



**SECRETARY OF THE AIR FORCE  
WASHINGTON, DC**

AFPD10-24\_AFPM1

6 January 2012

MEMORANDUM FOR DISTRIBUTION C  
ALMAJCOM-FOA-/DRU

SUBJECT: Air Force Policy Memorandum to AFPD 10-24, Air Force *Critical Infrastructure Program (CIP)*, 28 April 2006

By Order of the Secretary of the Air Force. This is an AF Policy Memorandum immediately changing AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with AFI 33-360, *Publications and Forms Management*.

Pending the rewrite and publication of AFPD 10-24, the policy changes at the attachment to this memorandum are effective immediately.

The policy in this Memorandum becomes void after 180 days have elapsed from the date of this memorandum, or upon incorporation by interim change to, or rewrite of AFPD 10-24, whichever is earlier.

Michael B. Donley  
Secretary Of The Air Force

Attachment:  
Policy Changes

## **ATTACHMENT** *Policy Changes*

**(Replace) Opening.** This directive implements DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, renames the Air Force Critical Infrastructure Program (CIP) to the Air Force Critical Asset Risk Management (CARM) Program, establishes the Air Force CARM Program, and assigns responsibilities for the execution of the program. This change in program name highlights the program's risk management focus on discrete Defense Critical Infrastructure (DCI) and their relationship to the mission. It was instituted to prevent continued confusion, such as thinking that the CIP is a force protection, civil engineering, or communications program. The program cuts across all mission sets and operational capability areas – it is not a civil engineering (CE), logistics, antiterrorism (AT), communications, or facilities-focused program. Air Force DCI includes Task Critical Assets (TCA) and Supporting Infrastructure Critical Assets (SICA).

### **(Replace) 1.**

#### 1. Overview.

1.1. 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.

1.2. The mission of the Air Force Critical Asset Risk Management (CARM) Program is to enhance the risk management decision-making capability at all levels to ensure that Air Force DCI is available when required to support Combatant Command (COCOM) and Air Force operational and Title 10 U.S.C. mission requirements in an all threat and all hazard environment. This risk management approach will support the prioritization of scarce resources across the Air Force, focusing priorities on the greatest risk based on assessed criticality, vulnerability, threats, and hazards. This approach includes the identification, assessment, and effective management of risk to assets essential for executing the National Defense Strategy.

1.3. The Air Force CARM Program will implement a criticality and sector characterization process to identify Air Force DCI. Through a threat and hazard identification process, the AF CARM Program will further define the potential for loss of Air Force DCI assets, and in conjunction with the vulnerability assessment process, will ascertain the overall risk to these assets. The analytic results of these incremental processes will provide to appropriate decision-makers the capability to properly assess the levels of risk to these assets.

1.3. The objectives of the Air Force CARM Program are:

- 1.3.1. Provide Air Force policy and program guidance.
- 1.3.2. Foster Air Force strategic partnerships and enabling technologies.
- 1.3.3. Integrate and implement Air Force plans, programs, and capabilities at all levels.
- 1.3.4. Facilitate Air Force resourcing at all levels.
- 1.3.5. Incorporate and promote Air Force CARM into education, outreach and training programs at all organizational levels.
- 1.3.6. Identify and validate AF DCI, assess vulnerabilities, risk and operational impact of loss or degradation of AF DCI.
- 1.3.7. Create situational awareness at the senior leadership levels to the status of Air Force DCI with emphasis on Defense Critical Assets (DCAs).
- 1.3.8. Establish the necessary lines of communication and promote information sharing among DoD Components and Defense Infrastructure Sector Lead Agents (DISLAs).

**(Replace) 2.**

2. Air Force policy. Headquarters, Air Force will:

2.1. Establish, implement and centrally resource the AF CARM Program. Oversee the implementation of AF CARM policy and guidance for the risk management of DCI, including issuance of strategies, plans, and standards. The Air Force CARM Program will coequally complement and not be subordinate to other DoD programs, functions, and activities that contribute to mission assurance through risk management.

2.2. Establish an office of primary responsibility (OPR) for all Air Force CARM Program related matters, with the capability to execute DoD Defense Critical Infrastructure Program (DCIP) requirements, and develop, coordinate and implement Air Force strategy and policy associated with the identification, prioritization, assessment, and protection of Air Force-owned DCI. The Air Force CARM program OPR will develop, communicate and maintain up to and including Top Secret, sensitive compartmented information (SCI) DCI-related data.

