencies, Direct Reporting Units, Air Force Sector Leads and Combatant Commands.

1. Air Force operations in support of the National Military Strategy are dependent on globally linked physical and cyber infrastructures (US and foreign, public and private sector). These interconnected infrastructures, while improving capabilities and mission effectiveness, also increase the Air Force's vulnerability, in regards to failures due to human error, natural disasters, and/or intentional attack. Consequently, it is important to identify and protect those infrastructures that are truly critical to the Air Force so it can accomplish its worldwide missions.

2. It is Air Force policy to:

2.1. Assure the availability of infrastructure critical to readiness and operations in peace, crisis, and war.

2.2. Establish and fund a comprehensive Air Force Critical Infrastructure Program (CIP) fully integrated with DoD and National level programs to coordinate, develop, and implement strategy and pol-

icy associated with the identification, prioritization, assessment, and protection of critical Air Force cyber and physical infrastructures.

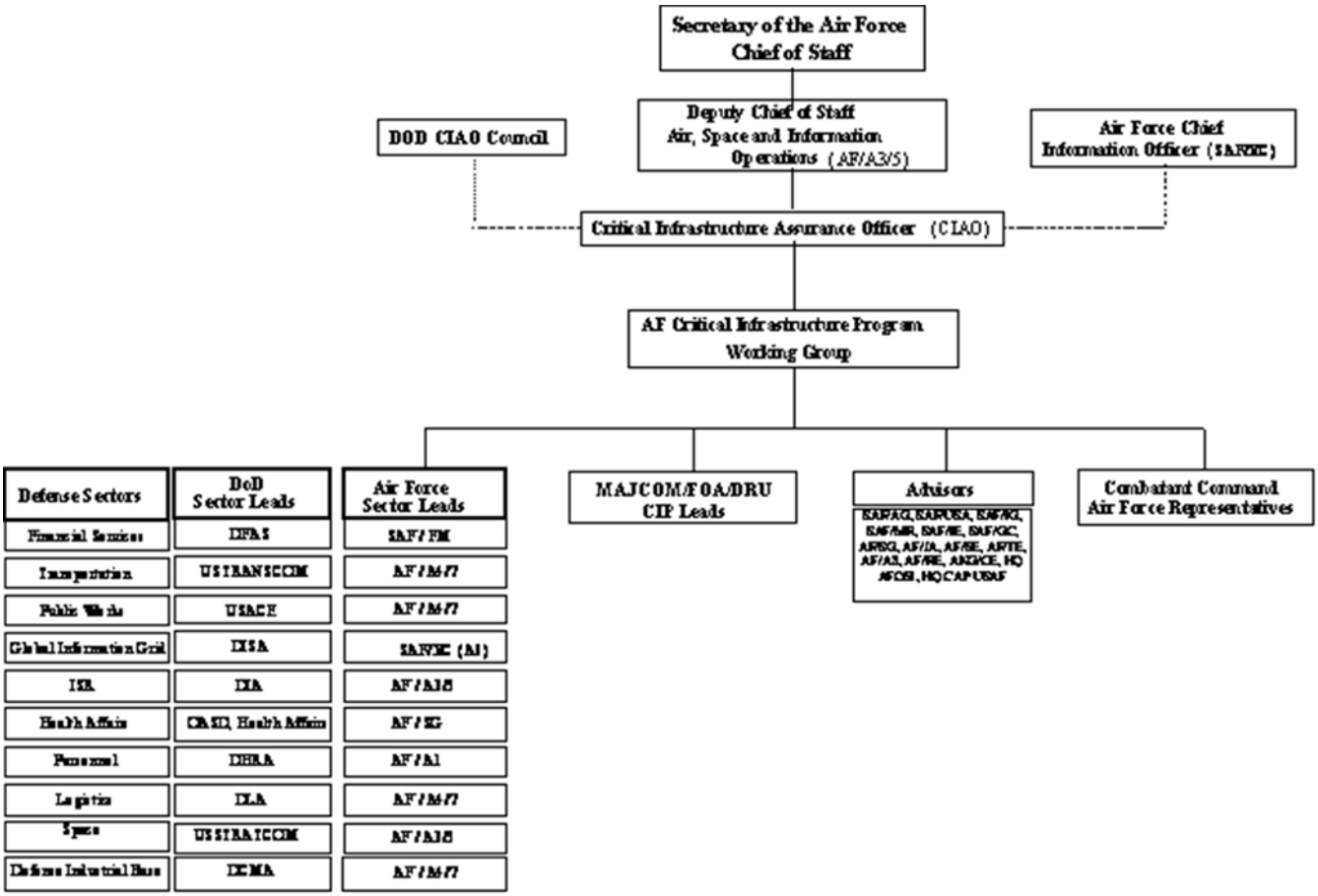
2.3. Establish Air Force Sector Leads to foster partnerships with other government and civil agencies and the private sector to address critical infrastructure issues.

