



Department of Defense INSTRUCTION

NUMBER 5240.19

August 27, 2007

Incorporating Change 1, December 28, 2010

USD(I)

SUBJECT: Counterintelligence Support to the Defense Critical Infrastructure Program

- References:
- (a) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
 - (b) DoD Directive ~~O-5240.02~~, "~~DoD~~ Counterintelligence (~~CI~~)," ~~May 22, 1997~~
December 20, 2007
 - (c) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
 - (d) ~~DoD Directive 5220.22, "National Industrial Security Program,"~~
~~September 27, 2004~~ DoD Instruction O-5100.93, "Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center (DCHC)," August 13, 2010
 - (e) through (l), see Enclosure 1

1. PURPOSE

This Instruction implements policy and assigns responsibilities pursuant to References (a) and (b), according to the authority in Reference (c), for Counterintelligence (CI) support to the Defense Critical Infrastructure Program (DCIP).

2. APPLICABILITY AND SCOPE

This Instruction applies to ~~the Office of the Secretary of Defense (OSD)~~, the Military Departments, the *Office of the* Chairman of the Joint Chiefs of Staff *and* the Joint Staff, the Combatant Commands (COCOMs), the Inspector General of the ~~Department of Defense DoD~~, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the ~~Department of Defense DoD~~ (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS

Terms used in this Instruction are defined in Enclosure 2.

Change 1, 12/28/2010

4. POLICY

It is DoD policy according to Reference (b) to:

4.1. Provide proactive and comprehensive CI support to the DCIP, to include the full spectrum of CI activities.

4.2. Provide comprehensive, timely reporting of potential foreign threat incidents, events, and trends to DCIP authorities and the DoD Components to support the DoD critical infrastructure program.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)), pursuant to Reference (c), shall establish policy, monitor implementation of this Instruction, and issue additional direction and guidance as necessary to provide CI support to the DCIP.

5.2. The Deputy Under Secretary of Defense for *Human Intelligence, CI and Security* (DUSD(*HCI&S*)), under the USD(I), shall serve as the principal advisor to the USD(I) regarding CI support to the DCIP.

5.3. The Director, CI, under the authority, direction, and control of the DUSD(*HCI&S*), shall:

5.3.1. Provide policy oversight for DoD CI support to the DCIP.

5.3.2. Serve as the staff point of contact within OSD for issues related to CI support to the DCIP.

5.3.3. Represent DoD in national-level forums on CI support to the DCIP.

5.4. The Director, Defense Intelligence Agency (DIA), under the authority, direction, and control of the USD(I), shall:

5.4.1. Analyze foreign intelligence threats directed against infrastructure critical to the Department of Defense and produce foreign intelligence threat assessments for use by DoD CI elements in support of the DCIP.

5.4.2. Manage DoD CI intelligence production in support of the DCIP.

5.4.3. Manage DoD CI collection requirements in support of the DCIP.

5.4.4. In coordination with the appropriate geographic Combatant Commander, through the Chairman of the Joint Chiefs of Staff, develop, update, and maintain a DCIP CI intelligence collection plan to satisfy the collection requirements of the Defense Sectors (Reference (a)).

5.4.5. Provide DCIP CI analytical support and distribute analytic products relating to intelligence, surveillance, and reconnaissance (ISR) to DoD CI elements. Provide threat assessments at the lowest level of classification possible for the widest dissemination.

5.5. The Director, Defense Counterintelligence and Human Intelligence Center (DCHC), under the authority, direction, and control of the Director, DIA, in accordance with DoD Instruction (DoDI) O-5100.93 (Reference (d)), shall:

~~5.4.6~~ 5.5.1. Deconflict CI activities when multiple CI elements have an interest in the same critical asset.

~~5.4.7~~ 5.5.2. Provide program management and deconfliction to DoD components providing CI support to the DCIP.

~~5.4.8~~ 5.5.3. Coordinate with DoD CI elements to develop and implement performance measures for CI support to the DCIP.

~~5.4.9~~ 5.5.4. In coordination with the ASD(HD/ASA), create and maintain information databases for DoD CI support to the DCIP.

~~5.4.10~~ 5.5.5. Develop and manage an advanced DoD-level training program for CI support to the DCIP.

~~5.5~~ 5.6. The Director, National Security Agency/Chief, Central Security Service (NSA/CSS), under the authority, direction, and control of the USD(I), shall collect, process, produce, and disseminate DCIP-related intelligence in support of the DCIP.

