Department of Defense
DIRECTIVE

NUMBER O-5240.02
December 20, 2007

USD(I)

SUBJECT: Counterintelligence

References: (a) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997 (hereby canceled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(c) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007
(d) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
(e) through (al), see Enclosure 1

1. PURPOSE

This Directive:

1.1. Reissues Reference (a) and implements References (b) and (c) as they pertain to counterintelligence (CI) responsibilities within the Department of Defense.

1.2. Establishes and maintains a comprehensive, integrated, and coordinated DoD CI effort under the authority and responsibility of the Under Secretary of Defense for Intelligence (USD(I)).

1.3. Updates policy and assigns responsibilities for direction, management, coordination, and control of Defense CI activities.

1.4. Continues to authorize the Defense Counterintelligence Board (DCIB).

2. APPLICABILITY

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

3. DEFINITIONS

Terms used in this Directive are defined in Reference (b), Joint Publication 1-02 (Reference (d)), and Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Defense CI activities shall be undertaken as part of an integrated DoD and national effort to detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize intelligence collection efforts, other intelligence activities, sabotage, espionage, sedition, subversion, assassination, and terrorist activities directed against the Department of Defense, its personnel, information, materiel, facilities, and activities, or against U.S. national security.

4.2. The Defense CI program shall proactively support the goals, strategies, imperatives, and areas of emphasis of the Secretary of Defense, the Director of National Intelligence (DNI), and the National Counterintelligence Executive (NCIX).

4.3. Defense CI activities shall be conducted according to applicable statutes, References (b) and (c), and DoD 5240.1-R (Reference (e)). DoD CI activities conducted within the United States shall be coordinated and conducted according to the Memorandum of Agreement and its supplement between the Attorney General and the Secretary of Defense (References (f) and (g), respectively). DoD CI activities conducted outside the United States shall be coordinated according to Director of Central Intelligence Directive 5/1 and its supplement (References (h) and (i), respectively) and any superseding Intelligence Community directives.

4.4. DoD CI support shall be integrated into the Defense Critical Infrastructure Program (DCIP), and all information operations and special access programs, according to DoD Directives 3020.40, O-3600.01, and 5205.07 (References (j), (k), and (l), respectively).

(b)(7)(E)

4.6. Defense CI organizations shall support the Joint Intelligence Operations Centers according to guidance from the Chairman of the Joint Chiefs of Staff (Reference (m)).

4.7. Contractors supporting Defense CI activities shall not direct or control CI activities or otherwise engage in the performance of inherently governmental functions, according to DoD Directive 1100.4 (Reference (n)) and the procedures in DoD Instruction 1100.22 (Reference (o)).

4.8. Defense CI organizations shall inform the DoD Components of planned or ongoing CI activities taking place within a DoD Component's assigned operational area or affecting a DoD Component's assigned responsibilities, and shall deconflict those activities as required.

4.9. DoD Component CI organizations and assets shall remain under the command and control of their respective DoD Components, except when a Combatant Commander or a joint task force commander assumes operational control of designated DoD Component CI elements.

4.10. All personnel conducting DoD CI activities shall attend formal CI training approved by the USD(I), the Military Secretaries, or their designees.

4.11. DoD CI personnel may be assigned or detailed to assist and conduct CI activities in support of designated DoD Components, Federal task forces, or other Federal agencies, consistent with Reference (e), DoD Directives 5525.5 and 1000.17 (References (p) and (q)), and applicable memorandums of understanding.

4.12. The DoD Components shall use USD(I)-approved CI information systems and architectures for DoD CI management and reporting.

4.13. The DoD Components shall classify CI activities according to the procedures in DoD Instruction C-5240.08 (Reference (r)).

4.14. The DoD Components shall not disclose planned, ongoing, or previous CI activities conducted by the Services or other supporting DoD Components without specific authorization from the DoD element conducting the CI activity.

4.14.1. Coordination with affected DoD Components shall be limited to essential personnel to preserve the security of planned and ongoing CI activities.

4.14.2. In all cases, the Heads of the DoD Components shall not inappropriately interfere with CI activities. Inappropriate interference includes, but is not limited to, unauthorized disclosure or actions that would compromise CI sources or methods.

4.15. When the Heads of the DoD Components are unable to resolve CI issues among themselves, the USD(I) or designee shall resolve them.

