



# Department of Defense DIRECTIVE

NUMBER 5240.2

May 22, 1997

---

---

ASD(C3I)

SUBJECT: DoD Counterintelligence (CI)

- References: (a) DoD Directive 5240.2, subject as above, June 6, 1983 (hereby cancelled)
- (b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
  - (c) Presidential Decision Directive/NSC-24, "U.S. Counterintelligence Effectiveness," May 3, 1994
  - (d) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I))," February 12, 1992
  - (e) through (bb), see enclosure 1

## 1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a), and implements Section 1.11 of reference (b) as it pertains to the assignment of CI responsibilities to the Secretary of Defense, and Section 1.12 of reference (b) as it pertains to the assignment of responsibilities to the Defense Intelligence Agency (DIA), National Security Agency (NSA), the Military Departments, and offices referenced in that section.

1.2. Integrates DoD CI capabilities and coordination procedures into a national CI structure under the direction of the National Security Council (NSC) under reference (c).

1.3. Establishes and maintains a comprehensive, integrated, and coordinated CI effort within the Department of Defense, pursuant to the responsibilities and

authorities assigned to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) in reference (d).

1.4. Assigns responsibilities to the DoD Components for the direction, management, coordination, and control of CI activities conducted under the authority of references (b), (d), (e), and this Directive.

1.5. Establishes the Defense Counterintelligence Board (DCIB).

## 2. APPLICABILITY

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

## 3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

## 4. POLICY

It is DoD policy that:

4.1. CI activities shall be undertaken to detect, identify, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against the Department of Defense, its personnel, information, materiel, facilities and activities.

4.2. CI activities shall be conducted in accordance with applicable statutes, E.O. 12333 (reference (b)), and DoD issuances that govern and establish guidelines and restrictions for these activities, to include procedures issued under DoD Directive 5240.1 (reference (f)) that govern, among other things, CI activities that affect U.S. persons, as contained in DoD 5240.1-R (reference (g)).

4.3. CI activities shall be coordinated and conducted within the United States in accordance with the Memorandum of Agreement (MOA) and its supplement between the Attorney General and the Secretary of Defense (references (h) and (i)), and outside

the United States between the Secretary of Defense and Director of Central Intelligence in accordance with the Director of Central Intelligence Directive 5/1 and its supplement (references (j) and (k)).

4.4. Military Department CI elements are under the command and control of their respective Military Department Secretaries, so as to carry out their statutory authorities and responsibilities under 10 U.S.C. 162 (a)(2) (reference (l)) and 10 U.S.C. 3013(c)(7), 5013(c)(7), and 8013(c)(7) (reference (m)).

4.5. Combatant Commanders may choose to exercise staff coordination authority over Military Department CI elements deployed in an overseas theater. Staff coordination authority is intended to encompass deconfliction of activities and assurance of unity of effort in attaining the Military Department Secretaries and Combatant Commander's objectives relating to CI. This coordination will normally be accompanied through the assigned CI Staff Officer (CISO), as found in DoD Instruction 5240.10 (reference (n)).

4.6. If a military operation plan or operation order so specifies, a Combatant Commander or the Combatant Commander's designated joint force commander, may, upon National Command Authority-directed execution, assume operational control of Military Department CI elements assigned to support the operation for the duration of the operation, to include pre-deployment, deployment, and redeployment phases. Under this circumstance, these CI elements come under the Combatant Commander's combatant command authority. However, law enforcement and CI investigations and attendant matters carried out by CI elements remain part of the Military Department's administrative responsibilities. Likewise, for joint training exercise purposes, the joint force commander may assume operational control of assigned CI elements for the purpose and duration of the exercise.

4.7. The Deputy Assistant Secretary of Defense (Intelligence and Security) (DASD(I&S)) will resolve CI issues, where a Military Department CI entity and a Combatant Commander disagree and when one or both appeal the matter through an appropriate channel to the OSD.

4.8. CI activities shall be inspected in accordance with DoD Directive 5148.11 (reference (o)).

4.9. There shall be a DCIB, as described in enclosure 3.

## 5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall delegate to the DASD(I&S) the authority to act for the ASD(C3I) in carrying out CI responsibilities assigned by DoD Directive 5137.1 (reference (d)), as follows:

5.1.1. The DASD(I&S) shall:

5.1.1.1. Oversee development and management of the DoD Foreign CI Program.

5.1.1.2. Establish and monitor management procedures to improve the effectiveness and efficiency of CI and resource management.