2.4. Incorporate CIP education and training into all appropriate command and base level courses as well as courses for senior staff (military & civilian) and senior enlisted professional military education (PME).

2.5. Incorporate CIP into MAJCOM and installation level training exercises to instill an awareness of the impact caused by the loss of critical assets through the exploitation of their vulnerabilities.

3. Air Force CIP is based on and directly supports National and DoD CIP guidance. Integral to the overall CIP management architecture is the reliance on DoD and Air Force Sector Leads within the 10 Defense Sectors (See **Figure 1.**). Collectively, the Sectors provide a picture of the infrastructure critical to the functioning of the Air Force. The Air Force CIP will complement and integrate the mission assurance aspects of existing Air Force Antiterrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs.

Figure 1. Air Force CIP Organization.



4. It is the Commanders' responsibility to judiciously manage risk in order to accomplish the mission.

5. The following responsibilities and authorities are established:

5.1. The HQ USAF Deputy Chief of Staff, Air, Space and Information Operations, Plans and Requirements (AF/A3/5):

5.1.1. Develops Air Force critical infrastructure strategy, policy and objectives, prepares and implements plans and programs, and advocates plans, operations and funding to Departmental and governmental agencies.

5.1.2. Is the Air Force Sector Lead for Space.

5.1.3. Is the Air Force Sector Lead for Intelligence, Surveillance, and Reconnaissance (ISR).

5.1.4. Serves as the Air Force Critical Infrastructure Assurance Officer (AF-CIAO) and the office of primary responsibility for the central management and oversight of the Air Force's CIP. The AF/A3/5 may delegate this responsibility. The CIAO:

5.1.4.1. Establishes a CIP Working Group (CIPWG).

5.1.4.1.1. The CIPWG is comprised of Air Force Sector Lead representatives, Headquarters Air Force (HAF) Advisors as well as representatives from the Major Commands (MAJCOM), Field Operating Agencies (FOA), Direct Reporting Units (DRU) and Air Force Component representatives from the Combatant Commands (See **Figure 1.**) as needed.

5.1.4.1.2. It serves as the principal working level forum to vet CIP-related strategy development, policies, procedures, plans and operations, raise CIP-related issues, share information of mutual interest, and informally coordinate CIP issues and recommendations among the members before formal staffing.

5.1.4.2. Identifies additional advisors to the CIPWG as required.

5.1.4.3. Represents the Air Force on the DoD Critical Infrastructure Protection Integration Staff (CIPIS). Coordinates Air Force CIP-related actions with DoD CIP activities.

5.1.4.4. Develops and establishes Air Force CIP policy procedural guidance.

5.1.4.5. Oversees Air Force CIP initiatives and is the single focal point for all Air Force CIP-related issues.

5.1.4.6. Identifies and assigns a Program Element Monitor (PEM) for Air Force CIP activities. The CIP PEM:

5.1.4.6.1. Identifies and programs CIP funding requirements for identification, prioritization, assessment, and management of CIP and related data.

5.1.4.6.2. Advocates MAJCOM funding requirements to include remediation.

5.1.4.7. Coordinates with and supports the Combatant Command Air Force Components, MAJCOMs, FOAs, DRUs and Sectors in standardizing, integrating, scheduling, executing and reporting of Air Force critical infrastructure identification, vulnerability assessment, and remediation.

5.1.4.8. Develops and implements a common Air Force CIP data management system, that will assist in providing commanders situational awareness of the AF critical infrastructure. The data management system will be interoperable with DoD level CIP data management systems.

5.1.4.9. Reviews and approves Air Force Sector, MAJCOM, FOA and DRU annual reports regarding Air Force CIP implementation and, in turn, report on the Air Force's CIP implementation status to the DoD-CIAO. Air Force CIP leads will provide their annual reports to the AF-CIAO by 1 October of each year.

5.2. The Secretary of the Air Force, Communications (SAF/XC dual-hatted as A6):

5.2.1. Provides overarching policy and oversight regarding information assurance and the Air Force Enterprise's operational, system, and technical architectures.

