

**BY ORDER OF THE COMMANDER  
AIR EDUCATION AND TRAINING  
COMMAND**



**AETC INSTRUCTION 10-2401**

**10 SEPTEMBER 2009**  
Certified Current 27 March 2014  
**Operations**

**CRITICAL INFRASTRUCTURE PROGRAM (CIP)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications are available for downloading or ordering on the e-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil).

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: HQ AETC/A2/30

Certified by: HQ AETC/A2/3 (Mr. James T. Parris)  
Pages: 23

---

This instruction implements AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*. It establishes standards to identify and assess, remediate, monitor and report, mitigate, and reconstitute critical infrastructure assets and mission-essential capabilities to achieve mission assurance. It applies to AETC commanders, tenant unit commanders on AETC installations, and commanders or officers in charge of AETC tenant activities on other military installations. It also applies to Air Force Reserve Command and Air National Guard units.

To the extent directions in this publication are inconsistent with other Air Force publications, the information herein prevails. Refer recommended changes and questions about this publication to HQ AETC/A2/30 using AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional chain of command. (AF Form 847 is prescribed in AFI 11-215, *USAF Flight Manuals Program (FMP)*). Refer to that publication for guidance on filling out the form.)

Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afirms/afirms/>. Attachment 1 contains a glossary of references and supporting information used in this publication.

Section A—Overview	2
1.    General. ....	2
2.    Developing a Successful AETC CIP: ....	3
3.    Force Protection and Mission Assurance. ....	3
4.    Air Force-Critical Asset Management System (AF-CAMS). ....	3
5.    Risk Management: ....	4
6.    Identification, Prioritization, and Assessment of Critical Air Force Assets: ....	4
Section B—Roles and Responsibilities	4
7.    HQ AETC: ....	5
8.    NAF: ....	9
9.    Host Wing Commander: ....	9
10.   Tenant Activities on AETC Installations: ....	10
11.   AETC Tenant Activities on Other Military Installations: ....	11
Section C—CIPWG	11
12.   Requirements and Contacts. ....	11
Table 1.   Air Force CIP Sector and HQ AETC Sector Lead Assignments. ....	11
Section D—TWG	12
13.   Description and Requirements. ....	12
Section E—CIP Executive Committee	12
14.   Description and Membership. ....	12
Section F—Adopted Forms	13
15.   Adopted Form: ....	13
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>14</b>
<b>Attachment 2—CHARTER FOR AETC CRITICAL INFRASTRUCTURE PROGRAM WORKING GROUP (CIPWG)</b>	<b>19</b>

### ***Section A—Overview***

**1. General.** The AETC Critical Infrastructure Program (CIP) is a commander’s risk management program designed to assure critical assets are available to support AETC-assigned mission-essential tasks (MET). The AETC CIP results from national policy provided by Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection*, and DoDD 3020.40, *Defense Critical Infrastructure Program*

(DCIP). The commander's emphasis on the importance of CIP at all levels of war to achieve an acceptable level of risk drives the level of effort and resources required for a successful CIP.

## 2. Developing a Successful AETC CIP:

2.1. This publication provides minimum standards to develop a successful program. Sections on procedural guidance and roles and responsibilities outline what is required from HQ AETC, wings, units, and tenant activities, but each critical asset has a different set of risk factors. Therefore, to the maximum extent possible and without compromising the chain of command, the responsible commander for the mission will determine acceptable levels of risk.

2.2. This instruction addresses the defense critical infrastructure (DCI) essential to achieving the successful execution of AETC-assigned missions. By definition, DCI includes critical assets that can include those assets owned by the Department of Defense (DoD), state and local governments, US commercial and private sector, foreign commercial and private sector, and host nations.

2.3. US Air Force and AETC critical asset risk management (CARM) focuses on mission assurance ensuring critical assets needed to execute missions and core capabilities essential to executing the National military strategy are available when required.

2.4. Members fulfilling duties as CIP managers, facilitators, or working group members must possess a secret security clearance at minimum because DoDM 3020.45, Volume 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*, Enclosure 3, paragraph 2b, requires information pertaining to the CIP be classified.

2.5. The AETC CIP is an all threats and hazards program, meaning, all threats and hazards to infrastructure capabilities that could disrupt the mission are relevant CIP issues. By no means constituting a complete list, threat examples include terrorist, insider, and nation state; hazard examples include pandemics, hurricanes, flooding, and fires.

2.6. The AETC CIP contributes to Air Force's ability to achieve mission assurance, as do antiterrorism (AT); continuity of operations (COOP); chemical, biological, radiological, nuclear, and high yield explosive (CBRNE) readiness and consequence management; and information assurance (IA).

**3. Force Protection and Mission Assurance.** Force protection is an overarching concept and mission responsibility inherent to command within all military operations. AT, in contrast, is a subelement of combating terrorism and complementary mission assurance activity like CIP, COOP, CBRNE, and IA. These activities when working in harmony provide a synergy to achieve mission assurance; that is to say, mission assurance is a goal or end state of force protection and these supporting activities.

**4. Air Force-Critical Asset Management System (AF-CAMS).** AF-CAMS is the authoritative data source in managing the baseline elements of information for the Air Force CIP. This system provides commanders a tool for recalling information regarding critical assets and missions, dependencies, vulnerability information, and other characteristics of a critical asset. This information can be displayed in tabular and geographical information system (GIS) viewing formats.