~~5.6~~ 5.7. The Director, Defense Security Service (DSS), under the authority, direction, and control of the USD(I), shall:

~~5.6.1~~ 5.7.1. Conduct CI functional services for cleared defense industrial base (DIB) critical assets in coordination with Service CI elements.

~~5.6.1.1~~ 5.7.1.1. Coordinate the conduct of CI activity at DIB critical asset facilities.

~~5.6.1.2~~ 5.7.1.2. Identify intelligence gaps related to protecting DIB critical assets and submit CI collection and production requirements to DIA.

~~5.6.2.~~ 5.7.2. Develop requirements and requests for DCIP threat assessments for DIB critical assets. Provide industrial security threat information and other CI-related information to CI elements engaged in supporting the DIB pursuant to DoD Directive 5220.22 (Reference (~~de~~)).

~~5.6.3.~~ 5.7.3. In coordination with the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD(HD/ASA)), under the Under Secretary of Defense for Policy (USD(P)), and the Director, Defense Contract Management Agency (DCMA), under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)):

~~5.6.3.1.~~ 5.7.3.1. Assist in the preparation and execution of DCIP CI Coverage Plans for individual DIB critical assets under DSS cognizance.

~~5.6.3.2.~~ 5.7.3.2. Coordinate CI activities in support of cleared DIB assets and capabilities nominated by the Director, DCMA, and under the cognizance of the Director, DSS, with DoD and Federal authorities.

~~5.6.3.3.~~ 5.7.3.3. Apprise the Director, DCMA, of actual or potential threat activity related to specific DIB assets; contribute to enhanced DIB security and protection in collaboration with the appropriate geographic Combatant Commander, through the Chairman of the Joint Chiefs of Staff, and the Director, ~~DoD Counterintelligence Field Activity (DoD CIFA) DCHC~~, under the authority, direction, and control of the ~~USD(I) Director, DIA~~.

~~5.6.3.4.~~ 5.7.3.4. Monitor DIB security, threats, suspicious incidents, and countermeasure implementation; apprise DCMA, the cognizant Combatant Commander, the ASD(HD/ASA), the Service CI Lead Agency, DIA, and ~~DoD CIFA DCHC~~ when changing conditions could result in an increased risk.

~~5.6.4.~~ 5.7.4. Provide industrial security threat and other CI-related information to CI elements engaged in CI support to the DCIP.

~~5.7.~~ 5.8. The Director, National Geospatial-Intelligence Agency (NGA), under the authority, direction, and control of the USD(I), shall provide geospatial intelligence in support of the DCIP.

~~5.8. The Director, DoD CIFA, under the authority, direction, and control of the USD(I), shall:~~

~~——— 5.8.1. Develop, review, and manage an integrated CI effort to support the DCIP pursuant to DoD Directive 5105.67 (Reference (e)).~~

~~——— 5.8.2. Deconflict CI activities when multiple CI elements have an interest in the same critical asset.~~

~~——— 5.8.3. Provide program management and deconfliction to DoD components providing CI support to DCIP.~~

~~5.8.4. Coordinate with DoD CI elements to develop and implement performance measures for CI support to the DCIP.~~

~~5.8.5. In coordination with the ASD(HD/ASA), create and maintain information databases for DoD CI support to the DCIP.~~

~~5.8.6. Develop and manage an advanced DoD level training program for CI support to the DCIP.~~

5.9. The ASD(HD/ASA), under the USD(P), and in coordination with the USD(I), shall:

5.9.1. Advise the DUSD(HCI&S) of policy, program, or process changes in the DCIP that may affect CI support.

5.9.2. Provide DCIP CI collection requirements to DIA for formal tasking.

5.9.3. Provide the authoritative Defense Critical Asset (DCA) List to the DUSD(HCI&S). This list shall be the basis of CI support to the DCIP, based upon ASD(HD/ASA) priorities.

5.10. The USD(AT&L), in coordination with the USD(I), shall advise the DUSD(HCI&S) of policy, program, or process changes in the DIB, logistics, public works, or transportation infrastructures that may affect CI support.

5.11. The Under Secretary of Defense (Comptroller/Chief Financial Officer), in coordination with the USD(I), shall advise the DUSD(HCI&S) of policy, program, or process changes in the financial services infrastructure that may affect CI support.

5.12. The Under Secretary of Defense for Personnel and Readiness, in coordination with the USD(I), shall advise the DUSD(HCI&S) of policy, program, or process changes in the health affairs or personnel infrastructures that may affect CI support.