5. RESPONSIBILITIES

5.1. The USD(I), or his or her designee, shall:

5.1.1. Oversee the Defense CI Program according to Reference (b); oversee CI capabilities to support stability operations according to DoD Directive 3000.05 (Reference (s)).

5.1.2. Provide staff oversight of DoD CI organizations to ensure compliance with DoD CI policy.

5.1.3. Represent the Secretary of Defense to the NCIX, the National Counterintelligence Policy Board, and other U.S. CI community forums.

5.1.4. Serve as the U.S. National CI Advisor for consultation and coordination of policy matters to the Allied Command, Europe.

5.1.5. Provide CI staff support to the OSD Principal Staff Assistants.

5.1.6. Share CI information as broadly as possible, except where limited by law, policy, or security classification. Appropriate data shall be visible, accessible, and understandable to the rest of the Department according to DoD Directives 8000.01 and 8320.02 (References (t) and (u)).

5.1.7. Assign special tasks to the Heads of the DoD Components when necessary to accomplish DoD CI objectives.

5.1.8. Approve common CI training standards and publish certification standards for the issuance of organizational CI credentials.

5.1.9. Approve releases of DoD CI information to Congress. In conjunction with the General Counsel of the Department of Defense or his or her designee, report all significant CI activities to Congress according to section 2723 of title 10, United States Code (U.S.C.) (Reference (v)), sections 402a-402c of title 50, U.S.C. (Reference (w)), and applicable DNI implementing guidance.

5.1.10. Approve the DoD CI strategy.

5.1.11. Authorize strategic CI campaigns and approve strategic CI campaign plans.

5.1.12. Designate and approve all CI information systems and architectures to be used for DoD CI management and reporting purposes.

(b)(7)(E)

5.1.14. Authorize the Directors of the Defense Agencies and DoD Field Activities to conduct offensive CI operations (OFCO) and CI investigations, when appropriate.

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

5.2.1. Carry out CI authorities and responsibilities according to DoD Directives 5105.67 and 2000.12 (References (x) and (y)).

5.2.2. Develop, manage, and maintain the DoD CI management and reporting information systems and architectures according to Reference (t) and DoD Directives 8100.1, 4630.05, 8500.01E, 8100.02, and 8190.3 (References (z) through (ad), respectively).

5.2.3. Exercise CI mission tasking authority to ensure the effective integration and synchronization of the DoD CI community.

5.2.4. Conduct internal CI preliminary inquiries, as required.

5.2.5. Support defense research and technology protection, the DCIP, and related programs.

5.2.6. Conduct CI functional services and collection management according to the procedures in DoD Instructions 5240.16 and 5240.17 (References (ae) and (af)).

5.2.7. Provide behavioral science support to DoD CI organizations.

5.2.8. Develop and recommend the DoD CI strategy to the USD(I).

5.2.9. Develop, organize, coordinate, manage, and direct DoD CI strategic campaigns when authorized by the USD(I) or higher authority.

5.2.9.1. Develop and implement a process to identify and coordinate requirements for strategic DoD CI campaigns and to develop proposed strategic CI campaign plans.

5.2.9.2. Coordinate all strategic DoD CI campaign plans with the Heads of the DoD Components to ensure integration, synchronization, and unity of effort.

5.2.10. Support Combatant Command intelligence plans through CI campaign plans.

5.2.11. Develop and implement an integrated process to gather, prioritize, and index strategic CI needs; monitor completion of their resultant requirements.

5.2.12. Oversee DoD CI activities associated with detecting and mitigating anomalies and the insider threat.

5.2.13. Manage the DoD Technical Surveillance Countermeasures Program.

5.2.14. Manage the DoD FPD program.

5.2.15. In coordination with the Commander, U.S. Joint Forces Command, develop and manage a system to identify and share detailed CI lessons learned, best practices, and new CI approaches within the DoD CI community.

5.2.16. Review all proposed releases of DoD CI information to Congress and submit an endorsement or recommendation to the USD(I) for final approval.

5.2.17. Review and deconflict CI training materials or handouts proposed for foreign nationals and periodically assess the impact of these releases upon DoD CI.

5.2.18. Receive and analyze damage assessments from the Heads of the DoD Components related to the compromise of classified or sensitive programs due to unauthorized releases to the public, security compromises, or foreign intelligence activities; coordinate with the NCIX in support of the NCIX responsibility for espionage damage assessments.