2.3. Develop, publish, and maintain comprehensive DCIP implementation plans that will include program vision and end state, program goals and objectives, major program milestones, major functional responsibilities and program capabilities, dissemination and/or sharing of program outputs, and results that support the overall DCIP execution.

2.4. Establish the necessary lines of communication and promote information sharing with each other and with Federal departments and agencies; State, local, regional, territorial, and tribal entities; the private sector; and foreign countries, as appropriate.

2.5. Incorporate requirements for the risk management of DCI in acquisition, maintenance, and sustainment contracts, as well as in facility construction, installation recapitalization and installation-level outsourcing and privatization efforts.

2.6. Identify, validate and prioritize core requirements of the AF CARM Program in the AF baseline budget generated through the Planning, Programming, Budgeting and Execution System (PPBES) to execute a comprehensive Air Force CARM Program fully integrated with DoD and national level programs. These core requirements are:

2.6.1. Define and validate credible manpower requirements and utilize the PPBES to plan, program and advocate for sufficient manpower resources to execute the AF CARM Program.

2.6.2. Establish a comprehensive and varying tiered performance measurement and compliance strategy to determine the CARM Program's overall effectiveness and compliance with AF CARM Program standards and benchmarks, including associated metrics.

2.6.3. Conduct Air Force Critical Asset Risk Assessments (CARAs) as mandated by DoD and Section 335 to the National Defense Authorization Act of 2009 (Public Law 110-417), of the threats and hazards, vulnerability and risk to Air Force-owned DCI and inter- and intra-dependencies needed to accomplish required COCOM and AF operational and Title 10 U.S.C. mission requirements. To comply, the Air Force will:

2.6.3.1. Develop, manage and implement Air Force CARM Program processes and procedures, including the nomination, scheduling, and execution of an Air Force CARA for all Air Force DCI.

2.6.3.2. Minimize the inspection/assessment footprint to the maximum extent practical. CARA evaluators will not interfere with deployments supporting COCOM missions or mission execution during Center/Wing home station daily operations.

2.6.4. Develop and implement an AF CARM Program long-term strategy for outreach, education, training and exercises to meet DCIP and Air Force CARM Program education and training goals and objectives.

2.6.5. Develop, manage and sustain the Air Force Critical Asset Management System (AF-CAMS), the Air Force CARM Program authoritative database for the total life-cycle management of DoD and Air Force CARM Program requirements. Air Force-CAMS captures CARA reports including risk-related data to TCAs and SICAs, and remediation and mitigation plans addressing risks to critical assets – all of which are shared with COCOMs, JS/J34, and ASD (HD&ASA).

2.7. Establish AF Sector Leads to foster relationships with other government and civil agencies and the private sector to address critical infrastructure issues.

2.8. Coordinate and integrate Air Force CARM Program guidance, procedures and capabilities into the overarching disciplines and instructions of other AF contingency planning programs, risk management, and mission assurance plans. These plans include: emergency management (EM); AT; force protection (FP); readiness; continuity of operations program (COOP); integrated defense (ID); counter-chemical, biological, radiological and nuclear (C-CBRN); information protection (IP)/information assurance (IA); communications security (COMSEC); operations security (OPSEC); homeland security, defensive counterinformation and multidisciplinary vulnerability assessments, and will:

2.8.1. Create a comprehensive, aggregated, coordinated and cohesive enterprise-wide approach to the identification, prioritization, mission analysis, and vulnerability risk assessment/management for Air Force DCI at all levels.

2.8.2. Integrate DCIP and Air Force CARM Program guidance and activities into organizational guidance, plans and orders as they relate to Air Force DCI. DCIP policies should be integrated into contracts, as appropriate.

2.8.3. Foster collaboration and synchronization among risk management planning tools, products and processes to ensure the Air Force's ability to execute its missions and capabilities. Establish necessary lines of communication to promote information sharing with each of these risk management programs, as appropriate.

2.9. Oversee monitoring and reporting of Air Force DCI with priority emphasis on DCAs. Maintain situational awareness of the risk to Air Force -owned DCI. Ensure relevant, timely and actionable DCI information is shared with DCIP and Air Force CARM Program stakeholders and operational end users. Assist in integrating and synchronizing threat, hazard and DCIP and Air Form CARM Program asset information to strengthen operational readiness and preparedness.