5.13. The Assistant Secretary of Defense for Networks and Information Integration shall:

5.13.1. Advise the DUSD(HCI&S) of policy, program, or process changes in the Global Information Grid (GIG) infrastructure that may affect CI support.

5.13.2. Provide DCIP CI collection requirements to DIA to protect the GIG and support computer network defense of DoD information systems.

5.13.3. Coordinate with the ASD(HD/ASA) and the Commanders of the COCOMs, through the Chairman of the Joint Chiefs of Staff, as appropriate, to:

5.13.3.1. Maintain continuing liaison with Federal authorities, including the Director, National Communication System, regarding the security and protection of the GIG and DCA.

5.13.3.2. Provide, in collaboration with the Director, ~~DoD-CIFA~~ *DIA*, the processes and means to apprise GIG critical asset owners and operators of known, imminent, and impending threats.

5.13.3.3. Monitor GIG and critical asset security and countermeasure implementation, monitor threat/suspicious activity, and apprise the ASD(HD/ASA), the CI Lead Agency, and the Director, ~~DoD-CIFA~~ *DIA*, when there is an increased risk to the GIG. (See Enclosure 3 for a list of CI Lead Agencies.)

5.13.4. Coordinate with the CI Lead Agency and the Executive Director, Defense Cyber Crime Center (DC3), for CI cyber investigations when a foreign intelligence connection is indicated.

5.14. The Heads of DoD Components with CI elements under their authority, direction, and control shall:

5.14.1. Provide for the conduct, management, coordination, control, integration, and oversight of CI activities within their Components to support the DCIP pursuant to References (a), (b), and (d) and DoD Instructions 5240.10, 5240.16, 5240.6, and 5240.17 (References (f), (g), (h), and (i), respectively).

5.14.1.1. Establish and implement CI activities to obtain, analyze, and report intelligence information regarding foreign threats to DoD critical assets or national security interests related to the DCIP for use in providing DCIP risk management support to the Intelligence Community.

5.14.1.2. Coordinate with Federal, State, and local authorities and the cognizant Combatant Commander, through the Chairman of the Joint Chiefs of Staff, to obtain and share information to protect DCIP critical assets. Integrate such efforts with ASD(HD/ASA) information sharing programs pursuant to Reference (a).

5.14.2. Coordinate all CI support activities involving the DCIP with ~~DoD-CIFA~~ *DCHC* and the cognizant Combatant Commander.

5.14.3. Report DCIP CI activities to ~~DoD-CIFA~~ *DCHC* and other affected CI elements using the appropriate defense CI information system pursuant to References (h) and (i).

5.14.4. Coordinate with organic CI elements to produce and periodically update threat assessments for DoD critical infrastructures and DIB critical assets; promptly report threat information to ~~DIA and DoD-CIFA~~.

5.14.5. Consult with the Executive Director, DC3, on DoD CI cyber investigations involving critical infrastructures and impacting the GIG to afford DC3 the first opportunity for digital forensic support.

5.14.6. Educate and train organic personnel in CI support to the DCIP.

5.15. The Secretary of the Air Force, as the DoD Executive Agent for Defense Cyber Crime Matters pursuant to Deputy Secretary of Defense Memorandum (Reference (j)), shall:

5.15.1. In coordination with the CI Lead Agency, apply computer forensic support to CI investigations and operations involving critical infrastructure in which a foreign power or transnational terrorist organization is indicated.

5.15.2. Promote CI programs against cyber crime by supporting investigations of illegal activities involving the GIG critical infrastructure.

5.15.3. Provide training in computer investigations and electronic forensics to forensics examiners, investigators, system administrators, and other DoD personnel involved in securing the GIG from unauthorized use.

5.15.4. Oversee the Executive Director, DC3, ensuring that DC3 programs and operations provide CI Support to the DCIP.

5.16. The Chairman of the Joint Chiefs of Staff shall:

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

5.16.2. Direct the Commanders of the COCOMs to submit to the Director, DIA, a prioritized set of collection requirements for CI support to the DCIP.

5.16.3. Coordinate with the Heads of the DoD Components to provide DCIP-related threat assessments and warnings to subordinate elements and other DoD Components.

5.16.4. Coordinate with the Director, NGA, to support DCIP CI data integration into Joint Staff geospatial systems that support emergency planning and operations within the National Military Command Center.

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

6. PROCEDURES

6.1. DoD CI elements providing CI support to Defense Sector assets shall do so in coordination with the Federal Bureau of Investigation (FBI) and pursuant to the provisions of their individually-tailored DCIP CI Coverage Plans. (See Enclosure 4 for the DCIP CI Coverage Plan format and Enclosure 5 for instructions on preparing the plan.)

