



# Department of Defense INSTRUCTION

NUMBER 3020.51

June 23, 2011

---

---

USD(I)

**SUBJECT:** Intelligence Support to the Defense Critical Infrastructure Program (DCIP)

**References:** See Enclosure 1

1. **PURPOSE.** In accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)) and pursuant to DoDD 3020.40 and DoD Instruction (DoDI) 3020.45 (References (b) and (c)), this Instruction establishes policy, assigns responsibilities, and prescribes procedures for intelligence support to the DCIP.

2. **APPLICABILITY.** This Instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the “DoD Components”).

3. **DEFINITIONS.** See Glossary.

4. **POLICY.** It is DoD policy that:

a. The Defense Intelligence Enterprise (hereinafter referred to in this Instruction as “the Enterprise”) shall provide timely intelligence and counterintelligence support to the DCIP. Responsibilities and procedures for counterintelligence support to the DCIP shall be executed in accordance with DoDI 5240.19 (Reference (d)).

b. Intelligence collection, processing, retention, and dissemination in support of the DCIP efforts shall be conducted in accordance with the National Intelligence Priorities Framework pursuant to Intelligence Community Directive (ICD) 204 (Reference (e)).

c. DCIP-related threat assessments will be produced at the lowest possible classification level and made accessible to all DoD Components and DISLAs through existing Enterprise processes, procedures, systems, and architectures to the greatest extent possible.

d. DCIP-related threat assessments shall be shared with other Defense Intelligence and Counterintelligence Components, the national Intelligence Community (IC), other relevant Federal agencies, and civilian law enforcement officials, as appropriate, in accordance with the need to protect intelligence sources and methods and with the provisions of Director of Central Intelligence Directive 8/1 (Reference (f)) and ICD 501 (Reference (g)). All sharing of information, data, research, and analysis shall adhere to the requirements and restrictions imposed by DoD 5400.11-R (Reference (h)), DoD 5240.1-R (Reference (i)), all other applicable DoD policies, Federal law, Presidential directives, Executive orders, and Director of National Intelligence (DNI) issuances.

e. All intelligence and intelligence-related activities in support of the DCIP shall adhere to Federal law, Presidential directives, Executive orders, and DNI and DoD policies. DoD personnel shall conduct authorized intelligence and intelligence-related activities in a manner that protects the privacy and civil liberties of U.S. persons. All intelligence and intelligence-related activities supporting the DCIP shall conform to DoDD 5240.01 (Reference (j)) and References (i) and (h).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

8. EFFECTIVE DATE. This Instruction is effective upon its publication to the DoD Issuances Website.



Michael G. Vickers  
Under Secretary of Defense  
for Intelligence

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),  
November 23, 2005
- (b) DoD Directive 3020.40, "DoD Policy and Responsibilities for Critical Infrastructure,"  
January 14, 2010
- (c) DoD Instruction 3020.45, "Defense Critical Infrastructure Program (DCIP) Management,"  
April 21, 2008
- (d) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical  
Infrastructure Program," August 27, 2007
- (e) Intelligence Community Directive 204, "Roles and Responsibilities for the National  
Intelligence Priorities Framework," September 13, 2007
- (f) Director of Central Intelligence Directive 8/1, "Intelligence Community Policy on  
Intelligence Information Sharing," June 4, 2004
- (g) Intelligence Community Directive 501, "Discovery and Dissemination or Retrieval of  
Information Within the Intelligence Community," January 21, 2009
- (h) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (i) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components  
That Affect United States Persons," December 1982
- (j) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
- (k) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," March 18, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I), pursuant to References (a), (b), and (c), shall:

- a. Establish policy for intelligence support to the DCIP.
- b. Oversee policies, plans, and programs, to include policies and issuances of DoD Components, for intelligence support to the DCIP.
- c. Oversee implementation of this Instruction and develop additional direction and guidance as necessary to provide intelligence support to the DCIP.

2. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, pursuant to DoDD 5105.21 (Reference (k)), under the authority, direction, and control of the USD(I), and in addition to the responsibilities in sections 9 and 10 of this enclosure, shall:

a. Pursuant to Reference (b), appoint the Critical Infrastructure Assurance Officer (CIAO) for the Defense Infrastructure Intelligence Sector, under the authority of the Director, DIA, to be the primary intelligence advisor for the DCIP. In this capacity, the Intelligence Sector CIAO shall:

(1) Plan, integrate, coordinate, direct, synchronize, and manage intelligence support to the DCIP.

(2) Represent the intelligence interests and equities of, and provide intelligence support to, the CIAOs of the Defense Infrastructure Defense Industrial Base (DIB), Financial Services, Health Affairs, and Personnel Sectors in all matters pertaining to the implementation and execution of this Instruction.

b. Establish and chair the DCIP intelligence working group (IWG). (See Enclosure 3.)

c. Pursuant to U.S. laws and DoD issuances, and within the legal authority granted to the DoD and subject to limitations on collection, retention, and dissemination of information on U.S. persons, coordinate with other appropriate Federal agencies, such as the Department of Homeland Security, regarding intelligence matters on defense critical infrastructure (DCI), in accordance with References (c), (h), (i), and (j).

d. Triennially, or more frequently if required, and in accordance with the Director, DIA's all-source intelligence analysis responsibilities produce or direct the production of a global baseline assessment of the threats to DCI that address, at a minimum, those topic areas identified in paragraph 2.a of Enclosure 3 and subject to Under Secretary of Defense for Policy (USD(P))

priorities. Ensure triennial updates capture all relevant intelligence collected or produced since the previous assessment. Make this assessment accessible to all DoD Components and DISLAs via existing intelligence channels. Where such channels do not exist, the assessments will be disseminated under the provisions of subparagraph 2.a.(2) of this enclosure.

e. Within 90 days of the publication of a triennial DCIP threat assessment, identify all knowledge gaps and consolidate into a single DCIP intelligence collection requirement. Collection will be conducted in accordance with priorities established by the National Intelligence Priorities Framework.

f. Produce, triennially or more frequently if required, a defense critical infrastructure threat assessment (DCITA) for each defense critical asset (DCA) addressing, at a minimum, the topics identified in section 4 of Enclosure 3. Where multiple DCAs are collocated on a single installation, a single installation baseline threat assessment may be produced, provided individual differences from the baseline are identified for each DCA, as appropriate. Completed assessments will be provided to the appropriate Military Department, Defense Agency, or DISLA and the Office of the USD(P).

g. Within 90 days of the production of a DCITA for a DCA, identify all knowledge gaps for consolidation into a single DCIP intelligence collection requirement. Collection will be conducted in accordance with priorities established by the National Intelligence Priorities Framework.

h. In response to a validated requirement for ad-hoc finished intelligence production, prepare or task the appropriate producer to prepare a finished intelligence assessment in response to the requirement. Ensure that the major findings of this assessment are incorporated into all subsequent triennial updates, as appropriate.

i. Annually, or more frequently as required, issue a standing, all-source collection requirement to address the intelligence gaps identified by DoD Components, DISLAs, and intelligence production elements.

3. USD(P). The USD(P) shall:

a. Provide a representative in observer status to the DCIP IWG.

b. Annually, or more frequently if required, provide the Director, DIA, through the USD(I), a statement of DoD priority intelligence requirements (PIRs) in support of the DCIP.

c. Consolidate DoD Component and DISLA requirements for ad-hoc intelligence production related to critical infrastructure responsibilities and provide them to the Director, DIA, through the USD(I).

d. Advise the Director, DIA, of policy, program, or process changes in the DCIP that may affect intelligence support.

e. Annually, or more frequently as required, provide the approved DCA list to the Director, DIA, through the USD(I). This list shall be used for prioritizing intelligence support to the DCIP, subject to USD(P) priorities.

f. In coordination with the USD(I), the Military Departments, and the CJCS, using existing communications channels, assess and recommend improvements to ensure the timely dissemination of DCI-related threat warnings to DoD Components, DISLAs, and other authorized activities as appropriate.

g. In coordination with the USD(I), advise the Director, DIA, of policy, program, or process changes in the Defense Infrastructure Space Sector that may affect intelligence support.