5.2.19. Develop, manage, and maintain a DoD CI research, development, test, and evaluation program.

5.2.20. In coordination with the Director, Defense Intelligence Agency (DIA), establish and lead a joint program office for development, deployment, and sustainment of the IDSRS CI component.

5.2.21. Chair the DCIB. (See Enclosure 3.)

5.2.22. Provide the significant CI reports as required by Enclosure 4.

5.2.23. Recognize outstanding DoD CI personnel through an annual DoD CI awards program.

5.3. The Director, DIA, under the authority, direction, and control of the USD(I), shall:

5.3.1. Conduct analysis and production on foreign intelligence and terrorist threats to meet DoD customer needs. Contribute to national products according to References (b) and (y) and DoD Directive 5105.21 (Reference (ag)).

5.3.2. Provide CI staff support to the Chairman of the Joint Chiefs of Staff and other staff support as stated in Chairman of the Joint Chiefs of Staff issuances.

5.3.3. Validate, register, and publish national and DoD CI collection requirements.

5.3.4. Validate DoD CI production requirements and provide them to the appropriate production elements within the DoD CI analysis and production community.

5.3.5. Direct the Defense Human Intelligence (HUMINT) Manager to collect and report information responsive to validated CI collection requirements, and to incorporate CI support into HUMINT operations.

5.3.6. Establish and manage a process to provide the seamless integration of DoD CI collection, production, and joint operations requirements with the activities managed and directed by the Director, DoD CIFA.

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

5.4.1. Assist cleared defense industry in recognizing and reporting foreign contacts and collection attempts, and in applying threat-appropriate security countermeasures.

5.4.2. Provide threat information to cleared defense industry points of contact.

5.4.3. Assist the Heads of the DoD Components in ensuring protection of critical DoD research and technologies in the defense industry.

5.4.4. Provide CI oversight of personnel security investigations conducted by the Office of Personnel Management on DoD personnel and contractors, except as stated in paragraph 5.5. Refer all cases of CI interest to the appropriate DoD CI organization, or to the Director, Federal Bureau of Investigation (FBI).

5.5. The Director, National Security Agency/Chief, Central Security Service (NSA/CSS), under the authority, direction, and control of the USD(I), shall:

5.5.1. Collect, process, and disseminate signals intelligence information for CI purposes.

5.5.2. Provide CI oversight of personnel security investigations of NSA personnel and contractors. Refer all cases of CI interest to the appropriate DoD CI organization or to the Director, FBI.

5.6. The Director, National Geospatial-Intelligence Agency (NGA), under the authority, direction, and control of the USD(I), shall receive, validate, prioritize, and satisfy requests for geospatial intelligence in support of DoD CI activities.

5.7. The Director, Defense Threat Reduction Agency (DTRA), under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics, shall provide CI functional services, as appropriate, to the Heads of the DoD Components in support of international arms control agreements and regimes for nuclear and other weapons of mass destruction matters.

5.8. The Heads of the DoD Components shall:

5.8.1. Integrate Defense CI activities into operations, programs, systems, exercises, planning, doctrine, strategies, policies, and architectures.

5.8.2. Establish and maintain proactive and comprehensive CI briefing, reporting, and awareness programs according to the procedures in DoD Instruction 5240.6 (Reference (ah)).

5.8.3. Request technical surveillance countermeasures support according to the procedures in DoD Instruction 5240.05 (Reference (ai)).

5.8.4. Provide authorized CI personnel with access to organizational databases that could assist Defense CI.

5.8.5. Provide written CI support requirements to the lead CI organization, if the DoD Component has no organic CI support; update support requirements annually at a minimum.

5.8.6. Provide to the Director, DoD CIFA, DoD Component damage assessments related to the compromise of classified or sensitive programs due to unauthorized releases to the public, security compromises, or foreign intelligence activities.

5.8.7. Coordinate with the head of the Military Department CI organization concerned to resolve issues related to a request for investigative or operational support.

5.8.8. Conform any CI training provided to foreign nationals to current statutes, Executive Orders, DNI Directives, Chairman of the Joint Chiefs of Staff and Combatant Command policies, and DoD issuances addressing CI policy and procedures.

5.8.8.1. As appropriate, release classified CI training information according to DoD Directive C-5230.23 (Reference (aj)).

5.8.8.2. Provide CI training material or handouts proposed for foreign nationals to the Director, DoD CIFA, for review and deconfliction.