5.1.1.3. Serve as the OSD Tactical Intelligence and Related Activities (TIARA) Functional Manager for CI programs.

5.1.1.4. Serve as the Functional Manager for information management matters related to designated CI systems.

5.1.1.5. Represent DoD CI interests on the National CI Policy Board (NACIPB) under PDD/NSC-24 (reference (c)), when necessary.

5.1.1.6. Delegate to the Director, CI, the following authority and functions:

5.1.1.6.1. Develop DoD CI policy and exercise policy supervision and management of DoD CI programs and activities as defined in this Directive.

5.1.1.6.2. Act as program manager for DoD FCIP resources, which include resources for the Military Departments, On-Site Inspection Agency (OSIA), DIA, and Defense Investigation Service (DIS).

5.1.1.6.3. Serve as functional CI manager to include reviewing and monitoring the progress and effectiveness of CI investigations, offensive operations, collection, analysis and production. Conduct or provide for the conduct of inspections of DoD CI Components; staff oversight of DoD CI components and resolve conflicts between those components; and assign special tasks to the DoD Components as may be necessary to accomplish DoD CI objectives.

5.1.1.6.4. Chair the DCIB.

5.1.1.6.5. Coordinate DoD CI programs and activities with other U.S. Government organizations.

5.1.1.6.6. Ensure adequate CI support is provided to the DoD Components, as necessary, to include support to Special Access Programs and support to Human Intelligence (HUMINT).

5.1.1.6.7. Support the DASD(I&S) role as the TIARA Functional Manager in areas relating to CI.

5.1.1.6.8. Support the DASD(I&S) role as the Functional Manager for the Defense CI Information System.

5.1.1.6.9. Be the U.S. National CI Advisor to the Allied Command Europe, for the purposes of consultation and coordination of policy matters.

5.1.1.6.10. Support or provide DoD representation on the National CI Policy Board, National CI Operations Board, Operations Chiefs Working Group, Investigations Working Group and representation to other national-level CI agencies in accordance with PDD/NSC-24 (reference (c)); and represent the ASD(C3I) on the Secretary's Board on Investigations in accordance with DoD Directive 5105.59 (reference (p)).

5.1.1.6.11. Approve or refer to the NSC or NACIPB operations or other CI matters that involve significant policy issues.

5.1.2. The Director, DIA, shall:

5.1.2.1. Conduct analysis and production on foreign intelligence and terrorist threats to meet customer needs within Department of Defense, and contribute to national products of these types as appropriate, in accordance with E.O. 12333 (reference (b)), and within the scope of assigned responsibilities and functions of DIA as described in DoD Directive 5105.21 (reference (q)).

5.1.2.2. Coordinate the CI production programs of all DoD CI components as requested by the Director of CI.

5.1.2.3. Provide CI analytic, production, and database support to the Services as requested.

5.1.2.4. Serve as the DoD CI Collection Requirements Manager as requested by the Director of CI.

5.1.2.5. Provide CI staff support to the Chairman of the Joint Chiefs of Staff and the Combatant Commanders as requested by the Director of CI and in conformance with DoD Instruction 5240.10 (reference (n)).

5.1.2.6. Provide CI staff support to the DoD HUMINT Manager as described in DoD Directive 5200.37 (reference (r)) and ensure CI support is provided to the DoD HUMINT collection program.

5.1.2.7. Develop, implement and maintain intelligence and CI capabilities designed to assist Commanders in the protection of DoD personnel and facilities from terrorism, in accordance with DoD Directive 0-2000.12 (reference (s)).

5.1.2.8. Conduct threat and vulnerability analysis and support decisions by commanders or program managers in the implementation of appropriate Operations Security (OPSEC) measures in accordance with DoD Directive 5205.2 (reference (t)).

5.1.2.9. Assess and provide information systems security threat and vulnerability information to support information operations requirements.

5.1.2.10. Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director of CI.

5.1.3. The Director, DIS, shall:

5.1.3.1. Integrate CI principles and experience into the DIS security countermeasures missions, which consist of conducting personnel security investigations and serving as the cognizant DoD security authority for the National Industrial Security Program, pursuant to E.O. 12829 (reference (u)).

5.1.3.2. Assist the defense industry in the recognition and reporting of foreign contacts and collection attempts, and the application of threat-appropriate security countermeasures.

5.1.3.3. Provide pertinent information on the defense industry to support the production of multidisciplinary intelligence threat analyses as required.

