Department of Defense
INSTRUCTION

NUMBER 5240.19
January 31, 2014
Incorporating Change 1, August 17, 2017

USD(I)

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

References: See Enclosure 1

1. PURPOSE. This instruction reissues DoD Instruction (DoDI) 5240.19 (Reference (a)) and implements policy and assigns responsibilities in accordance with DoD Directive (DoDD) 5143.01, DoDD O-5240.02, and DoDD 3020.40 (References (b) through (d)).

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 Department of Defense (DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that:

a. Counterintelligence (CI) activities be conducted in support of the DCIP in accordance with References (b) through (d).

b. CI organizations provide comprehensive and timely reporting of foreign intelligence entity (FIE) threats, incidents, events, and trends to DCIP authorities and the DoD Components in accordance with Reference (c).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. ~~**Unlimited** This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://dtic.mil/whs/directives.~~

Cleared for public release. *This instruction is available on the Directives Division Website at http://www.esd.whs.mil/DD/.*

7. EFFECTIVE DATE. This instruction *is effective January 31, 2014.* ~~:~~

~~a. Is effective January 31, 2014.~~

~~b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoDI 5025.01 (Reference (e)).~~

~~c. Will expire effective January 31, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (e).~~

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Procedures
4. DCIP CI Coverage Plan
5. DCIP CI Support Functions and Activities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)," August 27, 2007, as amended (hereby cancelled)

(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence, (USD(I)) " ~~November 23, 2005~~ *October 24, 2014, as amended*

(c) DoD Directive O-5240.02, "Counterintelligence," ~~December 20, 2007, as amended~~ *March 17, 2015*

(d) DoD Directive 3020.40, "~~DoD Policy and Responsibilities for Critical Infrastructure~~ *Mission Assurance (MA)*," ~~January 14, 2010, as amended~~ *November 29, 2016*

~~(e) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended~~

(~~f~~*e*) Presidential Policy Directive – 21, "Critical Infrastructure Security and Resilience," February 12, 2013

(~~g~~*f*) *Public Law 112-239, "*National Defense Authorization Act for Fiscal Year 2013*," January 1, 2013* ~~(Public Law 112-239)~~

(~~h~~*g*) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011*, as amended*

(~~i~~*h*) DoD Instruction 5205.13, "Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities," January 29, 2010

(~~j~~*i*) DoD Instruction 5240.10, "Counterintelligence (CI) in the Combatant Commands and Other DoD Components," October 5, 2011*, as amended*

(~~k~~*j*) DoD Instruction S-5240.17, "*(U)* Counterintelligence Collection ~~(U)~~ *Activities (CCA)*," ~~January 12, 2009~~ *March 14, 2014*

(~~l~~*k*) DoD Instruction 5240.16, "Counterintelligence Functional Services (CIFS) ~~(U)~~," August 27, 2012*, as amended*

(~~m~~*l*) DoD Instruction 5240.18, "Counterintelligence (CI) Analysis and Production," November 17, 2009, as amended

(~~n~~*m*) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended

(~~o~~*n*) DoD Manual 3020.45~~-M-~~ Volume 3, "Defense Critical Infrastructure Program (DCIP): Security Classification Manual (SCM)," February 15, 2011, as amended

(~~p~~*o*) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," ~~February 2, 2009, as amended~~ *April 1, 2016*

(~~q~~*p*) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009, as amended

(~~r~~*q*) DoD Instruction S-5240.09, "*(U)* Offensive Counterintelligence Operations (OFCO) ~~(U)~~," ~~October 29, 2008~~ *February 2, 2015, as amended*

(~~s~~*r*) DoD Instruction 3020.51, "Intelligence Support to the Defense Critical Infrastructure Program, (DCIP)" June 23, 2011

(~~t~~*s*) DoD Manual 3020.45~~-M-~~ Volume 5, "Defense Critical Infrastructure Program (DCIP): Execution Timeline," May 24, 2010*, as amended*

(~~u~~*t*) ~~Joint Publication 1-02~~ *Office of the Chairman of the Joint Chiefs of Staff*, "~~Department of Defense~~ *DoD* Dictionary of Military and Associated Terms," current edition

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). The USD(I):

a. Serves as the principal advisor to the Secretary of Defense regarding CI support to the DCIP.

b. Acts as the final decision authority on issues regarding CI support to the DCIP that cannot be resolved by the DoD Components.