## 5. Risk Management:

5.1. CIP is the primary method for prioritizing resources for a number of CIP processes including scheduling assessments, mitigation, and remediation strategies. Additionally, it helps provide the framework for Air Force critical asset risk assessments (CARA) and other DoD-sponsored vulnerability assessments.

5.2. The basic risk equation for qualifying risk in AETC is criticality *times* vulnerability *times* threat or hazard. This equation produces a product of these risk factors. A zero value in any of these factors results in no risk to the asset or mission.

## 6. Identification, Prioritization, and Assessment of Critical Air Force Assets:

6.1. **Identification of Critical Assets.** Air Force critical assets consist of systems and assets so vital the incapacity or destruction of such systems and assets would have a debilitating impact on the Air Force's ability to execute its mission-essential tasks and core capabilities. An asset is determined to be critical based solely on:

6.1.1. **Impact.** The asset's impact on the execution of a mission task, capability, or core function the asset supports, and:

6.1.1.1. The identified impact due to the unavailability of the asset for any reason would result in the failure to execute the mission task, core capability, or function; or,

6.1.1.2. The identified impact due to the unavailability of the asset for any reason would result in significant degradation in the execution of the mission task, core capability, or function.

6.1.2. **Critical Asset Tiers.** The tier definitions comply with and supplement the DoD tier definitions listed DODM 3020.45, Volume 1.

6.1.2.1. The use of these tier definitions will support information sharing with other DoD components who may request Air Force critical asset data by tiers.

6.1.2.2. Use of tiers is a high-level way to categorize the scope of impact caused by the loss of critical assets to the missions, functions, and tasks those assets support.

6.2. **Prioritization Criteria.** Six criteria are utilized to prioritize Air Force critical assets:

6.2.1. MET level of war being supported by the critical asset.

6.2.2. Impact of loss of the critical asset on the METs/functions.

6.2.3. Time for restoration of the asset and its capability.

6.2.4. Time from asset capability loss to impact on supported METs/functions.

6.2.5. Number of METs supported by the critical asset.

6.2.6. Number of organizations the critical asset supports.

6.3. **Determining the Impact.** This prioritization will be used to provide the *impact* measure of a critical asset. *Impact* refers to the undesirable results to the missions, core functions, or other capabilities caused by the loss or degradation of the critical asset, and are used in the critical asset risk formula.

## Section B—Roles and Responsibilities

## 7. HQ AETC:

### 7.1. AETC Commander (CC):

7.1.1. Designates an AETC office of primary responsibility (OPR) to address all Air Force and DoD CIP requirements established in formal governance.

7.1.2. Develops an AETC capability to monitor, report, and respond during an undesirable event that has impacted or may impact a critical asset's ability to support its linked MET as part of an Air Force-wide, comprehensive and fully integrated CIP effort.

7.1.3. Ensures that all subordinate commanders capture and document decisions made to remediate, mitigate, or accept risk for critical assets. Commanders will document decisions to accept risk to Tier I through Tier III critical assets in AF-CAMS.

### 7.2. HQ AETC/A2/3/10:

7.2.1. Ensures HQ AETC, numbered Air Forces (NAF), wings, and AETC tenant activities have documented and implemented COOP plans that provide the means to continue mission-essential functions during all disruptive events for all Tier I, II, and III assets.

7.2.2. Ensures policies, procedures, and strategies are in place for an effective AETC CIP.

7.2.3. Ensures the formal integration of CIP into all AETC staff processes for mission assurance planning.

7.2.4. Chairs the CIP Executive Committee. (See Section E.)

### 7.3. HQ AETC/A2/30:

7.3.1. Serves as OPR for overseeing implementation of the Air Force CIP. This oversight includes drafting policy guidance, standardized processes and methodologies, plans, and strategic direction for senior leader to review and approve providing the identification, assessment and management of risk of AETC-owned supporting critical assets. (The term *critical asset* encompasses task critical assets (TCA) and supporting infrastructure critical assets (SICA) within CIP.)

7.3.2. Chairs the AETC CIP working group (CIPWG) and participate in related mission assurance activities like the threat working group (TWG), the antiterrorism working group, and other executive-level forums that contribute to the command's ability to achieve mission assurance. (See Section C.)

7.3.3. Serves as the primary AETC CIP point of contact (POC) for coordination of CIP activities with the NAFs, wings, tenant activities on AETC installations, military services hosting AETC tenant activities, and major commands (MAJCOM) to include combatant commands (COCOM), Headquarters Air Force (HAF), DoD, and civil authorities.

7.3.4. Ensures AETC-assigned METs and critical assets are identified, validates NAF and wing critical asset data, and ensures data is entered into AF-CAMS.

7.3.5. Implements Air Force risk-management methodology for AETC to assist in prioritizing assessments and countermeasure options, and guides remediation and mitigation strategies for mission assurance.