4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). The USD(AT&L), in coordination with the USD(I), shall advise the Director, DIA, of policy, program, process, or operational changes in the DIB, logistics, public works, or transportation infrastructures that may affect intelligence support.

5. DIRECTOR, DEFENSE LOGISTICS AGENCY (DLA). The Director, DLA, under the authority, direction, and control of the USD(AT&L) and in addition to the responsibilities in sections 9 and 10 of this enclosure, shall, through DLA's internal intelligence element, provide intelligence support to the CIAO of the Defense Infrastructure Logistics Sector.

6. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R), in coordination with the USD(I), shall advise the Director, DIA, of policy, program, process, or operational changes in the health affairs or personnel infrastructures that may affect intelligence support.

7. UNDER SECRETARY OF DEFENSE (COMPTROLLER) (USD(C))/CHIEF FINANCIAL OFFICER (CFO), DEPARTMENT OF DEFENSE. The USD(C)/CFO, in coordination with the USD(I), shall advise the Director, DIA, of policy, program, process, or operational changes in the financial services infrastructure that may affect intelligence support.

8. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in coordination with the USD(I), shall advise the Director, DIA, of policy, program, process, or operational changes in the DoD information enterprise, which includes Global Information Grid (GIG) infrastructures that may affect intelligence support.

9. HEADS OF THE DoD COMPONENTS AND DISLAs. The Heads of the DoD Components and DISLAs, in support of their assigned critical infrastructure responsibilities, shall identify subjects for which ad-hoc intelligence production is required. They shall provide such requirements to the USD(P) through appropriate reporting channels.

10. SECRETARIES OF THE MILITARY DEPARTMENTS AND DIRECTORS OF DEFENSE AGENCIES, AND DoD FIELD ACTIVITIES. Secretaries of the Military Departments and Directors of Defense Agencies, and DoD Field Activities, in addition to the responsibilities in section 9 of this enclosure, shall:

- a. Designate an office of primary responsibility (OPR) within their intelligence component to coordinate DCIP-related intelligence activities.
- b. Provide representational membership to the DCIP IWG. (See Enclosure 3.)
- c. Provide PIRs related to warnings of impending threats to DCI to their organic or supporting intelligence element watch center. These PIRs shall be provided annually, or more frequently as required, in conjunction with the most recent internal list of DCI.
- d. Ensure staff elements responsible for critical infrastructure share DCI-related threats, indications, and warnings with the appropriate members of the DCIP community.

11. SECRETARY OF THE ARMY. The Secretary of the Army, in addition to the responsibilities in sections 9 and 10 of this enclosure, shall direct the Commander, U.S. Army Corps of Engineers (USACE) to provide intelligence support, through USACE's internal intelligence element, to the CIAO of the Defense Infrastructure Public Works Sector.

12. CJCS. The CJCS, in addition to the responsibilities in section 9 of this enclosure, shall:

- a. Integrate intelligence support to the DCIP into joint planning, programs, systems, exercises, doctrine, strategies, policies, and architectures.
- b. Incorporate DCIP-related threat scenarios requiring coordination with intelligence elements into joint training and exercises.