5.1.3.4. Assist the Military Departments' CI organizations in the protection of critical DoD technologies.

5.1.3.5. Perform those CI-related responsibilities assigned by the OSD, to include the investigative support to the DoD Components (exclusive of Military Departments) relative to unauthorized disclosures of classified information to the public in accordance with DoD Directive 5210.50 (reference (v)).

5.1.3.6. Participate on national, international, and interdepartmental boards, committees, and other organizations as requested by the Director of CI.

5.1.4. The Command, Control, Communications, Computers and Intelligence Integration Support Activity shall:

5.1.4.1. Provide CI programmatic analysis and expertise to ASD(C3I) and DASD(I&S) in accordance with DoD Directive 5100.81 (reference (w)), to include consolidation of Military Department and Defense Agency Foreign CI Program submissions and participation in Congressional Budget Justification Book production.

5.1.4.2. Support planning for CI capabilities, communications, and architectures.

5.2. The Secretaries of the Military Departments shall:

5.2.1. Provide for the conduct, direction, management, coordination, and control of CI activities as outlined in paragraphs 5.2.2. through 5.2.11., below; E.O. 12333 (reference (b)); 10 U.S.C. 3013, 5013, 8013 (reference (m)); 10 U.S.C. 535 (reference (x)); Pub. L. 99-145 (1985), Section 1223. (reference (y)); and DoD Instruction 5505.3 (reference (z)).

5.2.2. Conduct CI investigations of Active and Reserve military personnel and, as provided for in agreements with the Attorney General (references (h) and (i)), DoD civilian employees, who may be subject to judicial and/or administrative action under applicable Federal law and regulations, including the Uniform Code of Military Justice, 10 U.S.C. 801-940 (reference (aa)).

5.2.3. Conduct CI operations against foreign intelligence services and organizations.

5.2.4. Collect, process, exploit and report information of CI significance to

satisfy validated national and tactical CI collection requirements.

5.2.5. Conduct CI analysis focusing on support to DoD CI operations and investigations, military operations and force protection, security countermeasures, and national policy and programs.

5.2.6. Produce CI assessments, studies, estimates, and other finished products, to support U.S. military commanders, the Department of Defense, and the U.S. Intelligence Community.

5.2.7. Develop, implement and maintain antiterrorism programs designed to assist Commanders in the protection of DoD personnel and facilities, in accordance with DoD Directive O-2000.12 (reference (s)).

5.2.8. Conduct threat and vulnerability analysis and support decisions by commanders or program managers in the implementation of appropriate OPSEC measures in accordance with DoD Directive 5205.2 (reference (t)).

5.2.9. Assess and provide information systems security threat and vulnerability information to support information operations requirements.

5.2.10. Prescribe regulations providing to their military investigative organizations the authority to initiate, conduct, delay, suspend or terminate investigations and ensure Commanders outside those specified CI military organizations do not impede the use of military techniques permissible under law or regulation.

5.2.11. Maintain, operate, and manage their respective CI components, in accordance with the authorities and responsibilities assigned by this Directive, and provide personnel, equipment, and facilities that CI missions require.

5.2.12. Establish Military Department plans, programs, policies, and procedures to accomplish authorized CI functions.

5.2.13. Establish and maintain a worldwide CI capability for the purposes outlined in paragraphs 5.2.2. through 5.2.11., above.

5.2.14. Develop CI techniques, methods, and equipment required for CI activities and provide basic and specialized training to CI personnel.

5.2.15. Provide CI support to the Combatant Commands, other DoD



Components, U.S. Government organizations, and foreign CI and security agencies as provided for in this Directive.

5.2.16. Inform periodically the Combatant Commanders on CI investigations and operations through the appropriate CI entity and in coordination with the command CISO to fulfill briefing requirements set forth in this Directive and DoD Instruction 5240.10 (reference (n)).

5.2.17. Submit CI operational and investigative data and prepare CI analyses as required by the Director for CI.

5.2.18. Establish and maintain liaison with U.S. and foreign CI, security, and law enforcement agencies in accordance with policies formulated in E.O. 12333 (reference (b)); the MOA and its supplement between the Attorney General and Secretary of Defense (references (h) and (i)); DCID 5/1 (reference (j)) and the CIA/DoD MOA (reference (k)); and coordinate Military Department programs and activities with other U.S. Government organizations.

5.2.19. Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director for CI.

5.3. The Chairman of the Joint Chiefs of Staff shall integrate, where appropriate, CI support into all joint planning, programs, systems, exercises, doctrine, strategies, policies, and architectures.