6.2. DoD CI elements shall coordinate across Defense Sectors as necessary to ensure that CI vulnerabilities associated with interdependencies and support relationships are covered. (See Enclosure 3 for a list of Defense Sectors.)

6.3. DoD CI elements shall share the type of information defined in DoD Instruction ~~5340.6~~ **5240.6**, (Reference (h)), affecting DCA with the DoD Components via the DCA enterprise architecture.

6.4. DCIP CI or foreign intelligence service-related analytic products shall be disseminated among the relevant analytic centers, e.g. DIA, ~~DoD-CIFA~~, the U.S. Strategic Command, the NSA/CSS National Security Operations Center, the NSA/CSS Threat Operations Center, and the Joint Task Force – Global Network Operations.


6.5. CI support to the DCIP includes, but is not limited to, the CI activities listed in Enclosure 6.

7. INFORMATION REQUIREMENTS. The reporting requirements in this Instruction are exempt from licensing in accordance with paragraphs C4.4.1., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (k)).

8. 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 9. EFFECTIVE DATE

This Instruction is effective immediately.


James R. Clapper, Jr.
Under Secretary of Defense for Intelligence

Enclosures – 6

- E1. References, continued
- E2. Definitions
- E3. DCIP CI Support Structure
- E4. DCIP CI Coverage Plan Format
- E5. DCIP CI Coverage Plan Instructions
- E6. DCIP CI Support Functions and Activities

E1. ENCLOSURE 1

REFERENCES, continued

- (e) ~~DoD Directive 5105.67, "DoD Counterintelligence Field Activity," February 19, 2002~~
~~DoD Directive 5220.22, "National Industrial Security Program," September 27, 2004~~
- (f) DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004
- (g) DoD Instruction 5240.16, "DoD Counterintelligence Functional Services," May 21, 2005
- (h) DoD Instruction 5240.6, "Counterintelligence Awareness, Briefing and Reporting Programs," August 7, 2004
- (i) DoD Instruction 5240.17, "DoD Counterintelligence Collection Reporting," October 26, 2005
- (j) Deputy Secretary of Defense Memorandum, "Department of Defense Computer Forensics Laboratory (DCFL) and Department Computer Investigations Training Program (DCITP)," August 17, 2001¹
- (k) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (l) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended

¹ Copies may be requested from the Under Secretary of Defense (Intelligence) at USDI.Pubs@osd.mil

E2. ENCLOSURE 2

DEFINITIONS

E2.1. CI Activities. For the purposes of this Instruction, an alternate term for one or more of the CI functions of investigations, collection, operations, analysis and production, and functional services.

E2.2. CI Cyber Investigation. An investigation using techniques that identify and interdict the misuse of DoD information systems by a trusted insider or an external intruder. These investigations may involve computer intrusions, exceeding authorized network access, denial of service attacks, or the introduction of a virus or a malicious code.

E2.3. DCA. Defined in Reference (a).

E2.4. DCIP. Defined in Reference (a).

E2.5. DCIP CI Coverage Plan. A formally-coordinated, comprehensive plan that outlines the CI support to DCA protection. The 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.

E2.6. DCIP Threat Assessment. For the purposes of this Instruction, a compilation of strategic intelligence information incorporating multi-faceted threats facing DCAs. DCIP threat assessments address threats posed to DCAs from domestic and transnational terrorist elements, foreign intelligence and security services, and weapons of mass destruction.

E2.7. Defense Sector. Defined in Reference (a).

E2.8. DIB Critical Asset. Defined in Joint Publication 1-02 (Reference (1)).

E2.9. Intelligence Collection Plan. Defined in Reference (1).

E3. ENCLOSURE 3DCIP CI SUPPORT STRUCTURE

Table E3.T1. lists the Defense Sectors and Defense Sector Leads, assigned in Reference (a), with their supporting CI Lead Agencies (Reference (f)).

E3.1. The CI Lead Agency shall develop and coordinate CI coverage for the critical assets identified by the DCIP Sector Lead. The CI Lead Agency shall identify the DoD CI coverage provided to or required for a particular DCA and forward the DCIP CI Coverage Plan to ~~DoD~~ ~~CHFA~~ *DCHC* through the DCIP enterprise architecture.

E3.2. Enclosures 4 and 5 contain the DCIP CI Coverage Plan format and instructions for preparing it.