2.10. With the support of the appropriate DoD Components and DISLAs, document a risk management decision to remediate, mitigate or accept risk for all Air Force-owned DCI, to include Air Force CARM Plans at selected Air Force Tier I locations.

2.11. Manage the risk of loss or degradation of Air Force DCI through the HAF-level CARM Working Group (CARMWG). Coordinate with the COCOMs, JS/J34, and the Under Secretary of Defense for Policy to identify and integrate their priorities for remediation and mitigation and programming resources through the PPBES as appropriate to implement DCIP risk management decisions.

**(Delete) 5.1.4.9.**

**(Add New) 5.10.12.** The Administrative Assistant to the Secretary of the Air Force (SAF/AA).

**(Modify) 6.** Headquarters Air Force (HAF), Major Commands (MAJCOMs), Air Force

Component Commands, Field Operating Agencies (FOAs), Direct Reporting Units (DRUs) and the Air National Guard (ANG) will execute the Air Force CARM Program within the Operations Directorate (A3) or equivalent and maintain a CARM Program office in accordance with this policy and any implementing guidance consistent with available resources. They will:

**(Modify) 6.1.** Identify a central point of contact for all matters pertaining to the identification, prioritization and risk management of Air Force DCI. The HAF, MAJCOM, AF Component Commands, FOAs, DRUs and ANG HQ CARM Program manager will possess a Top Secret, SCI security clearance.

**(Modify) 6.2.** Participate in the AF CARMWG.

**(Modify) 6.4.** Implement policies and establish procedures, plans, and operations to reduce critical infrastructure vulnerabilities at all levels.

**(Modify) 6.5.** Identify and prioritize critical infrastructures, and assess their vulnerability to human error, natural disasters, or physical or cyber attack.

**(Delete) 6.12.**

**(Delete) 7.6.**

**(Delete) 8.4.**

#### **Attachment 1 (Add)**

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 31-601, *Industrial Security Program Management*, 29 June 2005

#### **Administrative Changes**

References throughout in AFPD 10-24 to “CIP or AF CIP” are hereby changed to “Air Force CARM Program.”

Reference in the Preface to DoDD 3020.40, *Defense Critical Infrastructure Program*, is hereby changed to DoDD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*, January 14, 2010.

#### **(Add New) Abbreviations and Acronyms**

**CARA**—Critical Asset Risk Assessment

**CARM**—Critical Asset Risk Management

**COCOM**—Combatant Command

**DCA**—Defense Critical Asset

**DCI**—Defense Critical Infrastructure

**DISLAs**— Defense Infrastructure Sector Lead Agents

**(Modify) Terms**

**Critical**—The level of importance of an asset to the success of the COCOMs or Air Force mission. For the AF CARM Program, this criticality is broken down into three tiers. These tiers are:

- Tier I TCA. An asset the loss, incapacitation or disruption of which could result in mission (or function) *failure* at the DoD, Military Department, Combatant Commander, sub-unified command, DA or DISLA level.

- Tier II TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) *severe degradation* at the DoD, Military Department, Combatant Commander, sub-unified command, DA or DISLA level.

- Tier III TCA. An asset the loss, incapacitation, or disruption of which could result in mission (or function) *failure* or *severe degradation* below the Military Department, Combatant Commander, sub-unified command, DA or DISLA level.

**(Add New)**

**Critical Asset**—An asset of such extraordinary importance that its incapacitation or destruction would have serious, debilitating effect on the ability of one or more DCIP components to execute the task or mission essential task it supports. In addition:

- Mission impact alone determines whether asset is critical.
- Generally one of a kind, or of such limited number, that loss has measureable mission impact – either mission failure or severe degradation.
- People, planes, installations, and nuclear weapons do not generally qualify as Tier I or II critical assets per DoD definition – redundancies exist.

**Risk**—Combination of the probability of an undesirable event occurring and the consequence of that undesirable event. Risk is quantified by multiplying *impact or criticality times threat/hazard times vulnerability*.

**Risk Assessment**—Systematic examination of risk using disciplined processes, methods, and tools. It provides an environment for decision making to continuously evaluate and prioritize risks and recommended strategies to remediate or mitigate those risks.

**Risk Management**—Process by which CA risk is assessed and calculated using the risk formula, and commanders/directors analyze the risk to their critical assets and make the decision to accept or remediate/mitigate that risk.