- 7.3.6. Annually coordinates AETC nominations for CARAs and vulnerability assessments for Tier I and II critical assets and sends nominations to the HAF CIP OPR.
- 7.3.7. Serves as the OPR for monitoring AETC wing CIP inputs to the DoD Core Vulnerability Assessment Management Program (CVAMP) to include vulnerability identification and risk-management actions and decisions.
- 7.3.8. Supports DoD and Air Force sector characterization initiatives to characterize end-to-end critical infrastructure functionality supporting AETC missions and function.
- 7.3.9. Assists in developing and implementing plans for the assurance of AETC-assigned METs, TCAs, and SICAs.
- 7.3.10. Coordinates AETC monitoring, reporting, and response activities with all HQ AETC infrastructure sector leads.
- 7.3.11. Implements and administers AF-CAMS for HQ AETC, NAFs, wings, and tenant activities.
- 7.3.12. Coordinates higher headquarters training teams, provides training, conducts staff assistance and annual program reviews of NAF, wing, and tenant activities to ensure program compliance. Maintains a process to track and correct observations.
- 7.3.13. Establishes processes and procedures to obtain AETC/CC approval of all Tier I, II, and III critical assets within AETC's area of responsibility. Reviews and validates all Tiers I, II, and III critical asset data supporting execution of NAF, wing, and tenant activity missions, core functions, and capabilities.
- 7.3.14. Provides oversight of standard CIP education, training, and exercises for AETC in accordance with Air Force CIP. Reviews training programs for standardization and effectiveness.
- 7.3.15. Coordinates with NAF and wing CIP representatives to develop a CIP training schedule for Air Force CIP mobile training team support, as needed.
- 7.3.16. Prepares CIP-specific after-action assessments capturing lessons learned and best practices. Incorporates best practices in updates to AETC CIP policy guidance and addresses lessons learned in CIPWG or other relevant forum.
- 7.3.17. Identifies and documents:
- 7.3.17.1. Command remediation and/or mitigation measures to reduce risk of loss to critical assets, and documents those measures in AF-CAMS.
  - 7.3.17.2. Command decisions to accept vulnerabilities and risk to any Tier I, II, and III critical assets. Decisions accepting risk made at all levels of command will be made in writing and documented in AF-CAMS.
- 7.3.18. Oversees the development of operational crisis and consequence management plans to include the development of COOP plans for mission assurance of all Tier I, II, and III assets.
- 7.3.19. Drafts and executes annual AETC CIP strategy as a roadmap to guide command CIP activities to achieve mission-assurance objectives. The standards and conditions used

to measure progress in implementing the strategy should align with the Air Force CARM program standards and benchmarks.

7.3.20. Prepares and presents submissions to the Air Staff in coordination with HQ AETC/A3R on the AETC CIP program in support of the planning, programming, and budgeting and execution process.

#### **7.4. HQ AETC/A1:**

7.4.1. Reviews and validates NAF and wing critical asset data, and adds critical infrastructure to the AETC list of TCAs and SICAs.

7.4.2. Acts as AETC liaison to facilitate coordination with Air Force force support lead agent.

7.4.3. HQ AETC/A1R (Force Support Sector):

7.4.3.1. Serves as the primary AETC CIP personnel sector POC for NAFs, wings, and tenant activities.

7.4.3.2. Provides force support sector subject matter expertise in AETC CIPWG, threat, and executive-level forums for mission assurance.

7.4.3.3. Assists the wings in the development of operational crisis and consequence-management plans to include the development of COOP plans for mission assurance for all Tier I, II, and III assets.

#### **7.5. HQ AETC/A4/7:**

7.5.1. Serves as the primary AETC CIP defense industrial base, logistics, public works, and transportation sector POC for NAFs, wings, and tenant activities.

7.5.2. Reviews, validates NAF and wing critical asset data, and adds critical infrastructure to the AETC list of TCAs and SICAs.

7.5.3. Acts as AETC liaison to facilitate coordination with Air Force defense industrial base, logistics, public works, and transportation sector lead agents.

7.5.4. Provides defense industrial base, logistics, public works, and transportation sector subject matter expertise in AETC CIPWG, threat, and executive level forums for mission assurance.

7.5.5. As a key contributor to force protection and in achieving mission assurance, injects relevant complementary CIP planning and programming activities into the AETC antiterrorism program.

7.5.6. Assists the wings in the development of operational crisis and consequence-management plans to include the development of COOP plans for mission assurance for all Tier I, II, and III assets.

#### **7.6. HQ AETC/A5/8/9:**

7.6.1. Ensures AETC CIP funding and resource requirements are included in the command's program objective memorandum processes and submissions.

7.6.2. Includes critical infrastructure requirements in command long-range plans for new weapons systems beddown, flying and technical training requirements, information systems, and efforts resolving current and future command issues.

7.6.3. Incorporates CIP planning into base realignment and closure (BRAC) process to address risks in consolidating mission critical processes, creating single points of service or failure to achieve mission assurance.

**7.7. HQ AETC/A6:**

7.7.1. Serves as the primary AETC CIP global information grid (GIG) sector POC for NAFs, wings, and tenant activities.

7.7.2. Reviews and validates NAF and wing critical asset data, and adds critical infrastructure to the AETC list of TCAs and SICAs.

7.7.3. Acts as AETC liaison to facilitate coordination with the Air Force GIG sector lead agent.

7.7.4. Identifies and reports any known and postulated threats and hazards (both virtual and physical) to communications systems to HQ AETC/A2/30.

7.7.5. Assesses threats to information systems and recommends changes in the information condition (INFOCON).

7.7.6. Provides GIG sector subject matter expertise in AETC CIPWG, threat, and executive-level forums for mission assurance.

7.7.7. Assists the wings in the development of operational crisis and consequence management plans to include the development of COOP plans for mission assurance for Tier I, II, and III assets.

**7.8. HQ AETC/FM:**

7.8.1. Serves as the primary AETC CIP finance sector POC for NAFs, wings, and tenant activities.

7.8.2. Reviews and validates NAF and wing critical asset data, and adds critical infrastructure to the AETC list of TCAs and SICAs.