2. DIRECTOR FOR DEFENSE INTELLIGENCE FOR INTELLIGENCE & SECURITY (DDI(I&S)). Under the authority, direction, and control of the USD(I), the DDI(I&S):

a. Provides policy oversight for CI support to the DCIP.

b. Serves as the OSD staff point-of-contact (POC) for issues regarding CI support to the DCIP.

c. Represents DoD in national-level forums on CI support to the DCIP.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in sections 11 and 12 of this enclosure, the Director, DIA:

a. Plans, integrates, coordinates, directs, synchronizes, and manages intelligence and CI support for the DCIP. This includes providing functional management and includes assigning a chair for the CI Support to the DCIP integrated management group (IMG).

b. Coordinates with the DoD Components to integrate CI support into overall intelligence support to the DCIP.

c. Ensures the current Global Baseline Assessment is available as a resource for CI organizations.

d. Analyzes CI Information and FIE threats directed against the defense critical infrastructure (DCI) and:

(1) Produces assessments for use by CI and other organizations supporting the DCIP.

(2) Provides CI analytical support and distributes analytical products concerning FIE threats to CI and other organizations providing support to the DCIP.

(3) Ensures these products are coordinated with the intelligence sector Critical Infrastructure Assurance Officer (CIAO).

e. Manages CI collection requirements and intelligence production in support of the DCIP.

f. In coordination with the appropriate combatant commanders (CCDRs), develops and maintains CI collection plans to satisfy the collection requirements of the Defense Infrastructure Sectors in accordance with Reference (d).

g. Deconflicts activities when multiple CI organizations have equities in the same Defense Critical Assets (DCA)/Tier 1 Task Critical Assets (TCA) and the issue cannot be resolved at the component or CCMD level.

h. In coordination with the DoD Components, develops and implements performance measures for CI support to the DCIP.

i. In coordination with the Assistant Secretary of Defense for Homeland Defense and ~~Americas' Security Affairs (ASD(HD&ASA))~~ *Global Security (ASD(HD&GS))* and the intelligence sector CIAO, creates and maintains information databases for CI support to the DCIP.

j. Ensures DoD Component heads with organic CI assets address providing CI support to the DCIP in their CI training courses.

k. In coordination with the DoD Component CI organizations, develops standardized core elements and criteria for CI threat assessments supporting the DCIP.

4. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I), and in addition to the responsibilities in sections 11 and 12 of this enclosure, the Director, DSS:

a. Conducts CI functional services for cleared defense industrial base (DIB) critical assets in coordination with the DoD Components, identifies intelligence gaps related to protecting DIB critical assets, and submits CI collection and production requirements to DIA and the intelligence sector CIAO.

b. Develops requirements and requests for threat assessments for DIB critical assets. Provides industrial security threat information and CI-related information to CI organizations supporting the DIB in accordance with Reference (c).

c. In coordination with the ~~ASD(HD&ASA)~~ *ASD(HD&GS)*, Army CI, and the Director, Defense Contract Management Agency (DCMA):

(1) Helps prepare and execute DCIP CI coverage plans for designated DIB critical

assets.

(2) Coordinates CI activities with the appropriate CI organizations and federal departments and agencies when in support of cleared DIB assets and capabilities nominated by the Director, DCMA.

(3) Informs the Director, DCMA, and Army CI of an actual or potential threat to specific DIB assets; contributes to enhanced DIB security and protection in collaboration with the appropriate CCDR, the intelligence sector CIAO, and the Director, DIA.

(4) Monitors DIB security, threats, suspicious incidents, and countermeasures implementation. As appropriate, notifies the Director, DCMA, appropriate CCDR, ~~ASD(HD&ASA)~~ *ASD(HD&GS)*, supporting CI organization, intelligence sector CIAO, and the Director, DIA, when changing conditions could result in an increased risk.

d. Provides threat and other CI-related information to CI organizations engaged in CI support to the DCIP.

5. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) notifies the USD(I) of policy, program, or process changes in the space sector that may affect CI support in accordance with Reference (d).