5.2.2. Coordinates with other federal Chief Information Officers on CIP/information assurance issues.

5.2.3. Plans and develops procedures to ensure continuity of operations for information systems that support the operations and assets of the Air Force.

5.2.4. Is the Air Force Sector Lead for the Global Information Grid.

5.2.5. Develops guidance and procedures to implement National, DoD, JCS, and Air Force IA direction.

5.3. The HQ USAF Deputy Chief of Staff for Logistics, Installations and Mission Support (AF/A4/7):

5.3.1. Is the Air Force Sector Lead for the following:

5.3.1.1. Logistics.

5.3.1.2. Transportation.

5.3.1.3. Public Works.

5.3.1.4. Defense Industrial Base.

5.4. The HQ USAF Deputy Chief of Staff, Manpower and Personnel (AF/A1) is the Air Force Sector Lead for Personnel.

5.5. The HQ USAF Surgeon General (AF/SG):

5.5.1. Is the Air Force Sector Lead for Health Affairs.

5.6. The Assistant Secretary of the Air Force, Acquisition (SAF/AQ), is responsible for Air Force CIP acquisition policies and procedures used during non-space system acquisition process. In this capacity, SAF/AQ will:

5.6.1. Establish critical infrastructure acquisition procedures and requirements; and implement policies that reduce the vulnerabilities of critical infrastructures by incorporating CIP requirements into the acquisition and procurement process.

5.6.2. Provide an acquisition Advisor to the Air Force CIP Working Group.

5.7. The Assistant Secretary of the Air Force, Financial Management and Comptroller (SAF/FM) is the Air Force Sector Lead for appropriations, financial management, and systems.

5.8. The Assistant Secretary of the Air Force, Inspector General (SAF/IG) is responsible for assuring compliance with Air Force CIP policy. In the capacity, SAF/IG:

5.8.1. Ensures CIP policy is integrated and assessed during Air Force inspections.

5.8.2. Provides an Advisor to the Air Force CIP Working Group.

5.9. The Under Secretary of the Air Force, Directorate of Space Acquisition (SAF/USA) is the Air Force Lead for acquisition of space systems and provides an advisor to the Air Force CIP Working Group.

5.10. The following organizations shall provide Advisors to the CIPWG as needed:

5.10.1. The Assistant Secretary of the Air Force, Manpower and Reserve Affairs (SAF/MR).

5.10.2. The Assistant Secretary of the Air Force, Installations, Environment, and Logistics (SAF/IE).

5.10.3. The HQ USAF Directorate of Test and Evaluation (AF/TE).

5.10.4. The Deputy Chief of Staff, Strategic Plans and Programs (AF/A8).

5.10.5. The Air Force Office of Chief of Safety (AF/SE).

5.10.6. The Office of Air Force Reserve (AF/RE).

5.10.7. The Air National Guard Civil Engineer Directorate (ANG/CE).

5.10.8. HQ Civil Air Patrol-USAF (HQ CAP-USAF).

5.10.9. The Office of the Air Force General Counsel (SAF/GC)

5.10.10. The Office of the Judge Advocate General of the Air Force (AF/JA).

5.10.11. The Air Force Office of Special Investigations (AFOSI).

6. The Headquarters Air Force, Major Commands, Field Operating Agencies, and Direct Reporting Units, are responsible for implementing Air Force CIP requirements in accordance with this policy. They will:

6.1. Establish and maintain a critical infrastructure program within the Operations Directorate or equivalent.

6.2. Participate in the Air Force CIPWG.

6.3. Identify and program CIP related funding requirements to include remediation.

6.4. Implement policies and establish procedures, plans, and operations to reduce critical infrastructure vulnerabilities of MAJCOMs, FOAs or DRUs.

6.5. Identify and prioritize critical MAJCOM, FOA or DRU owned and/or managed infrastructures, and assess their vulnerability to human error, natural disasters, or intentional physical or cyber attack.

6.6. Coordinate with the HQ USAF/A3/5 and Air Force Sector Leads on the identification, vulnerability assessment and remediation of critical Air Force and non-Air Force owned and/or managed infrastructure that support the MAJCOMs, FOAs or DRUs.

6.7. Monitor and report decisions undertaken to remediate identified critical asset vulnerabilities. In case of loss or disruption of critical infrastructure, develop strategies for mitigating the effects of such loss or disruption and include them in the Continuity of Operations Plans (COOP).