5.8.9. Provide CI-related information or data requested by the USD(I); the Director, DoD CIFA; the Director, DIA; the Chairman of the Joint Chiefs of Staff; and appropriate Combatant Commanders.

5.8.10. Recommend new CI approaches, including techniques, methods, and equipment, to the DCIB and the Director, DoD CIFA, for incorporation into DoD-wide CI efforts.

5.8.11. Recommend standardized CI training and certification criteria to the USD(I).

5.8.12. Provide to the Director, DoD CIFA, after-action reports, lessons learned, and best practices concerning CI activities, to improve information sharing and enhance DoD CI program effectiveness and efficiency.

5.8.13. Support information sharing among CI, security, intelligence, and law enforcement organizations.

5.8.14. Provide to the Director, DoD CIFA, for USD(I) prior approval, copies of CI information to be released to Congress.

5.8.15. Provide CI source registration data to IDSRS or other registries as the USD(I) designates.

5.8.16. Assign, detail, and prescribe the duties of CI personnel to effectively manage their careers.

5.9. The Directors of the Defense Agencies with organic CI organizations shall:

5.9.1. Conduct CI analysis and other CI activities according to applicable organizational charters; conduct CI functional services and collection according to References (ai) and (aj).

5.9.2. Support and participate in authorized CI campaign plans.

5.9.3. Respond to mission taskings from the Director, DoD CIFA.

5.9.4. Conduct internal CI preliminary inquiries, as required.

5.9.5. Refer all information concerning potential OFCO opportunities to the head of the Military Department CI organization concerned as soon as possible.

5.9.6. Report significant CI activities promptly to the Director, DoD CIFA, and to the Head of the affected DoD Component (see Enclosure 4).

5.9.7. Issue organizational CI credentials, when appropriate, to individuals meeting USD(I)-approved certification standards.

5.10. The Secretaries of the Military Departments shall:

5.10.1. Provide for the conduct, direction, management, coordination, and control of the CI program within their Departments according to sections 3013, 5013, and 8013 of Reference (v).

5.10.2. Conduct the full range of CI activities according to the procedures in References (ac), (af), (ah), and (ai); conduct investigations of active duty and Reserve Component personnel, DoD civilians, and other DoD-affiliated personnel according to References (c), (e) through (i), and sections 801-940 of Reference (v).

5.10.3. Retain administrative control for those Service CI resources under operational control of the Combatant Commanders. CI investigations and attendant matters shall remain under each Military Department's control and supervision.

5.10.4. Respond to mission taskings from the Director, DoD CIFA.

5.10.5. Represent the Military Department on CI matters with local, regional, national, and international boards, committees, and other organizations.

5.10.6. Support and participate in authorized CI campaign plans.

5.10.7. Provide CI support to designated Defense Agencies, Field Activities, and Combatant Commands according to DoD Instruction 5240.10 (Reference (ak)).

5.10.8. Provide CI support to DoD HUMINT organizations.

5.10.9. Exercise operational control over designated FPDs. Provide logistics, administrative, and other support to designated FPDs as necessary.

5.10.10. Provide CI support and participation in joint exercises and Combatant Command-designated CI exercises.

5.10.11. Designate organizations within their Departments authorized to conduct OFCO and CI investigations.

5.10.12. Report significant CI activities promptly to the Director, DoD CIFA, and to the Head of the affected DoD Component (see Enclosure 4).

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

5.11.1. Integrate CI into joint planning, programs, systems, exercises, doctrine, strategies, policies, Joint Universal Lessons Learned System, and architectures, where appropriate.

5.11.2. Develop a global, joint CI strategy linked to national and DoD CI strategies, theater strategies, and other Combatant Command plans.

5.11.3. Serve as a member of the National Counterintelligence Policy Board.

5.12. The Commanders of the Combatant Commands, through the Chairman of the Joint Chiefs of Staff, shall:

5.12.1. Develop and implement a comprehensive CI program within their Commands; provide general guidance on their CI objectives that is linked to the global CI strategy of the Chairman of the Joint Chiefs of Staff and to the DoD CI strategy.

5.12.2. Educate supporting CI organizations on their theater strategy or functional mission, as appropriate, to ensure CI organization efforts support or do not conflict with the Command's activities.

5.12.3. Appoint a CI Staff Officer (CISO) to serve as the authoritative point of contact for the Command on CI issues and activities.