6. ~~ASD(HD&ASA)~~ *ASD(HD&GS)*. Under the authority, direction, and control of the USD(P) and in coordination with the USD(I), the ~~ASD(HD&ASA)~~ *ASD(HD&GS)*:

a. Advises the DDI(I&S) of policy, program, or process changes in the DCIP that may affect CI support.

b. Provides DCIP CI collection requirements to DIA.

c. Provides the authoritative DCA and TCA lists to the DDI(I&S). These lists will be the basis of CI support to the DCIP, based upon ~~ASD(HD&ASA)~~ *ASD(HD&GS)* priorities.

d. Establishes DCIP information sharing policy and agreements with appropriate Federal, State, and local CI and law enforcement mission partners in order to enhance DCI protection in accordance with Presidential Policy Directive – 21 (Reference (~~f~~*e*)).

7. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L))

a. The USD(AT&L) notifies the USD(I) of policy, program, or process changes in the DIB, logistics, public works, or transportation sectors that may affect CI support.

b. The USD(AT&L) Damage Assessment Management Office will notify the USD(I) of all compromises of information related to critical infrastructure discovered in the course of damage assessments.

8. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). The USD(C)/CFO notifies the USD(I) of policy, program, or process changes in the financial services sectors that may affect CI support.

9. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) notifies the USD(I) of policy, program, or process changes in the health affairs or personnel sectors that may affect CI support.

10. DoD CHIEF INFORMATION OFFICER (CIO). The DoD CIO:

a. Notifies the USD(I) of policy, program, or process changes in the Global Information Grid (GIG) sector that may affect CI support.

b. Provides DCIP CI collection requirements to DIA to protect the GIG sector and support computer network defense of DoD information systems.

c. Coordinates with the ~~ASD(HD&ASA)~~ *ASD(HD&GS)* and the CCDRs, through the CJCS, as appropriate, to:

(1) Provide, in collaboration with the Director, DIA, the processes and means to notify GIG DCA/Tier 1 TCA owners and operators of known, imminent, and impending threats that may be related to the efforts of an FIE.

(2) Notify the supporting CI organization, the Director, DIA, and the intelligence sector CIAO when there is an increased risk to the GIG sector.

d. Coordinates with the supporting CI organizations designated in Enclosure 3 of this instruction and the Executive Director, Defense Cyber Crime Center (DC3), regarding cyber-related activities affecting the DCIP that may involve an FIE. This includes coordinating with DSS and Army CI when information is exfiltrated from identified DIB sector assets and ensuring that a report (of such a successful penetration of a defense contractor network or information system) is provided to DoD under voluntary agreements or pursuant to Section 941 of *Public Law 112-239* ~~the National Defense Authorization Act for Fiscal Year 2013~~ ~~Public Law 112-239~~ (Reference (~~g~~*f*)).

e. Consults with the executive director, DC3, for all-source cyber analytics, enterprise-wide threat information and National Cyber Investigative Joint Task Force Analytical Group (NCIJTF AG) products relative to FIE activities affecting the GIG and DIB sector assets.

f. Passes information, reportable in accordance with Reference (~~h~~*g*), to the supporting CI

organization that has Defense Infrastructure Sector (DIS) responsibilities in accordance with Enclosure 3 of this instruction.

11. DoD COMPONENT HEADS WITH ORGANIC CI. In addition to the responsibilities in section 12 of this enclosure, the DoD Component heads with organic CI will:

a. Conduct, manage, coordinate, control, integrate, and provide oversight of CI activities to support the DCIP in accordance with References (c), (d), (~~h~~*g*), DoDI 5205.13, DoDI 5240.10, and DoDI S-5240.17 (References (~~i~~*h*), (~~j~~*i*), and (~~k~~*j*)).

b. Conduct a full range of authorized CI activities supporting the DCIP to obtain, analyze, and report intelligence information regarding FIE threats to DCI.

c. Coordinate with Federal, State, and local authorities and the appropriate CCDR to obtain and share information to protect DCI assets. Integrate these efforts with ~~ASD(HD&ASA)~~ *ASD(HD&GS)* information sharing programs in accordance with Reference (c).

d. Coordinate DCIP support with DIA and the appropriate CCDR.

e. Coordinate with Military Department Counterintelligence Organizations to request investigative and or operational support in accordance with Reference (c).

f. Report CI activities supporting the DCIP to DIA and the appropriate CI organizations using the designated defense CI information system in accordance with Reference (b).

g. Produce and annually update threat assessments for DCI and DIB sector critical assets; promptly report threat information to the Director, DIA.

h. As appropriate, consult with the Executive Director, DC3, for digital forensics support and analysis services on CI cyber-related investigations involving DCIP elements.

i. Educate and train Component personnel on FIE threats to the DCIP in accordance with DoDI 5240.16 (Reference (~~l~~*k*)).