**Supporting Infrastructure Critical Asset (SICA)**—A supporting infrastructure asset (SIA) that is directly used to support the functioning or operation of a TCA, such that the SIA's loss, degradation, or denial will result in the inability of the TCA to function or operate as intended in the execution of its associated MET or function. In other words, a TCA cannot operate or function without a SICA being available or functioning.

**Task Critical Asset (TCA)**—An asset that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability to execute the mission it supports.

**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 AFD 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.

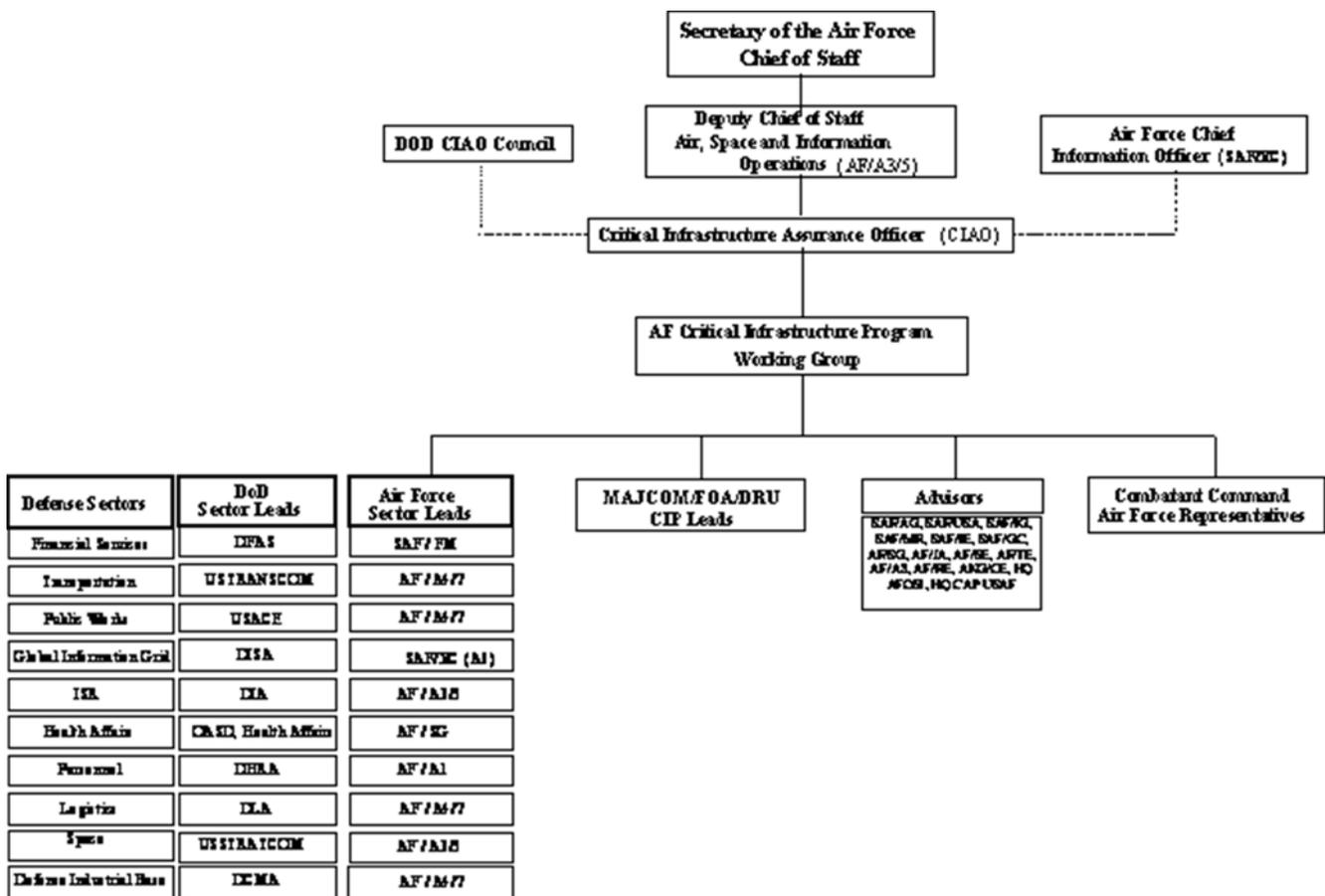
2.3. Establish Air Force Sector Leads to foster partnerships with other government and civil agencies and the private sector to address critical infrastructure issues.

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)*, 3 May 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.