7.8.3. Acts as AETC liaison to facilitate coordination with the Air Force finance sector lead agent.

7.8.4. Provides finance sector subject matter expertise in AETC CIPWG, threat, and executive-level forums for mission assurance.

7.8.5. Assists the wings in the development of operational crisis and consequence management plans to include the development of COOP plans for mission assurance for all Tier I, II, and III assets.

**7.9. HQ AETC/SG:**

7.9.1. Serves as the primary AETC CIP health sector POC for NAFs, wings, and tenant activities.

7.9.2. Reviews and validates NAF and wing critical asset data, and adds critical infrastructure to the AETC list of TCAs and SICAs.

7.9.3. Acts as AETC liaison to facilitate coordination with the Air Force health sector lead agent.

7.9.4. Provides health sector subject matter expertise in AETC CIPWG, threat, and executive-level forums for mission assurance.

7.9.5. Assists the wings in the development of operational crisis and consequence management plans to include the development of COOP plans for mission assurance for all Tier I, II, and III assets.

**7.10. HQ AETC/IG:**

7.10.1. Assesses compliance of Air Force and AETC CIP requirements during management and compliance inspections.

7.10.2. Reports to HQ AETC/A2/3/10 operational constraints or infrastructure issues affecting mission assurance discovered during unit compliance inspections.

**8. NAF:**

8.1. Identifies an OPR for matters pertaining to the identification, prioritization, and protection of mission-critical assets and infrastructure. Appoints a CIP officer or POC in writing and provides to the AETC CIP OPR.

8.2. Provides and monitors training, performs program reviews, and supports vulnerability assessments in accordance with this instruction, AFD 10-24, and DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*. Ensures an annual vulnerability and risk self-assessment is completed on all respective wing critical infrastructures. Ensures results of program reviews and assessments are entered in AF-CAMS.

8.3. Ensures CIP is addressed in all operational plans, orders, and exercises to ensure critical capabilities are maintained.

8.4. Ensures respective wings have documented and implemented COOP plans that provide the means to continue mission-essential functions during all disruptive events for all Tier I, II, and III assets.

**9. Host Wing Commander:**

9.1. Establishes a wing CIP to execute Air Force and AETC CIP requirements in order to assure successful execution of wing assigned METs.

9.2. Appoints a CIP officer or POC in writing to implement the wing CIP. While OPR placement of the wing CIP is a wing commander prerogative, CIP is traditionally an operations function at the HAF, MAJCOMs, COCOMs, and Joint Staff to maintain an operational focus on the implications of the loss or degradation in critical assets capabilities. The wing CIP OPR will perform the following CIP activities on behalf of the wing commander:

9.2.1. At least annually, coordinate with all wing-assigned, tenant activities, and commercial entities to identify host critical assets supporting wing and tenant-owned missions.

9.2.2. Annually, authenticate and validate existing data in AF-CAMS. Document any new validated data in AF-CAMS.

9.2.3. Form a CIPWG that includes members from tenant units and subordinate commands residing on or assigned to the host installation.

9.2.4. Participate in and provide substantive input to other force protection-related forums and working groups to represent CIP equities in order to achieve mission assurance.

9.2.5. Ensure all Tier I, II, and III critical assets and supporting infrastructure dependencies are addressed by incorporating those assets into the following planning activities, as a minimum:

9.2.5.1. Physical security, antiterrorism, force protection.

9.2.5.2. COOP plans.

9.2.5.3. Utility restoration priorities and plans.

9.2.5.4. Emergency management, first responder and consequence management priorities and plans.

9.2.6. Execute annual vulnerability and risk self-assessments on all Tier I, II, and III critical assets. These assessments may be executed in conjunction with the annual antiterrorism program self-assessments. Ensure assessment results are entered in AF-CAMS.

9.2.7. Support the execution and conduct of periodic vulnerability and risk assessments by a higher headquarters assessment team. Ensure assessment results are entered in AF-CAMS. **Note:** If a higher headquarters CARA or Joint Staff integrated vulnerability assessment is conducted in a given year, a self-assessment is not needed.

9.2.8. Report changes in status of Tier I, II, and III critical assets within 24 hours in the situational report (SITREP) and operational report (OPREP) notification and in AF-CAMS or as soon as safety precautions allow.

9.2.9. Track and monitor all Tier III and Tier IV critical assets. Enter Tier III critical assets into AF-CAMS as directed.

9.2.10. Conduct annual CIP exercises to validate and verify plans and orders; these exercises may be in conjunction with other complementary exercises (e.g., AT, CBRNE, COOP, IA).

9.2.11. Identify and document:

9.2.11.1. Wing remediation and/or mitigation measures to reduce risk of loss to critical assets, and document those measures in AF-CAMS.

9.2.11.2. Wing decisions to accept vulnerabilities and risk to any Tier I, II, and III critical assets. Decisions accepting risk will be in writing and documented in AF-CAMS.

9.3. Wing commanders will ensure capturing and documenting decisions are made to remediate, mitigate, or accept risk for critical assets. Commanders will document decisions to accept risk to Tier I through Tier III critical assets in AF-CAMS.

