

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400
APO AE 09131-0400

DIRECTIVE
NUMBER 56-26

24 April 2003

PLANS AND POLICY

USEUCOM Critical Infrastructure Protection (CIP) Program

1. **Summary.** This directive establishes policy; assigns duties and responsibilities; and provides guidance for planning, developing and executing USEUCOM's Critical Infrastructure Protection (CIP) Program.
2. **Applicability.** This Directive is a USEUCOM publication that applies to all USEUCOM Subordinate Commands and Staff Directorates. It also applies to all agencies or activities supporting or associated with USEUCOM.
3. **Internal Control Systems.** This Directive does not contain internal control provisions and is not subject to the requirements of the internal management control program. For USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program.
4. **Suggested Improvements.** The proponent for this Directive is the Director, USEUCOM Plans and Policy (ECJ5). If you have any recommended changes, forward them to ECJ5 Strategy, Resources, and Legislative Affairs Division (ECJ5-S).
5. **References.**
 - a. Presidential Decision Directive 63, "Critical Infrastructure Protection," 22 May 1998.
 - b. "National Plan for Information Systems Protection," January 2000.
 - c. "The DoD Critical Infrastructure Protection (CIP) Plan," 18 November 1998.
 - d. DoD Directive 3020, "Critical Infrastructure Protection Program," (Draft).
 - e. DoD Instruction 3020, "Implementation of the Critical Infrastructure Protection Program," (Draft).
 - f. DoD Directive 8590.1 (formerly 5160.54), "Critical Infrastructure Protection," (draft 10 July 2001).
 - g. JCS msg 110940Z May 1999, Interim Guidance to CJCSI 3110.01, Joint Strategic Capabilities.
 - h. CJCSI 3209.01 (9 July 2002), "Critical Infrastructure Protection," (Draft).

6. **Explanation of Terms.** See references (b), (d), and (e).

7. **General.** CIP is Mission Assurance. It is the identification, assessment and assurance of cyber and physical mission critical capabilities and requirements, to include the political, economic, technological, and information security environments essential to the execution of the National Military Strategy (NMS). It encompasses the infrastructure necessary for deterrence operations and those essential to plan, mobilize, deploy, and sustain military operations, and transition to post conflict operations. Involved infrastructures may be DoD-owned or belong to other U.S. Government agencies, commercial or private sector entities. Additionally, infrastructure may be owned and controlled by foreign commercial, private sector, and/or host nation organizations and governments. (Joint Staff Definition)

Military mission success depends upon the readiness, availability, reliability, and sustainability of military forces. The successful training, equipping, deployment and support of these forces are dependent upon critical supporting infrastructures. CIP ensures that infrastructure assets required to execute operational missions and essential functions are available when needed. CIP supports the full range of military operations, and extends beyond the immediate theater of operations to protect reach-back and key supporting capabilities.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. At the national level, these sectors of the economy are managed by lead agencies (departments) as appointed by the President (PDD 63).

The Department of Defense, the Joint Staff, and HQ USEUCOM have developed and identified their own sectors as indicated below:

	Joint Staff/DoD Defense Sectors	DoD Lead	JS Lead	USEUCOM Lead
1.	Financial Services	DFAS	JSJ1	ECCM
2.	Transportation	TRANSCOM	JSJ4	ECJ4
3.	Public Works	USACE	JSJ4	ECJ4
4.	Defense Information Infrastructure (DII)	DISA	JSJ3 & JSJ6	ECJ6 (for DII and Comm.)
	Command, Control, and Communications (C3)			ECJ3 (for C2 only)
5.	Intelligence, Surveillance, & Reconnaissance (ISR)	DIA	JSJ2	ECJ2
6.	Health Affairs	OASD	JSJ1	ECJ4-MR
7.	Personnel	DHRA	JSJ1	ECJ1
8.	Space	STRATCOM	JSJ3	ECJ3

Joint Staff/DoD Defense Sectors		DoD Lead	JS Lead	USEUCOM Lead
9.	Logistics	DLA	JSJ4	ECJ4

8. **Responsibilities.** Following are the responsibilities of USEUCOM Subordinate Commands and Staff Directorates.

a. ECJ5.