13. COMMANDERS OF THE CCMDs. The Commanders of the CCMDs, through the CJCS as appropriate, and in addition to the responsibilities in section 9 of this enclosure, shall:

- a. Designate an OPR within their intelligence component to coordinate DCIP-related intelligence activities.
- b. Provide representational membership to the DCIP IWG. (See Enclosure 3.)

c. Ensure that staff elements and components responsible for critical infrastructure share DCI-related threats, indications, and warnings with the appropriate members of the DCIP community.

d. Incorporate DCIP-related threat scenarios requiring coordination with intelligence elements into joint training and exercises.

14. COMMANDERS OF THE GEOGRAPHIC CCMDs. The Commanders of the Geographic CCMDs, through the CJCS as appropriate, and in addition to the responsibilities in sections 9 and 13 of this enclosure, shall:

a. Triennially or more frequently if required, and in accordance with the Defense Intelligence Analysis Program, produce an area of responsibility (AOR)-specific supplement to the DIA-produced, global baseline assessment of the threats to DCI that addresses, at a minimum, those topic areas identified in paragraph 3.a. of Enclosure 3, subject to the USD(P) priorities. Ensure triennial updates capture all relevant intelligence collected or produced since the previous supplement. Make these supplements accessible to all DoD Components and DISLAs via existing intelligence channels. Where such channels do not exist, they will be disseminated under the provisions of subparagraph 2.a.(2) of this enclosure.

b. Within 90 days of the publication of the triennial, AOR-specific DCIP threat assessment supplement, identify all existing knowledge gaps and forward to the Director, DIA, for consolidation into a single DCIP intelligence collection requirement.

c. Address intelligence requirements and production responsibilities pertinent to critical infrastructure-related responsibilities in the intelligence support plan for their respective theater campaign plans.

d. Identify PIRs related to warnings of impending threats to DCI within their respective AORs, and ensure these PIRs are provided to their organic intelligence element watch center. These PIRs shall be provided annually, or more frequently as required, in conjunction with the most recent internal list of DCI.

15. COMMANDER, U.S. STRATEGIC COMMAND (USSTRATCOM). The Commander, USSTRATCOM, in addition to the responsibilities in sections 9 and 13 of this enclosure, shall:

a. Through USSTRATCOM's internal intelligence element, provide intelligence support to the CIAO of the Defense Infrastructure Space Sector.

b. Direct the Commander, U.S. Cyber Command (USCYBERCOM), to provide, through USCYBERCOM's internal intelligence element, intelligence support to the CIAO of the Defense Infrastructure GIG Sector and Defense Information Systems Agency.



16. COMMANDER, U.S. TRANSPORTATION COMMAND (USTRANSCOM). The Commander, USTRANSCOM, in addition to the responsibilities in sections 9 and 13 of this enclosure, shall, through USTRANSCOM's internal intelligence element, provide intelligence support to the CIAO of the Defense Infrastructure Transportation Sector.

ENCLOSURE 3

PROCEDURES

1. DCIP IWG

a. The DCIP IWG shall consist of an executive steering panel and an action officer panel with membership consisting of military members or full-time or permanent part-time civilian employees.

(1) The executive steering panel shall consist of those general or flag officers or their equivalents appointed by the Secretaries of the Military Departments, the Directors of Defense Agencies and DoD Field Activities, and the Commanders of the CCMDs.

(2) The action officer panel shall consist of those representatives within the Enterprise and the internal intelligence elements of the CCMDs, the Military Departments, the Defense Agencies, and the DoD Field Activities responsible for DCIP-related intelligence activities. Defense infrastructure sectors whose parent organizations lack an internal intelligence element shall be represented at the working group by the CIAO of the Intelligence Sector of the DCIP.

b. The executive steering panel will meet annually, or more frequently as required.

c. The action-officer panel will meet quarterly, or more frequently as required.

d. The DCIP IWG shall serve as the primary coordination mechanism for intelligence support to the DCIP.

2. GLOBAL BASELINE ASSESSMENT OF THE THREATS TO DCI

a. The DIA-produced triennial assessment of the threats to DCI shall include, at a minimum and subject to the USD(P) priorities:

(1) Foreign intelligence threat to DCI.