## 10. Tenant Activities on AETC Installations:

- 10.1. Coordinate with the host wing CIP OPR to identify tenant critical assets requiring host infrastructure asset support in the execution of the tenant’s missions.
- 10.2. Participate in host CIPWG activities to include critical asset identification, vulnerability and risk assessments, and mitigation and remediation planning for host critical assets supporting tenant-owned missions and critical assets.
- 10.3. Report changes in status of supporting Tier I, II, and III critical assets to wing CIP OPR when degraded status is expected to last more than 24 hours or less if appropriate.
- 10.4. Fully support host installation and AETC CIP management efforts and data calls as well as training and exercise events.

**11. AETC Tenant Activities on Other Military Installations:**

- 11.1. Coordinate with the host or installation commands to identify tenant critical assets requiring host infrastructure asset support in the execution of the tenant’s missions.
- 11.2. Participate in host CIPWG activities to include critical asset identification, vulnerability and risk assessments, and mitigation and remediation planning for host critical assets supporting AETC tenant-owned missions and critical assets.
- 11.3. Report changes in status of Tier I, II, and III critical assets to host CIP OPR when degraded status is expected to last more than 24 hours or less if appropriate. Also, report to respective NAF and HQ AETC/A2/3O within 24 hours in SITREP and OPREP reporting and in AF-CAMS.
- 11.4. Fully support host installation and AETC CIP management efforts and data calls as well as training and exercise events.

*Section C—CIPWG*

**12. Requirements and Contacts.** The CIPWG is a permanent working group to address CIP policies, processes, planning, and execution required for AETC mission assurance. Core working group includes representatives from the ten CIP sectors as defined by Air Force CIP and DCIP. At a minimum, the CIPWG should meet quarterly or more frequently as required.

- 12.1. Each wing will establish a CIPWG comprised of representatives from all functional areas within the wing and other tenant organizations to facilitate decisionmaking regarding CIP issues. This CIPWG may be combined with the AT working group to ensure coordination and reduce administrative burden. CIPWG members should participate in the wing’s antiterrorism working group and complementary mission-assurance activity working groups to share information and support program objectives.
- 12.2. Refer to Table 1 for information on Air Force CIP sector and HQ AETC sector lead assignments:

**Table 1. Air Force CIP Sector and HQ AETC Sector Lead Assignments.**

<b>I T E M</b>	<b>A</b>	<b>B</b>
	<b>CIP Sector (HAF OPR)</b>	<b>Corresponding AETC Sector Leads</b>

1	Defense Industrial Base (HQ USAF/A4/7)	Logistics/Installation and Mission Support (HQ AETC/A4/7)
2	Finance (SAF/FM)	Comptroller (HQ AETC/FM)
3	GIG (SAF/XC)	Communications (HQ AETC/A6)
4	Health (HQ USAF/SG)	Medical Services and Training (HQ AETC/SG)
5	Intelligence, Surveillance, and Reconnaissance (HQ USAF/A3/5)	Directorate of Intelligence, Operations, and Nuclear Integration (HQ AETC/A2/3/10)
6	Logistics (HQ USAF/A4/7)	Logistics/Installation and Mission Support (HQ AETC/A4/7)
7	Personnel (HQ USAF/A1)	Manpower, Personnel, and Services (HQ AETC/A1)
8	Public Works (HQ USAF/A4/7)	Logistics/Installation and Mission Support (HQ AETC/A4/7)
9	Space (HQ USAF/A3/5)	Directorate of Intelligence, Operations and Nuclear Integration (HQ AETC/A2/3/10)
10	Transportation (HQ USAF/A4/7)	Logistics/Installation and Mission Support (HQ AETC/A4/7)

#### *Section D—TWG*

**13. Description and Requirements.** The TWG is a multifunctional team; the working group develops and refines terrorism threat assessments and coordinates and disseminates threat warnings, reports, and summaries.

13.1. It reviews, coordinates, and disseminates threat warnings, reports, and summaries. They should consider terrorist threats and their asymmetrical methods of organization, intelligence, planning, and operations that could pose a threat to the installation or operations in the base boundary and/or base security zone. The TWG also tracks CBRN active defense warnings and intelligence community threat alerts and advisories regarding terrorist groups and analyze the applicability to the installation and its operations.

13.2. Each wing should already have a TWG established to address the current threat. For threats involving critical infrastructure, the CIPWG chair and applicable functional representatives will support mission analysis and course of action to mitigate threats to critical infrastructure in order to achieve mission assurance.

#### *Section E—CIP Executive Committee*

**14. Description and Membership.** The CIP Executive Committee provides oversight for senior director and special staff principals on CIP issues within AETC. As the highest authoritative forum responsible to the AETC/CC, this executive committee evaluates CIP issues and develops a roadmap for remediating systemic critical infrastructure vulnerabilities of the highest risk. It provides AETC a multidisciplinary forum for ensuring the availability of critical infrastructure throughout AETC in assuring assigned missions. Chaired by HQ AETC/A2/3/10, the CIP Executive Committee meets at least annually at Randolph AFB TX. The core members include HQ AETC directors or deputy directors and NAF representatives for CIP at the field officer, general officer, or colonel level and HQ AETC/A2/30.