6.8. Identify with the Combatant Command Air Force Components the impact resulting from our reliance on both Air Force and non-Air Force critical infrastructure and the risk of their loss, damage, or destruction to the Air Force mission.

6.9. Coordinate with the Combatant Command Air Force Components on the development of procedures for remediation, mitigation, and assurance that the minimum essential levels of operations can be maintained.

6.10. Incorporate CIP education and training concepts into MAJCOM, FOA or DRU command level courses as well as courses for senior staff (military and civilian) and senior enlisted personnel PME. Air Education and Training Command will coordinate with the AF CIAO to standardize the CIP education and training across the Air Force.

6.11. Incorporate CIP concepts into MAJCOM, FOA, DRU and installation level training exercises, including COOP exercises, to instill an awareness of the impact caused by the loss of critical assets through the exploitation of their vulnerabilities, and that lessons learned are applied to remediate such vulnerabilities.

6.12. Provide the AF-CIAO an annual report by 1 October regarding MAJCOM, FOA or DRU implementation and status of the Air Force CIP for inclusion in the annual report to the DoD CIAO.

7. The Air Force Components to the Combatant Commands will:

7.1. Participate in the Air Force CIPWG as required.

7.2. Identify and prioritize Air Force assets critical to the capabilities required by the Combatant Commander.

7.3. Coordinate with the MAJCOM, FOA, DRU and Air Force Sector leads on the identification, vulnerability assessment, and remediation of critical Air Force and non-Air Force owned and/or managed infrastructure.

7.4. Identify the impact resulting from loss, damage or destruction of internal and external infrastructure critical to the Combatant Command's mission.

7.5. Coordinate with the MAJCOM, FOA, DRU and Air Force Sectors on the development of procedures for remediation, mitigation, and mission assurance that ensure the minimum essential levels of Air Force operations can be maintained.

7.6. Provide the AF-CIAO an annual assessment by 1 October regarding Air Force implementation of CIP initiatives for inclusion in the annual report to the DoD CIAO.

8. Air Force Sector Leads will:

8.1. Identify and assign a representative to participate in the Air Force CIPWG and the DoD Sector working groups.

8.2. Coordinate with the Combatant Command Air Force Components, MAJCOM, FOA, DRU, and DoD Sector leads on the identification, vulnerability assessment, and remediation of critical Air Force

and non-Air Force owned and/or managed sector infrastructures to ensure that essential sector operations can at least be maintained at minimum level.

8.3. Identify the impact resulting from loss, damage or destruction of internal and external infrastructure critical to the Combatant Command's mission.

8.4. Provide the AF-CIAO an annual report by 1 October regarding the sector's implementation and status of the Air Force's CIP for inclusion in the annual report to the DoD CIAO.

9. See **Attachment 1** for a glossary of CIP-related documents and an explanation of terms used in this directive.

MICHAEL W. WYNNE
Secretary of the Air Force

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Homeland Security Presidential Directive/HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection* 17 December 2003

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

DoDD 2000.12, *The DoD Antiterrorism (AT) Program*, 18 August 2003

DoDD S-3600.1, *Information Operations (IO)* (U), 9 December 1996

DoDD 3020.40, Defense Critical Infrastructure Program (DCIP), 19 Aug 2005

DoDD 5000.1, *The Defense Acquisition System,* 12 May 2003

DoDD 5200.39, *Security, Intelligence, and CI Support to Acquisition Program Protection*, 10 Sep 1997

DoDD 5240.2, *DoD Counterintelligence*, 22 May 1997

DoDD 8500.1, *Information Assurance*, 24 October 2002

DoDI 2000.16, *DoD Antiterrorism Standards*, 14 Jun 2001

DoDI 5000.2, *Operation of the Defense Acquisition System,* 12 May 2003

DoDI 8500.2, *Information Assurance Implementation*, 6 February 2003

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

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

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

OSD Memo, *Management of the DoD Information Assurance Program (DIAP)*, 30 January 1998

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

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

CJCSI 6510.01, *Defense in Depth: Information Assurance and Computer Network Defense,* 23 March 2003

AFJI 31-102, *Physical Security,* 31 May 1991

AFDD 2-5, *Information Operations,* 5 August 1998

AFPD 10-20, *Air Force Defensive Counterinformation Operations,* 1 October 1998

AFPD 10-25, *Full-Spectrum Threat Response,* 18 July 2002

AFPD 32-10, *Installations and Facilities,* 27 March 1995

AFPD 32-40, *Disaster Preparedness,* 1 May 1997

AFPD 33-2, *Information Protection*, 1 December 1996

AFPD 63-7, *Industrial Facilities,* 17 May 1993

AFPD 99-1, *Test and Evaluation Process,* 22 July 1993

AFI 23-111, *Management of Government Property in Possession of the Air Force,* 1 February 1996