12. THE DoD COMPONENTS HEADS OF DEFENSE INFRASTRUCTURE SECTOR LEAD AGENCIES. The DoD Components Heads of Defense Infrastructure Sector Lead Agencies coordinate with their supporting CI organization to identify and provide CI collection and production requirements in accordance with References (d), (~~j~~*i*), and DoDI 5240.18 (Reference (~~m~~*l*)).

13. CJCS. In addition to the responsibilities in section 12 of this enclosure, the CJCS:

a. Integrates CI support to the DCIP into joint planning, programs, systems, exercises,

doctrine, strategies, policies, and architectures.

b. Coordinates and prioritizes CCMD CI collection requirements, and forwards the requirements to the Director, DIA.

c. Coordinates with the DoD Components to provide DCIP-related threat assessments to the CCMDs.

d. Coordinates with the Director, National Geospatial-Intelligence Agency, to support DCIP CI data integration into Joint Staff geospatial systems that support emergency planning and operations within the National Military Command Center.

14. CCDRs. In addition to the responsibilities in sections 11 and 12 of this enclosure, the CCDRs:

a. Request, synchronize, de-conflict, and coordinate CI activities in support of the CCMD DCIP.

b. Integrate CI support to the DCIP into command planning, programs, systems, exercises, doctrine, strategies, policies, and architectures.

ENCLOSURE 3

PROCEDURES

1. CI organizations providing support to defense infrastructure sector assets will coordinate with the Federal Bureau of Investigation (FBI), Intelligence Community, and the Department of Homeland Security (DHS) to ensure that threat information is shared among Federal partners that have responsibilities to protect the DCIs in accordance with Reference (~~f~~e). Additionally, CI threat reporting and information will be made available to organizations responsible for various risk management reports, including Hazards and Vulnerability Assessments mandated under the DCIP in accordance with Reference (c).

2. CI organizations will coordinate across defense infrastructure sectors as necessary to ensure that vulnerabilities associated with multiple sectors are adequately addressed.

3. Threat information related to the GIG sector will be disseminated to the Defense Information Systems Agency (DISA) and the appropriate analytic centers, e.g., DIA, U.S. Strategic Command, the National Security Agency/Central Security Service (NSA/CSS) National Security Operations Center, the NSA/CSS Threat Operations Center, and U.S. Cyber Command.

4. This instruction designates the supporting CI organizations for the respective Defense Infrastructure Sectors and Defense Infrastructure Sector Lead Agents (DISLAs) (see Table 1). The supporting CI organizations will:

a. Develop and coordinate CI coverage for the DCAs and Tier 1 TCAs identified by the DISLA.

b. Forward DCIP CI coverage plans to DIA .

Table 1. Defense Infrastructure Sectors, Sector Leads, and Supporting CI Organizations

Defense Infrastructure Sector	Defense Infrastructure Sector Lead Agent (DISLA)	Supporting CI Organizations
DIB	Director, DCMA	Army CI (Lead) DSS (supporting)
Financial Services	Director, Defense Finance and Accounting Service	Naval Criminal Investigative Service (NCIS)
GIG	Director, Defense Information Systems Agency	Army CI
Health Affairs	Assistant Secretary of Defense for Health Affairs	Air Force Office of Special Investigations (AFOSI)
Intelligence	Director, DIA	DIA

Table 1. DCIP Sectors, Sector Leads, and Supporting CI Organizations, Continued

Logistics	Director, Defense Logistics Agency	Army CI
Personnel	Director, DoD Human Resources Activity	NCIS
Public Works	Chief, U.S. Army Corps of Engineers	Army CI
Space	Commander, U.S. Strategic Command	AFOSI
Transportation	Commander, U.S. Transportation Command	AFOSI

ENCLOSURE 4

DCIP CI COVERAGE PLAN

1. GENERAL. The DCIP CI Coverage Plan (CICP) collects data and information requirements and CI support activities for critical assets within the DCIP. A CI Support Plan (CISP) takes precedence over a CICP at supported locations when a CISP is required in accordance with DoDI 5240.24 (Reference (~~n~~*m*)).

2. BACKGROUND

a. The DCIP divides DCI into ten sectors, in accordance with Reference (d).