*Section F—Adopted Forms*

**15. Adopted Form:** AF Form 847, *Recommendation for Change of Publication*

SCOTT BETHEL, Brig Gen, USAF  
Deputy Director, Intelligence, Operations, and  
Nuclear Integration

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, 17 December 2003

Defense Critical Infrastructure Security Classification Guide, May 2007

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

DoDI 3020.45, *Defense Critical Infrastructure Program (DCIP) Management*, 21 April 2008

DoDM 3020.45, Volume 1, *Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP)*, 24 October 2008

DoD 5200.1-R, *Information Security Program*, January 1997

DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*, April 1997

DODD 5230.09, *Clearance of DoD Information for Public Release*, 22 August 2008

AFPD 10-24, *Air Force Critical Infrastructure Program (CIP)*, 28 April 2006

AFI 11-215, *USAF Flight Manuals Program (FMP)*, 22 December 2008

AFMAN 33-363, *Management of Records*, 1 March 2008

***Abbreviations and Acronyms***

**AF—CAMS**—Air Force Critical Asset Management System

**AT**—antiterrorism

**CARA**—critical asset risk assessment

**CARM**—critical asset risk management

**CBRNE**—chemical biological radiological nuclear high explosive

**CC**—commander

**CIP**—critical infrastructure program

**CIPWG**—CIP working group

**COCOM**—combatant command

**COOP**—continuity of operations

**DCI**—defense critical infrastructure

**DCIP**—Defense Critical Infrastructure Program

**GIG**—global information grid

**HAF**—headquarters Air Force

**IA**—information assurance

**MAJCOM**—major command

**MET**—mission-essential task

**NAF**—numbered Air Force

**OPR**—office of primary responsibility

**OPREP**—operational reporting

**POC**—point of contact

**SIA**—supporting infrastructure asset

**SICA**—supporting infrastructure critical asset

**SITREP**—situational reporting

**TCA**—task critical asset

**TWG**—threat working group

### *Terms*

**All—Hazards/Threats Environment**—An environment that includes natural or manmade incidents and events to include acts of terror.

**Analysis and Assessment**—The 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 and infrastructures; and assessment of the operational impact of loss or compromise.

**Asset (Infrastructure)**—A distinguishable network entity that provides a service of capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public or private sector organizations.

**Asset Owner**—The DoD components with responsibility for a DoD asset or organizations that own or operate a non-DoD asset.

**Baseline Elements of Information**—The minimum defined information requirements necessary to support a risk management decision.

**Benchmarks**—For the purpose of this instruction, a series of necessary objectives-based questions for the Defense Critical Infrastructure Program, where the answers indicate the degree to which specific standards have been met.

**Continuity of Operations (COOP)**—An internal effort within individual components of the executive, legislative, and judicial branches of Government assuring the capability exists to continue uninterrupted essential component functions across a wide range of potential emergencies, including localized acts of nature, accidents, and technological and/or attack-related emergencies. COOP involves plans and capabilities that must be maintained at a high level of readiness, and be capable of implementation with or without warning.

**Criticality**—For the purpose of this instruction, a metric used to describe the consequence of loss of an asset, based on the effect the incapacitation or destruction of the asset would have on DoD operations and the ability of the DoD to fulfill its missions.

**Defense Critical Infrastructure**—A TCA of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the DoD to fulfill its missions.

**Defense Critical Infrastructure Program**—A DoD risk management program that seeks to ensure the availability of networked assets critical to DoD missions. Activities include the identification, assessment, and security enhancement of assets essential for executing the national military strategy (DoDD 3020.40).

**Defense Industrial Base (DIB) Defense Sector**—The DoD, the US Government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements.

**Dependency**—A relationship or connection where one entity is influenced or controlled by another entity.

**Global Information System**—The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel including all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority. It also includes national security systems as defined in Section 5142 of the Clinger-Cohen Act of 1996 (DoDD 3020.40).

**Hazard (Infrastructure)**—Nonhostile incidents such as accidents, natural forces, technological failure, etc., that cause loss or damage to infrastructure assets.

**Infrastructure**—The framework of networked assets that comprise identifiable industries, institutions, or distribution capabilities and enable a continued flow of goods and services.

**Mission Assurance**—A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the DoD to carry out the national military strategy. It links numerous risk management program activities and security-related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

**Mission—Essential Tasks**—A mission task selected by a commander deemed essential to mission accomplishment and defined using the common language of the universal joint task list in terms of task, condition, and standard. Differs from a joint MET in that it may reflect missions tasked within a sole DoD component's authority. In DCIP METs are linked to those higher-level responsibilities of the DoD derived from national essential functions, primary mission-essential functions, and mission-essential functions.

**Mission Owner**—DoD organizations having responsibility for the execution of missions assigned by statute or the Secretary of Defense, and supporting organizations with responsibility for execution of all or part of those missions.

**Mitigation**—Actions taken in response to a warning or after an incident occurs intended to lessen the potentially adverse effects on a given military operation or infrastructure.

**National Military Strategy**—It links numerous risk management program activities and security-related functions—such as force protection; antiterrorism; critical infrastructure protection; information assurance; continuity of operations; chemical, biological, radiological, nuclear, and high-explosive defense; readiness; and installation preparedness—to create the synergistic effect required for DoD to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.

**Reconstitution**—The process of restoring critical assets and their necessary infrastructure support systems (or their functionality) to pre-incident operational status.

**Remediation**—Actions taken to correct known deficiencies and weaknesses. These actions are undertaken once a vulnerability has been identified.

**Resiliency**—The characteristic or capability to maintain functionality and structure (or degrade gracefully) in the face of internal and external change.

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

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

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

**Susceptibility**—The inherent capacity of an asset to be affected by one or more threats or hazards.

**Tabular**—Relating to or arranged in a table specifically set up in rows or columns

**Task Critical Asset**—An asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD components or defense infrastructure sector lead agents to execute the task or MET it supports. TCAs are used to identify defense critical assets.