(2) Insider threat.

(3) Foreign nuclear, biological, chemical, and radiological threat to DCI.

(4) Emerging technologies threat to DCI.

(5) Cyber threat to DCI.

(6) Foreign special operations forces threat to DCI.

- (7) Global terrorism threat to DCI.
- (8) Foreign threats to space-borne DCI.
- (9) Hazards posed by epidemics and pandemics.

b. Production tasking in support of this assessment will be provided via Community On-Line Intelligence System for End Users (COLISEUM), or via such tasking mechanism in use within the Enterprise at that time, by the CIAO for the Intelligence Sector of the DCIP.

### 3. AOR-SPECIFIC THREAT ASSESSMENT SUPPLEMENTS

a. The geographic CCMD-produced, AOR-specific supplement to the DIA-produced triennial DCIP threat assessment shall include, at a minimum and subject to USD(P) and Combatant Commander priorities:

- (1) Regional terrorist threat to DCI.
- (2) Conventional military threat to DCI as posed by those Priority 1, 2, or 3 countries as established by the National Intelligence Priorities Framework.
- (3) Hazards posed to DCI from natural disasters common to the AOR.
- (4) Host-nation government interference, as appropriate.
- (5) Host-nation civil population events, such as protests, strikes, and unrest.
- (6) Potential insider threats, such as the leaking of classified information.

b. Triennial updates will capture all relevant intelligence information collected or produced since the preceding supplement.

c. Production tasking in support of this assessment will be provided via COLISEUM, or via such tasking mechanism in use within the DIE at that time, by the CIAO for the Intelligence Sector of the DCIP.

4. DEFENSE CRITICAL INFRASTRUCTURE THREAT ASSESSMENTS. The DIA-produced triennial Defense Critical Infrastructure Threat Assessments shall address, at a minimum and subject to USD(P) priorities, the threats to each DCA individually arising from:

- a. Intelligence collection.
- b. Chemical weapon attacks.

- c. Biological weapon attacks.
- d. Nuclear weapon attacks.
- e. Radiological weapon attacks.
- f. Electromagnetic spectrum attacks.
- g. Cyber attacks.
- h. Kinetic attacks.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AOR	area of responsibility
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CCMD	Combatant Command
CIAO	Critical Infrastructure Assurance Officer
COLISEUM	Community On-Line Intelligence System for End Users
DCA	defense critical asset
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DCITA	defense critical infrastructure threat assessment
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISLA	Defense Infrastructure Sector Lead Agent
DLA	Defense Logistics Agency
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
GIG	Global Information Grid
IC	Intelligence Community
ICD	Intelligence Community Directive
IWG	intelligence working group
OPR	office of primary responsibility
PIR	Priority Intelligence Requirement
USCYBERCOM	U.S. Cyber Command
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics

USD(C)/CFO	Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO), Department Of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command

## PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

ad-hoc intelligence production. Production of finished, all-source intelligence outside the periodic, scheduled production established by this Instruction.

COLISEUM. An analysis requirements management tool used throughout the DIE for tasking and managing requirements for finished intelligence production.

DCA. Defined in Reference (b).

DCI. Defined in Reference (b).

DCIP. Defined in Reference (b).

Defense CI Component. Defined in Reference (a).

Defense Intelligence Component. Defined in Reference (a).

Defense Intelligence Enterprise. The intelligence combat support agencies, the intelligence elements of the Military Services and CCMDs, and DoD intelligence, counterintelligence, and security organizations (e.g., Defense Security Service).

finished intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

intelligence collection requirement. An established intelligence need, validated against the appropriate allocation of intelligence resources to fulfill the PIRs and other intelligence needs of an intelligence consumer.

PIR. A prioritized requirement a commander or decision maker has stated in the process of planning and decision making. PIRs are used to determine and prioritize intelligence collection and analytic resources in support of the mission.