- (1) Serve as the office of primary responsibility for the USEUCOM CIP program.
- (2) Organize and chair the USEUCOM CIP Council.
- (3) Integrate CIP into deliberate planning by completing Appendix 16 (CIP) to Annex C for all plans and, in coordination with ECJ3, ensure CIP is integrated into crisis action planning.
- (4) Assist USEUCOM Subordinate Commands to develop and implement their CIP programs.
- (5) Provide USEUCOM Subordinate Commands with guidance and direction required to complete an Appendix 16 (CIP) to Annex C for all supporting plans.
- (6) Conduct strategic analysis and assessment of USEUCOM's CIP capability as directed by the Joint Requirements Oversight Council (JROC).
- (7) As part of JROC; Joint Warfighting Capabilities Assessment (JWCA); Planning, Programming, and Budgeting System (PPBS); and Integrated Priority List (IPL); review the adequacy of resourcing proposed by the Services to support USEUCOM Subordinate Commands' CIP efforts.
- (8) Coordinate all Joint Strategic Capabilities Plan (JSCP) deliberate planning matters related to CIP with ECJ3.
- (9) Ensure that the review of JSCP-tasked deliberate plans includes a review of CIP issues by the Joint Planning and Execution Community (JPEC).
- (10) Ensure CIP assessments are coordinated with AT/FP and other installation assessments.
- (11) Coordinate with ECJ3 to ensure that disruption and loss of critical infrastructure, to include supporting host nation infrastructures, are scripted and responded to in joint exercises.

b. ECJ1.

(1) Serve as USEUCOM lead for the Personnel infrastructure sector and as the primary POC to interface with the Personnel Sector lead (JSJ1) to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plan for the Personnel infrastructure sector.

(3) Provide a representative to the USEUCOM CIP Council.

c. ECJ2.

(1) Serve as USEUCOM lead for the Intelligence, Surveillance, and Reconnaissance (ISR) infrastructure sector; and as the primary POC to interface with the DoD ISR Sector lead (JSJ2/DIA) to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plan for the ISR infrastructure sector.

(3) Provide a representative to the USEUCOM CIP Council.

(4) Coordinate Subordinate Command counterintelligence activity in support of the CIP Program.

d. ECJ3.

(1) Serve as USEUCOM lead for the C2 and Space infrastructure sectors and as the primary POC to interface with the DoD C2 (JSJ3/JSJ6/DISA) and Space (JSJ3/STRATCOM) Sector leads to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plans for the C2 and Space infrastructure sector.

(3) Coordinate with ECJ5 to ensure CIP is fully integrated into the deliberate and the crisis action planning process.

(4) Integrate CIP performance measures into the readiness reporting system for periodic submission by the USEUCOM Subordinate Commands to the Joint Quarterly Readiness Review (JQRR).

(5) Ensure that disruption and loss of Critical Infrastructure, to include supporting host nation infrastructures, are scripted and responded to in Joint Exercises.

(6) Provide a representative to the USEUCOM CIP Council.

e. ECJ4.

(1) Serve as USEUCOM lead for the Transportation, Public Works, Health Affairs, and Logistics infrastructure sectors; and as primary POC to interface with the DoD Transportation Sector lead (JSJ4/TRANSCOM), Public Works Sector lead (JSJ4/USACE), Health Affairs Sector lead (JSJ4/OASD, Health Affairs), and Logistics Sector lead (JSJ4/DLA), to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plans for the Transportation, Public Works, Health Affairs, and Logistics infrastructure sectors.

(3) Provide a representative to the USEUCOM CIP Council.

f. ECJ6.

(1) Serve as USEUCOM lead for the DII sector (to include Communications) and as primary POC with the DII Sector lead (JSJ6/DISA) to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plan for the DII sector (to include Communications).

(3) Serve as primary POC to interface with USEUCOM Subordinate Commands, host nation agencies, the Defense-wide Information Assurance Program (DIAP), and other Information Assurance specific advisory groups to facilitate the comprehensive integration of Information Assurance and Network Operations into the USEUCOM CIP program.