**Threat**—An adversary having the intent, capability, and opportunity to cause loss or damage.

**Tier I Critical Asset**—An asset whose loss, incapacitation, or disruption of which could result in mission (or function) failure at the DoD, military department, combatant command, subunified command, defense agency, or defense infrastructure sector level. More specifically, critical asset loss or disruption results in failure of strategic national- or theater-level missions or functional capabilities.

**Tier II Critical Asset**—An asset whose loss, incapacitation, or disruption could result in severe mission (or function) degradation at the DoD, military department, combatant command, subunified command, defense agency, or defense infrastructure sector level. More specifically, critical asset loss or disruption results in severe degradation of strategic national- or theater-level missions or functional capabilities

**Tier III Critical Asset**—An asset whose loss, incapacitation, or disruption could result in mission (or function) failure or severe degradation below the military department, combatant command, subunified command, defense agency, or defense infrastructure sector level. More specifically, critical asset loss or disruption results in failure or severe degradation of operational level missions or functional capabilities.

**Tier IV Critical Asset**—An asset whose loss, incapacitation, or disruption could result in mission (or function) failure or severe degradation below the military department, combatant command, subunified command, defense agency, or defense infrastructure sector level. More specifically, the critical asset loss or disruption results in failure or severe degradation of unit- or *tactical*- level of missions.

**Vulnerability (Infrastructure)**—The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

**Vulnerability Assessment (Infrastructure)**—A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities.

## Attachment 2

### CHARTER FOR AETC CRITICAL INFRASTRUCTURE PROGRAM WORKING GROUP (CIPWG)

**A2.1. Establishment.** The chartering authority of the AETC Commander establishes the AETC CIPWG, under the chair of the Directorate of Intelligence, Operations, and Nuclear Integration (HQ AETC/A2/3/10). This charter contains the following general responsibilities:

A2.1.1. Identify and address CIP issues.

A2.1.2. Advise AETC senior leadership on DoD, Air Force, and AETC CIP policies and issues.

A2.1.3. Foster awareness of CIP within AETC by providing a context and forum for collaboration on CIP issues.

A2.1.4. Provide a common management environment for planning, coordinating, integrating, and administering all AETC CIP efforts.

A2.1.5. Develop positions and policy recommendations for submission to the formal coordination process.

#### **A2.2. CIPWG Objectives:**

A2.2.1. Serve as the principal, working-level, advisory forum for developing and providing AETC CIP policy, programs, and oversight recommendations to HQ AETC/A2/3/10.

A2.2.2. Assist the US Air Force POC (AF/A3O-AHD) by:

A2.2.2.1. Monitoring activities relating to overall Air Force CIP planning, program development, and execution.

A2.2.2.2. Supporting and leveraging Air Force CIP-related programs.

A2.2.2.3. Ensuring CIP policies and standards are integrated into all appropriate policy guidance.

A2.2.3. Develop AETC CIP functional objectives, as well as processes, definitions, critical asset criteria, and data collection methodology to:

A2.2.3.1. Support the assessment of risks to AETC missions and capabilities.

A2.2.3.2. Provide situational awareness of critical infrastructure asset availability and reliability.

A2.2.3.3. Support consequence management and continuity of operations decisions.

A2.2.4. Provide a forum for the AETC CIP community to vet CIP-related policies and procedures, raise CIP-related issues, share information of mutual interest, and informally coordinate issues and recommendations among the members prior to formal staffing.

A2.2.5. Identify and prioritize critical AETC-owned and/or managed infrastructures and assess their vulnerability to human error, natural disasters, or intentional physical or cyber attack. Develop strategies for remediating or mitigating vulnerabilities to critical infrastructure.

A2.2.6. In case of loss or disruption to a critical infrastructure, develop strategies for mitigating the effects of such loss or disruption and include them in COOP plans.

A2.2.7. Incorporate CIP education and training concepts into AETC Command-level courses as well as courses for senior staff (military and civilian) and senior enlisted personnel.

A2.2.8. Incorporate CIP concepts into AETC 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 so that lessons learned are applied to remediate such vulnerabilities.

### **A2.3. Organization:**

A2.3.1. HQ AETC/A2/3O, or designee, will chair the CIPWG. He or she will:

A2.3.1.1. Act as the OPR for identification, assessment, and security enhancement of the AETC CIP.

A2.3.1.2. Provide direction to the CIPWG to facilitate execution of its assigned CIP responsibilities.

A2.3.1.3. Participate in the Air Force CIPWG.

A2.3.1.4. Represent AETC in CIP-related discussions and agreements with HAF.

A2.3.1.5. Prepare and present submissions to the Air Staff in coordination with HQ AETC/A3R on the AETC CIP program in support of the planning, programming, and budgeting and execution process.

A2.3.1.6. Oversee the AETC CIP-related training and awareness programs.

A2.3.1.7. Establish and oversee a staff to maintain and administer the AETC CIP program.

A2.3.1.8. Implement policies and establish procedures, plans, and operations to reduce the vulnerabilities of critical AETC infrastructures and assets.

A2.3.1.9. Coordinate with the Air Force sector leads on the identification, vulnerability assessment, and remediation of the loss or degradation of DCI supporting AETC and its impact on the Air Force mission.