5.12.4. Exercise staff coordination authority over Military Department CI organizations, when appropriate, to deconflict activities and assure unity of effort in attaining Military Department and Combatant Command CI objectives.

5.12.5. Analyze and disseminate foreign intelligence and terrorist threat information to meet the Command's needs and to contribute to national products.

5.12.6. Include CI requirements and tasking in Command plans and operations as appropriate.

5.12.7. Assume operational control of designated DoD CI organizations when specified by a military operation or operation order, or for the duration of a joint training exercise.

5.12.8. Establish measures to compartment and protect sensitive CI investigations and OFCO information and techniques.

5.12.9. Provide CI source registration data to IDSRS and other registries as the USD(I) designates.

5.12.10. Task the FPDs through the USDR.

6. INFORMATION REQUIREMENTS

The reporting requirements in this Directive are exempt from licensing in accordance with paragraphs C4.4.1., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (al)).

7. EFFECTIVE DATE

This Directive is effective immediately.

Gordon England

Enclosures - 4
- E1. References
- E2. Definitions
- E3. DCIB
- E4. Significant Counterintelligence Reporting Criteria

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982
(f) Memorandum of Agreement Between the Attorney General and the Secretary of Defense, "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation (U)," April 5, 1979[1]
(g) Supplement to the 1979 Federal Bureau of Investigation and Department of Defense Memorandum of Understanding, "Coordination of Counterintelligence Matters Between FBI and DoD (U)," June 3 and June 20, 1996[1]
(h) Director of Central Intelligence Directive 5/1, "Espionage and Counterintelligence Activities Abroad (U)," December 19, 1984[2]
(i) Supplement to Director of Central Intelligence Directive 5/1, "Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense Regarding Counterintelligence Activities Abroad (U)," February 3, 1995[1]
(j) DoD Directive 3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005
(k) DoD Directive O-3600.01, "Information Operations," August 14, 2006[1]
(l) DoD Directive 5205.07, "Special Access Program (SAP) Policy," January 5, 2006
(m) Chairman of the Joint Chiefs of Staff Message, "Joint Intelligence Operations Center (JIOC) Execute Order (EXORD) (U)," April 3, 2006[3]
(n) DoD Directive 1100.4, "Guidance for Manpower Management," February 12, 2005
(o) DoD Instruction 1100.22, "Guidance for Determining Workforce Mix," September 7, 2006
(p) DoD Directive 5525.5, "DoD Cooperation with Civilian Law Enforcement Officials," January 15, 1986
(q) DoD Directive 1000.17, "Detail of DoD Personnel to Duty Outside the Department of Defense," February 24, 1997
(r) DoD Instruction C-5240.08, "Counterintelligence Security Classification Guide (U)," December 7, 2005[1]
(s) DoD Directive 3000.05, "Military Support for Stability, Security, Transition, and Reconstruction (SSTR) Operations," November 28, 2005
(t) DoD Directive 8000.01, "Management of DoD Information Resources and Information Technology," February 27, 2002
(u) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004
(v) Sections 801-940, 2723, 3013, 5013, and 8013 of title 10, United States Code
(w) Sections 402a-402c of title 50, United States Code
(x) DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002

---

[1] Copies may be requested from the Under Secretary of Defense (Intelligence), at USDI.Pubs@osd.mil.
[2] Copies are available to authorized users via the Defense SECRET Internet Protocol Router Network at http://capco.dssc.sgov.gov/dcids_home.htm.
[3] Copies are available to authorized users via the Intelink at http://djioc.dodiis.ic.gov.

(y) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
(z) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(aa) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 5, 2004
(ab) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(ac) DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004
(ad) DoD Directive 8190.3, "Smart Card Technology," August 31, 2002
(ae) DoD Instruction 5240.16, "DoD Counterintelligence Functional Services," May 21, 2005
(af) DoD Instruction 5240.17, "DoD Counterintelligence Collection Reporting," October 26, 2005
(ag) DoD Directive 5105.21, "Defense Intelligence Agency (DIA)," February 18, 1997
(ah) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004
(ai) DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM) Program," February 22, 2006
(aj) DoD Directive C-5230.23, "Intelligence Disclosure Policy (U)," November 18, 1983[1]
(ak) DoD Instruction 5240.10, "Counterintelligence Support to the Combatant Commands and the Defense Agencies," May 14, 2004
(al) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Anomalies. Foreign power activities or knowledge, inconsistent with the expected norms, that suggest prior foreign knowledge of U.S. national security information, processes, or capabilities.