Table E3.T1. DCIP Sectors, Sector Leads, and CI Lead Agencies

DEFENSE SECTOR	DEFENSE SECTOR LEAD	CI LEAD AGENCY
DIB	Director, DCMA	Army Military Intelligence (Army MI)
Financial Services	Director, Defense Finance and Accounting Service	Naval Criminal Investigative Service (NCIS)
GIG	Director, Defense Information Systems Agency	NCIS
Health Affairs	Assistant Secretary of Defense for Health Affairs	Air Force Office of Special Investigations (AFOSI)
ISR	Director, DIA	DIA
Logistics	Director, Defense Logistics Agency	Army MI
Personnel	Director, DoD Human Resources Activity	AFOSI
Public Works	Chief, U.S. Army Corps of Engineers	Army MI
Space	Commander, U.S. Strategic Command	AFOSI
Transportation	Commander, U.S. Transportation Command	AFOSI

E4. ENCLOSURE 4

DCIP CI COVERAGE PLAN FORMAT

Defense Sector:

Defense Sector Lead Agency:

Defense Sector Lead Point of Contact (POC):

DCA Name:

DCA Location:

On DoD Installation (Y/N):

DCA Priority:

DCA POC:

Local Enforcement POC:

Contact Method:

Joint Worldwide Intelligence Communications Systems (JWICS) _____

SECRET Internet Protocol Router Network (SIPRNET) _____

Secure Telephone Equipment (STE) _____

Unclassified Only _____

CI Lead Agency:

Supporting CI Element:

Supporting CI Location:

Supporting CI POC:

Other CI Elements (Research and Technology Protection (RTP); Force Protection (FP); Base, Post, or Installation CI Elements):

Other CI Element Mission:

Other CI Element Designator:

Other CI Element Location:

Other CI Element POC:

Threat Assessment Type and Date:

Threat Assessment Produced By (e.g., ~~DoD CIFA~~, DIA):

Joint Staff Integrated Vulnerability Assessment (JSIVA) Date:

Non-DoD Supporting CI Element (e.g. FBI, DHS):

Non-DoD Supporting CI Location:

Non-DoD Supporting CI Agency POC:

Other Defense Sectors Affected:

Other Defense Sector:

Defense Sector Lead Agency:

Lead Agency POC:

DoD CI Lead Agency:

Supporting CI Element Name:

Supporting CI Element Location:

Supporting DoD CI Agent POC:

E5. ENCLOSURE 5

DCIP CI COVERAGE PLAN INSTRUCTIONS

E5.1. PURPOSE

To collect data and information requirements to identify the CI supporting elements and CI support activities for DCAs within the DCIP.

E5.2. BACKGROUND

Pursuant to Reference (a), the DCIP divides DoD assets into ten Sectors. Each Sector is assigned a Sector Lead. Each Sector Lead is responsible for identifying the critical assets under their purview. CI support to the DCIP is aligned according to Reference (d), based on the Sectors, Sector Leads, and CI Lead Agencies. As such, CI support to the DCIP crosses traditional Service boundaries and may create overlaps or gaps in CI coverage. The CI Lead Agency's ~~Field Agent~~ shall complete and submit this form to ~~DoD-CIFA~~ *DCHC* to create a baseline of CI asset coverage.

E5.3. INSTRUCTIONS

E5.3.1. Defense Sector. As identified in Reference (a) and Enclosure 3. If the asset falls under more than one Sector, list all applicable Sectors.

E5.3.2. Defense Sector Lead Agency. The responsible DoD Component assigned pursuant to Reference (a).

E5.3.3. Defense Sector Lead POC. The POC designated by the Sector Lead to coordinate CI activities and receive CI reports. This could be a member of the Sector Lead Staff or of a watch center or operations center.

E5.3.4. DCA Name. As identified in the DCA List. Keeping the same name is important for tracking information on the asset.

E5.3.5. DCA Location. Full street address and the latitude and longitude.

E5.3.6. On DoD Installation (Y/N). If yes, enter installation name.

E5.3.7. DCA Priority. Based upon the priority assigned by the Defense Sector Lead in the DCA List.

E5.3.8. DCA POC. The primary interface with the CI community. Give full contact information including name, address, telephone numbers, and email address.

E5.3.9. Local Law Enforcement POC. The first responder to an incident involving a DCA. Should be the closest police department, sheriff's office, fire department, or Military Police. Include organizational name and emergency numbers in 10-digit format.

E5.3.10. Contact Method. List communications capabilities for each asset. If the asset has access to the JWICS or the SIPRNET, insert the appropriate classified email addresses or STE numbers.