A2.3.2. The executive agent for the AETC CIP is the Deputy Chief, Intelligence, Operations, and Readiness Division, HQ AETC/A2/3O, who is responsible for:

A2.3.2.1. Developing and maintaining an AETC CIP strategy, defining goals and performance objectives, and establishing timelines.

A2.3.2.2. Coordinating the activity and participation of the AETC CIPWG members as well as invited guests.

A2.3.2.3. Maintaining oversight of CIPWG operations and administration such as scheduling meetings and maintaining minutes.

A2.3.2.4. Ensuring all participants remain informed of related functional group's activities in order to examine consequences and adjust action plans accordingly.

A2.3.2.5. Establishing and coordinating AETC positions on CIP issues for AETC CIPWG consideration.

A2.3.2.6. Establishing and maintaining liaison with Air Force and MAJCOM CIP POCs.

A2.3.2.7. Supporting HQ USAF/A3SHD as required.

#### **A2.4. Membership:**

A2.4.1. AETC representatives from the following directorates are responsible for bringing directorate issues to the attention of the CIPWG: A1, A2/3/10, A4/7, A5/8/9, A6, RS, SG, and FM.

A2.4.2. The directorates identified in paragraph A2.4.1 will appoint and maintain primary and alternate representatives to serve as members on the CIPWG. Provide their names and contact information to HQ AETC/A2/30, DSN 487-7833. At least one of these representatives is expected to attend all CIPWG meetings.

A2.4.3. Additional permanent members are encouraged from divisions with multiple missions.

A2.4.4. The Chair, upon advice of the members, may add additional members as required. Appropriate subject matter experts will be invited to participate as deemed necessary by the CIPWG.

A2.4.5. When necessary, the Chair may establish subgroups to address topics of special CIP interest.

#### **A2.5. Relationships with Other Organizations:**

A2.5.1. The AETC CIPWG will serve as the primary AETC forum responsible for coordination of AETC CIP activities with all CIP and CIP-related organizations.

A2.5.2. The AETC CIPWG is responsible for the development of CIP issues and recommendations to ensure they are properly framed prior to final staffing actions.

A2.5.3. Tasking authority is delegated to HQ AETC/A2/30 via this charter for all CIP related issues. This authority extends over all AETC divisions.

#### **A2.6. Meetings:**

A2.6.1. Minutes and Agendas:

A2.6.1.1. The CIPWG will meet at least quarterly as determined by the Chair, his or her designee, or by request of the membership.

A2.6.1.2. HQ AETC/A2/30 will announce meetings, request agenda items, and provide an agenda for each regularly scheduled CIPWG.

A2.6.1.3. The CIPWG agenda will include recurring items, such as the review and approval of previous minutes, prioritization of assets, review of new missions and assets, and discussion of agenda items for the next CIPWG meeting.

A2.6.1.4. Members may nominate additional missions, assets, and issues for consideration.

A2.6.1.5. Members nominating agenda items will provide supporting documentation to HQ AETC/A2/30 at least 24 hours prior to the meeting as appropriate.

A2.6.1.6. HQ AETC/A2/30 will generate and distribute minutes not later than 5 working days after each meeting.

**A2.6.2. Meeting Management:**

A2.6.2.1. Representatives attending each meeting are expected to represent their organization's position on CIPWG matters.

A2.6.2.2. The CIPWG will address each issue on the agenda with the intent to agree upon a position based on consensus.

**A2.6.3. Unresolved Issues.** Issues not resolved by the CIPWG will be referred to HQ AETC/A2/30 or A2/3/10 for a final decision.

A2.6.3.1. When consensus on an issue is not achieved at a CIPWG, dissenting parties will develop position papers for review by HQ AETC/A2/30.

A2.6.3.2. HQ AETC/A2/30 will prepare appropriate staff correspondence with recommendations for each unresolved agenda item based on position papers prepared by CIPWG representatives. All such correspondence will be coordinated with CIPWG members prior to being sent to HQ AETC/A2/3/10.

**A2.6.4. Operations Security, Communications Security, and Information Security.** Use appropriate guidelines when developing and transmitting information that identifies critical infrastructures, threats, vulnerabilities, risks, and recommended responses. This information will be marked a minimum of "For Official Use Only" since it identifies AETC mission-critical information.

A2.6.4.1. **Classification Guidance.** The Defense Critical Infrastructure Security Classification Guide (hereafter referred to as the DCIP SCG), May 2007, is the primary source for classification guidance. It will be cited as the basis for classification, reclassification, and declassification of information and materials under DoD cognizance and control related to CIP. Refer to other classification guidance such as original classification authority (OCA) or original agency's determination required (OADR) for specific classification information, for specific classification information.

A2.6.4.2. **Compiled Information.** See DoD 5200.1-R, *Information Security Program*, for guidance on compiled information, such as when information otherwise marked UNCLASSIFIED could become classified if the compiled information reveals an additional association or relationship.

A2.6.4.3. **Public Release.** Unclassified CIP information is not automatically releasable to the public. See the DCIP SCG and DoDD 5230.09, *Clearance of DoD Information for Public Release*, for details.

A2.6.4.4. **Marking Requirements.** See DCIP SCG and DoD 5200.1-PH, *DoD Guide to Marking Classified Documents*.

**A2.7. Duration.** This charter will be reviewed annually during the first quarter of the fiscal year or more frequently as required.

**A2.8. Effective Date.** This charter is effective upon signature by the Commander, Air Education Training Command.