E2.2. CI Activities. For the purposes of this Directive, an alternate term for one or more of the CI functions of investigations, collection, operations, analysis and production, and functional services.

E2.3. CI Analysis. For the purposes of this Directive, the methodical process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of foreign powers, international terrorists, and other entities.

E2.4. CI Force Protection Detachment. A CI element that provides CI support to transiting and assigned ships, personnel, and aircraft in regions of elevated threat.

E2.5. CI Functional Services. CI activities that support other intelligence or DoD operations by providing specialized CI services (e.g., technical surveillance countermeasures, support to critical technology protection) to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against U.S. national security.

E2.6. CI Investigation. For the purposes of this Directive, inquiries and other activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, or international terrorist activities, and actions to neutralize such acts.

E2.7. CI Mission Tasking Authority. The authority to task a Military Service CI organization's headquarters or a Defense Agency's organic CI element to execute a specific CI mission or conduct a CI function within that organization's CI charter.

E2.8. CI Preliminary Inquiry. An examination of the facts surrounding an incident of potential CI interest, to determine if a full CI investigation is necessary.

E2.9. CI Production. For the purposes of this Directive, the creation of finished intelligence products incorporating CI analysis in response to known or anticipated customer CI concerns.

(b)(7)(E)

E2.11. Offensive CI Operation. An approved CI operation involving a formally recruited human source conducted for DoD or national purposes against a target having suspected or known foreign intelligence and security services affiliation, international terrorist affiliation, or other foreign persons or organizations, to counter terrorism, espionage, or other clandestine intelligence activities that threaten the security of the Department and/or the United States.

E3. ENCLOSURE 3

DCIB

E3.1. ORGANIZATION AND MANAGEMENT

E3.1.1. The DCIB shall be convened and chaired by the Director, DoD CIFA. DCIB membership shall include the following:

E3.1.1.1. The Deputy Director, DoD CIFA; the Senior Deputy General Counsel for Intelligence, DoD Office of the General Counsel; the Assistant to the Secretary of Defense for Intelligence Oversight; and the Director of Counterintelligence, Office of the USD(I).

E3.1.1.2. A representative from:

E3.1.1.2.1. Each of the Military Department CI organizations

E3.1.1.2.2. The Marine Corps Counterintelligence and Human Intelligence Branch

E3.1.1.2.3. DSS

E3.1.1.2.4. DTRA

E3.1.1.2.5. DIA

E3.1.1.2.6. NSA/CSS

E3.1.1.2.7. The National Reconnaissance Office

E3.1.1.2.8. NGA

E3.1.1.2.9. The Missile Defense Agency

E3.1.1.2.10. The J2CI and J-39 Deputy Director for Global Operations/Special Access Division/Tactical Security Branch, of the Joint Staff.

E3.1.1.3. The Combatant Command CISOs.

E3.1.2. The DCIB shall be supported by working groups dedicated to specific DoD CI functions, missions, or other areas, with participation from appropriate organizations represented on the DCIB. These working groups shall report their progress and efforts periodically as required by the DCIB.

E3.2. FUNCTIONS

The DCIB shall:

E3.2.1. Focus on achieving better efficiencies, standardizing where appropriate, responding to customer requirements, and transforming DoD CI to meet the needs of the Department in the future.