(1) Each defense infrastructure sector is assigned a DISLA.

(2) Each DISLA is responsible for identifying the CI requirement for its sector.

b. CI support to the DCIP is aligned in accordance with Reference (~~j~~*i*), based on the DCI, DISLA, and supporting CI organization identified in Table 1. CI support to the DCIP crosses traditional Service and Defense Agency boundaries and may create overlaps or gaps in CI coverage. Therefore, CI organizations will coordinate across DCI sectors as necessary to ensure that threats associated with multiple sectors are adequately addressed.

c. If a CISP has been developed for the DCIP organizations and meets the requirements of the DCIP CICP in Table 2 of this instruction, then another plan does not need to be prepared. The preparing organization will forward the completed CISP to the applicable DISLA and supporting CI organizations identified Table 1 of this instruction.

d. When a CI organization's supported DCA/Tier 1 TCA is located within a second CI organization's installation or area of responsibility (physical assets not located on installations), the second CI organization will:

(1) Provide CI support to the asset.

(2) Coordinate and forward information to the supporting CI organization designated in Table 1.

e. The CI organization that supports the installation or area will complete and submit a DCIP CICP to the DISLA, the supporting CI organization (for the particular defense infrastructure sector), and DIA to create a baseline of CI support to the defense infrastructure sector asset. For example, a GIG infrastructure sector DCA/Tier 1 TCA facility is located on a U.S. Air Force installation; AFOSI will complete a DCIP CICP and forward it to Army CI, DISA CI, and DIA.

(1) The DCIP CICP will be completed for all DCAs and Tier 1 TCAs.

(2) DCIP CICPs will be classified in accordance with *Volume 3 of* DoD Manual (DoDM) 3020.45~~-M Volume 3~~ (Reference (~~o~~*n*)).

3. INSTRUCTIONS FOR COMPLETING A DCIP CI COVERAGE PLAN. The DCIP CICP must include the information in Table 2: however, the CI organization writing the plan may develop its own format.

Table 2. DCIP CICP

DCIP CI Coverage Plan

1. Information Cutoff Date: Enter the date of the latest information in the report

2. Critical Asset Name: Enter the name of the DCA/Tier 1 TCA as identified in the critical asset list. Keeping the same name is important for tracking information on the critical asset.

a. Critical Asset Location (DCA/Tier 1 TCA): Enter the mailing address, and the latitude and longitude. Is the critical asset located on a DoD installation? If yes, identify the installation. If no, identify the installation or the DoD program that the critical asset supports.

c. Critical Asset POC: Enter the primary and alternate local facility POCs. Provide contact information that includes the POC's name, work address, telephone number(s), and e-mail addresses.

d. Contact Information: Enter a contact communications capabilities for each POC. If the POC has access to the Joint Worldwide Intelligence Communications Systems or the Secret Internet Protocol Router Network, insert the appropriate classified e-mail addresses and secure telephone equipment numbers.

e. Alternate Critical Asset POC: Provide the same information listed above for the alternate POC.

f. Contact information:

3. Critical Asset Organizational Structure: Provide personnel demographics for the DCA/Tier 1 TCA.

a. Total number of personnel:

(1) Civilian: Number of DoD Civilian Employees
(2) Military: Number of Military Personnel
(3) Contractors: Number of Contractor Personnel
(4) Clearances:

(a) Cleared: Number of personnel with security clearances

Table 2. DCIP CICP, Continued

(b) Uncleared: Number of personnel without security clearances

b. Number of foreign nationals:

(1) Cleared: Number of foreign nationals with Limited Access Authorizations (LAAs)
(2) Uncleared: Number of foreign nationals without LAAs

4. Defense Infrastructure Sector(s): Identify the Defense Infrastructure Sector that the facility falls under. If the DCA/Tier 1 TCA falls under more than one sector, list all the sectors.

5. Defense Infrastructure Sector Lead Agent (DISLA) POC: Enter the DISLA POC designated by the sector lead to coordinate CI activities and receive CI reports. This could be a member of the sector lead Staff, watch center, or operations center.

6. Primary CI Organization: Enter the name of the primary organization identified in Enclosure 3 of DoDI 5240.19 to provide CI support to the Sector Lead for this critical asset.

a. CI organization POC: Enter the POC for the primary CI organization.

b. Contact information: Provide phone and e-mail contact information.