AFI 10-245, *Air Force Antiterrorism Standards,* 21 Jun 2002

AFI 32-1061, *Providing Utilities to US Air Force Installations,* 15 March 2002

AFH 32-4014V4, *USAF Ability to Survive and Operate Procedures in a Nuclear, Biological, and Chemical (NBC) Environment,* 1 March 1998

AFI 33-115V1, *Network Operations (NETOPS), 3May 2004*

AFI 33-116, *Long-Haul Telecommunications Management,* 17 April 2002

AFI 33-230, Information Assurance Assessment and Assistance Program, 4 August 2004

AFI 63-701, Managing Industrial Facilities, 24 June 1994

Abbreviations and Acronyms

AF—Air Force

AF/A1—Deputy Chief of Staff, Manpower and Personnel

AF/A3/5—Deputy Chief of Staff, Air, Space and Information Operations, Plans and Requirements

AF/A4/7—Deputy Chief of Staff, Logistics, Installations and Mission Support

AF/A8—Deputy Chief of Staff, Strategic Plans and Programs

AF/JA—The Judge Advocate General

AF/RE—Office of the Air Force Reserve

AF/SE—Chief of Safety

AF/SG—Surgeon General of the Air Force

AF/TE—Directorate of Test and Evaluation

AF-CIAO—Air Force Critical Infrastructure Assurance Officer

AF-CIO—Air Force Chief Information Officer

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

CIAO—Critical Infrastructure Assurance Officer

CIO—Chief Information Officer

CIP—Critical Infrastructure Program

CIPIS—Critical Infrastructure Protection Integration Staff

CIPWG—Critical Infrastructure Program Working Group

DoD—Department of Defense

DRU—Direct Reporting Units

FOA—Field Operating Agency

GIG—Global Information Grid

HAF—Headquarters Air Force

HSPD—Homeland Security Presidential Directive

HQ USAF—Headquarters United States Air Force

ISR—Intelligence, Surveillance, and Reconnaissance

MAJCOM—Major Command

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

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

SAF/IE—Assistant Secretary of the Air Force, Installation, Environment, and Logistics

SAF/IG—Assistant Secretary of The Air Force, Office of The Inspector General

SAF/MR—Assistant Secretary of the Air Force, Manpower and Reserve Affairs

SAF/XC—Deputy Chief of Staff, Warfighting Integration

SAF/USA—Under Secretary of the Air Force, Directorate of Space Acquisition

Terms

Critical—The level of importance of an asset to the success of the Combatant Commands or Air Force mission. For the AF CIP, criticality is broken down into four Tiers:

- Tier I - Warfighter/Combatant Commands suffers strategic mission failure. Specific timeframes and scenarios assist in infrastructure prioritization.
- Tier II - The Air Force suffers mission failure, but warfighter strategic mission is accomplished.
- Tier III - Individual element failures, but no debilitating strategic or Air Force mission failure.
- Tier IV - Everything else.

Critical Infrastructure—Cyber and physical systems and assets so vital to the Air Force that the incapacity or destruction of such systems and assets would have a debilitating impact on the Air Force's ability to execute its missions.

Critical Infrastructure Asset—An infrastructure asset deemed essential to Air Force operations or the functioning of a Critical Asset.

Critical Infrastructure Program (CIP)—The identification, assessment, and security enhancement of cyber and physical assets and associated infrastructures essential to the execution of the National Military Strategy. It is a complementary program linking the mission assurance aspects of the Anti-Terrorism, Force Protection, Information Assurance, Continuity of Operations, and Readiness programs.

Defense Sector—A group of infrastructures and assets that perform a similar function. The Defense Infrastructure Sectors include, but are not limited to: defense industrial base; financial services; logistics; global information grid; transportation; personnel; health affairs; intelligence, surveillance and

reconnaissance; space; and public works.

Infrastructure—A framework of interdependent assets, 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.

Infrastructure Asset—Any infrastructure facility, equipment, service or resource that supports an Air Force Mission.

Mitigation—Actions taken to lessen the chance of the loss or degradation of a critical infrastructure

Remediation—Actions taken to recover from the effects of the loss or degradation of a critical infrastructure.

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.**

Vulnerability—

- The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.
- The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.
- In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.