E5.3.11. CI Lead Agency. The primary CI element identified in Enclosure 3 to provide CI support to the Sector Lead for this asset.

E5.3.12. Supporting CI Element. The CI element that either exists on-site or has agreed to cover the asset due to proximity, mission, or other reasons.

E5.3.13. Supporting CI Location. The identifying data for the principal CI element that provides CI services to the asset. Include organization, address, and telephone numbers.

E5.3.14. Supporting CI POC. Name of CI agent covering the asset or a DCIP POC at the DoD CI element.

E5.3.15. Other CI Elements (RTP; FP; Base, Post, or Installation CI Elements). When an assigned asset has organic CI support or is provided CI support by another DoD Component, the CI Lead Agency shall annotate this coverage in the DCIP CI Coverage Plan. The CI Lead Agency retains responsibility for ensuring CI coverage but can accomplish this through the supporting CI element. For example, the DIB may have an RTP presence with a counterintelligence support plan in place. A military installation will likely have organic CI personnel or someone assigned to provide coverage from another installation. List all known activities.

E5.3.16. Other CI Element Mission. The main duties performed by the assigned CI element (e.g., RTP, FP, investigations, operations).

E5.3.17. Other CI Element POC. Name of agent or other method of contacting the CI activity.

E5.3.18. Threat Assessment Type and Date. List all previous threat assessments created for the asset and the date created.

E5.3.19. Threat Assessment Produced By. Organization(s) that produced the assessment(s).

E5.3.20. JSIVA Date. Date of any JSIVAs and identities of the producers.

E5.3.21. Non-DoD Supporting CI Elements. Other agencies that have jurisdiction of the asset such as the FBI, DHS, or Central Intelligence Agency. Repeat this entry if multiple agencies.

E5.3.22. Non-DoD Supporting CI Location. Identifying data for the CI element that provides CI activities for the critical asset. Include organization name, address, telephone numbers, and email addresses.

E5.3.23. Non-DoD Supporting CI POC. Name of agent covering the asset or a DCIP POC at the servicing unit.

E5.3.24. Other Sectors Affected. Due to multiple missions and interdependencies of assets, identify any other Defense Sector that may be affected or related to this asset.

E6. ENCLOSURE 6

DCIP CI SUPPORT FUNCTIONS AND ACTIVITIES

E6.1. CI SUPPORT FUNCTIONS

DoD CI agents providing DoD CI support to the DCIP shall perform the following key functions.

E6.1.1. Conduct CI investigations and operations to determine attribution for attacks against DCAs.

E6.1.2. Provide other CI activities or functional services to the DoD components responsible for the identification, prioritization, and protection of DCAs.

E6.2. CI SUPPORT ACTIVITIES

DoD CI agents supporting DCIP shall perform some or all of the following activities.

E6.2.1. Identify the critical information system administrators and technicians that foreign intelligence services or terrorist organizations would most likely target.

E6.2.2. Use the internet and other open sources to determine the level of visibility of critical assets, personnel, and technologies to determine if countermeasures should be implemented.

E6.2.3. Identify individuals in critical information technology (IT) jobs who are most vulnerable to Internet and open-source collection and exploitation.

E6.2.4. Provide defensive threat briefings to critical asset personnel focusing on threats to DoD critical infrastructures and assets. Threats should include anomalous activity by trusted insiders. Anomalous activity includes, but is not limited to, exceeding or attempting to exceed established network permissions, intra-net surfing of topics outside the purview of the job, circumventing or attempting to circumvent network security restrictions, introducing malicious code, introducing unauthorized hardware, accessing systems during non-business hours, using file transport protocol above baseline parameters, and having a higher ratio than normal of suspicious foreign email content to network usage.

E6.2.5. Simulate adversary attacks against facility critical information systems to identify specific vulnerabilities and/or information that should not be accessible to the public.

E6.2.6. Employ data exploration and exploitation tools and link analysis capabilities to identify potential threats to DCAs.

E6.2.7. Support the computer security audit enforcement process for critical information systems.

E6.2.8. Develop defensive programs to identify and exploit computer-based modus operandi and tradecraft employed against DoD systems. Employ information operations methodologies to deceive, deny, degrade, detect, deter, and neutralize foreign intelligence activity against DoD critical networked assets.

E6.2.9. Provide CI information to IT managers assigned to critical DoD information infrastructures for their use in enhancing security training programs.

E6.2.10. Obtain applicable vulnerability assessments for use in collaborative DoD CI analytical products.