7. DoD Supporting CI Organization: Provide the identifying data for the CI organization that supports the DCA/Tier 1 TCA. Include organization, POC, address, telephone numbers, and e-mail addresses.

a. DoD supporting CI organization POC:

b. Contact information:

c. DoD supporting CI organization location:

d. Contact information:

8. Other CI Organization: List all other CI organizations that provide CI support to DoD agencies on the installation. Include POCs and the type of support provided.

a. Other CI organization POC information:

b. Contact information:

c. Other CI organization location:

d. Other CI organization mission: e.g., RDA; FP; base, post, or installation CI organizations:

Table 2. DCIP CICP, Continued

9. Non-DoD Supporting CI Organizations: For Example: FBI, DHS. List other non-DoD agencies that have jurisdiction of the critical asset such as the FBI, DHS, Central Intelligence Agency, etc. Provide identifying data for the CI agency that provides CI activities for the critical asset. Include organization, POC, address, telephone numbers, and e-mail addresses.

ENCLOSURE 5

CI ACTIVITIES SUPPORTING THE DCIP

1. CI support to the DCIP includes identifying, neutralizing, or exploiting FIE threats to DCI. Additionally, CI support notifies the DoD Components and the DISLAs of FIE threats. With the threat information, DCIP personnel will be able to implement appropriate security procedures and countermeasures.

2. CI personnel providing support to the DCIP will:

a. Conduct CI investigations, inquiries, and operations, as authorized and in accordance with DoDI 5240.04, DoDI O-5240.21, and DoDI S-5240.09 (References (~~þ~~*o*) through (~~ŕ~~*q*)).

b. Conduct CI collection and reporting to identify threats to the DCIP.

c. Conduct CI analysis and production to:

(1) Identify FIE threats and CI gaps.

(2) Develop collection requirements in support of the DCIP.

d. Produce FIE threat assessments supporting DCIP in accordance with Reference (d), DoDI 3020.51, and DoDM 3020.45, Volume 5 (References (~~ś~~*r*) and (~~ŧ~~*s*)).

e. Provide functional services, including technical security countermeasures support, polygraph support, and CI briefings and debriefings to personnel assigned to DCAs and Tier 1 TCAs to ensure they are aware of FIE threats and their reporting in accordance with Reference (~~ħ~~*g*).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AFOSI	Air Force Office of Special Investigation
~~ASD(HD&ASA)~~ *ASD(HD&GS)*	Assistant Secretary of Defense for Homeland Defense and ~~Americas' Security Affairs~~ *Global Security*
CCDR	Combatant Commander
CCMD	Combatant Command
CI	counterintelligence
CIAO	critical infrastructure assurance officer
CIO	Chief Information Officer
CICP	Counterintelligence Coverage Plan
CISP	Counterintelligence Support Plan
CJCS	Chairman of the Joint Chiefs of Staff
DC3	DoD Cyber Crime Center
DCA	defense critical asset
DCI	defense critical infrastructure
DCIP	Defense Critical Infrastructure Program
DCMA	Defense Contract Management Agency
DDI(I&S)	Director for Defense Intelligence for Intelligence & Security
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISA	Defense Information Systems Agency
DISLA	Defense Infrastructure Sector Lead Agent
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DSS	Defense Security Service
FBI	Federal Bureau of Investigation
FIE	foreign intelligence entity
GIG	Global Information Grid
NSA/CSS	National Security Agency/Central Security Service
POC	point of contact
RDA	research, development, and acquisition
TCA	task critical asset

USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

DCA. Defined in Reference (d).

DCI. Defined in Reference (d).

DCIP. Defined in Reference (d).

DCIP CI coverage plan. A formally coordinated, comprehensive plan that outlines the CI support to DCA and Tier 1 TCA protection. A DCIP CI coverage plan is prepared by the critical asset manager and identifies the appropriate support of DoD, non-DoD, and other CI elements necessary to the development and validation of DoD-wide CI support to the DCIP.

DCIP threat assessment. A compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs and Tier 1 TCAs. DCIP threat assessments address threats posed to DCAs from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction.

defense infrastructure sector. Defined in Reference (d).

defense critical asset. Defined in Reference (d).

DIB critical asset. Defined in ~~Joint Publication 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (~~ut~~)).

FIE. Defined in Reference (~~ut~~).

TCA. Defined in Reference (d).