(4) Provide a representative to the USEUCOM CIP Council.

(5) Coordinate all USEUCOM Information Assurance (IA) activities related to CIP.

g. ECSM.

(1) Assist USEUCOM Subordinate Commands and Staff Directorates to determine vulnerabilities of critical infrastructure to acts of terrorism (minus cyber-terrorism), and to develop vulnerability, remediation, and mitigation plans and procedures.

(2) Coordinate all Antiterrorism/Force Protection (AT/FP) assessments conducted by HQ USEUCOM and Joint Staff Integrated Vulnerability Assessments through ECJ5 to ensure coordination and integration with CIP assessments.

(3) Provide a representative to the USEUCOM CIP Council.

h. ECCM.

(1) Serve as USEUCOM lead for the Financial Services infrastructure sector and as the primary POC to interface with the Financial Services Sectors lead (JSJ1/DFAS) to facilitate coordination between the USEUCOM Subordinate Commands, Staff Directorates, and the Joint Staff.

(2) Publish and maintain the USEUCOM Sector Assurance plan for the Financial Services infrastructure sector.

(3) Provide a representative to the USEUCOM CIP Council.

i. COMUSEUCOM Subordinate Commanders.

(1) Establish a CIP Program to meet National, DoD, and USEUCOM CIP requirements.

(2) Provide support to HQ USEUCOM required to complete Appendix 16 (CIP) to Annex C for USEUCOM plans.

(3) Complete Appendix 16 (CIP) to Annex C for all supporting plans to COMUSEUCOM plans, as required.

(4) Integrate CIP into Joint and Service exercises.

(5) Establish the capability to monitor, report, and respond as part of a defense-wide, comprehensive, and fully integrated CIP effort.

(6) Provide annually, as part of the PPBS cycle, a COMUSEUCOM Subordinate Commanders' assessment of the adequacy of the proposed resources to meet respective command CIP requirements.

(7) COMUSEUCOM Subordinate Commands are invited, but not required, to provide a representative to the USEUCOM CIP Council.

9. Policies and Procedures.

a. Policies.

(1) Policy References. Policies and procedures for USEUCOM's CIP program are derived from Presidential Decision Directive 63, DoD Directive 8590.1, DoD Directive 3020 (Draft), DoD Instruction 3020 (Draft), and CJCSI 3209.01 (Draft).

(2) DoD Policy. The Joint Staff, in coordination with the Unified Combatant Commands and Services, will: develop CIP policies and guidance; provide oversight, expertise, and requirements management; and be a proponent for CIP in the Joint Community and with the DoD CIP Program. The complex nature of the challenge posed by critical infrastructure inter-dependencies requires full integration across all elements of the Joint Staff.

(3) USEUCOM Policy. USEUCOM Subordinate Commands and Staff Directorates shall comply with this Directive and accurately and effectively support the programs and policies listed in the above references.

b. Procedures.

(1) USEUCOM's CIP Program will focus on eliminating significant vulnerabilities to both physical and cyber attacks on critical infrastructures.

(2) For each of the DoD defense infrastructure sectors, there is a designated corresponding USEUCOM Staff Directorate. These Directorates will further appoint a lead action officer to serve as the USEUCOM Defense Sector Liaison Official to address CIP issues associated with that sector.

(3) ECJ5 will chair the USEUCOM CIP Council. The Council will consist of all USEUCOM Defense Sector Liaison Officials, as identified in Directorate Responsibilities above. The CIP council will meet periodically to review, plan, prepare, and respond to CIP issues and requirements within the USEUCOM AOR.

(4) All CIP resource requirements will be submitted to: ECJ5 via the JWCA/JROC process (see ED-56-20); ECJ5 via the IPL process (see ED 56-20 and ED 56-17); or ECJ3 via the Joint Quarterly Readiness Review (JQRR) process.

FOR THE COMMANDER:

OFFICIAL:

JOHN B. SYLVESTER
Lieutenant General, USA
Chief of Staff

RICKEY K. WILLIAMS
LTC, USA
Adjutant General

DISTRIBUTION:

P