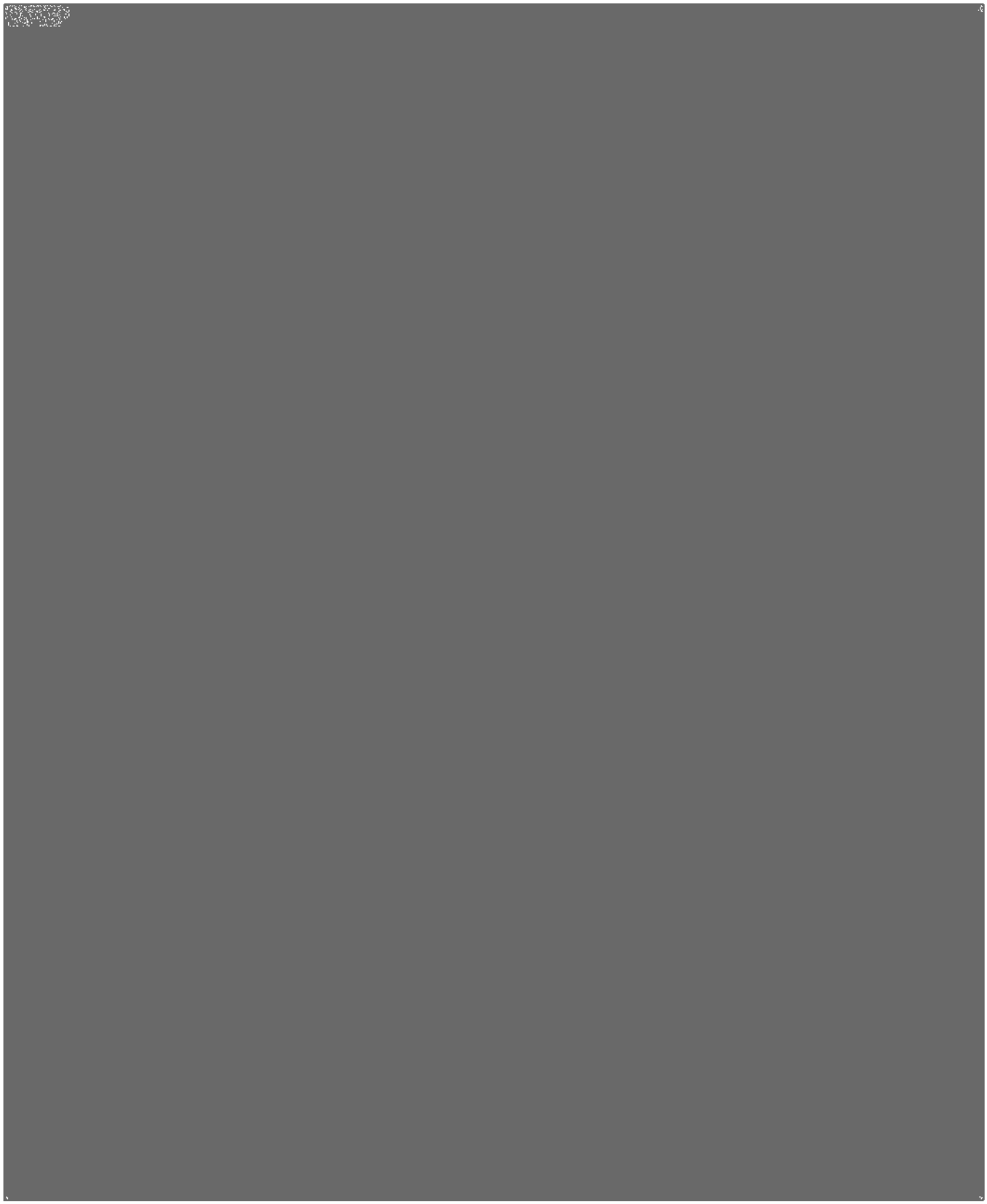
E3.2.2. Advise and assist the USD(I) or designee on CI matters contained in this Directive concerning oversight and implementation of DoD CI policy, and the need for and allocation of DoD CI resources.

E3.2.3. Monitor and evaluate DoD CI functional areas and support functions, such as information technology and training.

E3.2.4. Carry out specific tasks as outlined by the Chair, DCIB.

E3.2.5. Review and evaluate reforms within the DoD CI program.

E4. ENCLOSURE 4



[redacted]

E4.3. CLASSIFICATION GUIDELINES. The report shall be classified according to Reference (r). Using the format below, fill in only the applicable fields.

Agency: (Organization name/desk officer (principal point-of contact, telephone and e-mail address))

Criteria: (Identify the criteria from paragraph E4.2.)

File Number: (Agency's File Number or Case Control Number)

Agency Project Code:

FBI Project Code:

Executive Summary: (The salient points)

Date Opened: (MM/DD/YYYY)

Incident Date: (MM/DD/YYYY or any part known or inclusive period YYYY to YYYY)

[redacted]

Investigative Status (if appropriate): (Open, pending, or closed)

Allegation: (Summary of the suspected offense, if any)

Details: (Detailed narrative of the known facts)

Update: (Narrative of information developed since the last report. Little or no change should be reported as "Nothing Significant to Report.")