5.4. The Commanders of the Combatant Commands shall integrate, where appropriate, CI support into all command planning, programs, systems, exercises, doctrine, strategies, policies, and architectures.

5.5. The Under Secretary of Defense for Acquisition and Technology shall ensure that the Director, OSIA, shall:

5.5.1. Provide for the internal security of OSIA's inspection, escort, and portal monitoring teams.

5.5.2. Participate in the production of multidisciplinary intelligence threat analyses as required.

5.5.3. Participate on national, international and interdepartmental boards, committees, and other organizations involving CI as required by the Director of CI.

5.6. The Director, National Security Agency/Chief, Central Security Service shall:

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

5.6.2. Participate in the production of multidisciplinary intelligence threat analyses, as required.

5.6.3. Participate on national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director for CI.

5.7. The Director, National Reconnaissance Office, shall:

5.7.1. Utilize its systems to support CI activities and requirements.

5.7.2. Support the production of multidisciplinary intelligence threat analyses as required.

5.7.3. Participate on DoD, national, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director of CI.

5.8. The Heads of the Other DoD Components shall:

5.8.1. Refer to the applicable Military Department CI Agency any CI information involving military personnel assigned to their Components for investigation and disposition. Refer reported CI information involving civilian employees employed by their Component in the United States to their servicing Military Department CI Agency and, when overseas, to the Military Department responsible for providing administrative and logistical support, in accordance with DoD Directive 5240.6 (reference (bb)).

5.8.2. Contact the nearest Military Department CI Agency office for guidance should a question arise as where to refer reported CI information.

6. EFFECTIVE DATE

This Directive is effective immediately.

A handwritten signature in black ink, appearing to read "John P. White", is written over a horizontal line.

John P. White  
Deputy Secretary of Defense

Enclosures - 3

1. References
2. Definitions
3. Defense CI Board

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Title 10, United States Code, "Armed Forces"
- (f) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988
- (g) DoD 5240.1-R, "Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 24, 1988
- (h) "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction with the Federal Bureau of Investigation," between the Attorney General and the Secretary of Defense, April 5, 1979
- (i) Supplement to 1979 FBI/DoD Memorandum of Understanding: "Coordination of Counterintelligence Matters Between FBI and DoD," June 3 and June 20, 1996
- (j) Director of Central Intelligence Directive 5/1, "Espionage and Counterintelligence Activities Abroad," December 19, 1984
- (k) Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense regarding counter intelligence activities abroad, February 3, 1995
- (l) Section 162 *et seq.* of title 10, United States Code
- (m) Sections 3013, 5013, and 8013 of title 10, United States Code
- (n) DoD Instruction 5240.10, "DoD Counterintelligence Support to Unified and Specified Commands," May 18, 1990
- (o) DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight," July 1, 1992
- (p) DoD Directive 5105.59, "The Secretary's Board on Investigations," September 25, 1995
- (q) DoD Directive 5105.21, "Defense Intelligence Agency," May 19, 1977
- (r) DoD Directive 5200.37, "Centralized Management of the Department of Defense Human Intelligence (HUMINT) Operations," December 18, 1992
- (s) DoD Directive O-2000.12, "DoD Combating Terrorism Program," September 15, 1996
- (t) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983
- (u) Executive Order 12829, "National Industrial Security Program," January 6, 1993
- (v) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," February 27, 1992
- (w) DoD Directive 5100.81, "Department of Defense Support Activities," December 5, 1991

- (x) Section 535 of title 10, United States Code
- (y) Section 1223 of Public Law 99-145, "Authority for Independent Criminal Investigations by Navy and Air Force Investigative Units," November 8, 1985
- (z) DoD Instruction 5505.3, "Initiation of Investigations by Military Criminal Investigative Organizations," July 11, 1986
- (aa) Sections 801-940 of title 10, United States Code, "Uniform Code of Military Justice"
- (bb) DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program," July 16, 1996

## E2. ENCLOSURE 2

### DEFINITIONS

E2.1.1. Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

E2.1.2. Counterintelligence (CI) Analysis. CI analysis is the function of assimilating, evaluating, and interpreting information about areas of CI proponency and responsibility. Information derived from all available sources is considered and integrated in the analytical process.

E2.1.3. Counterintelligence (CI) Collection. The systematic acquisition of information concerning espionage, sabotage, terrorism, and related foreign activities conducted for or on behalf of foreign nations, entities, organizations, or persons and that are directed against or threaten DoD interests.

E2.1.4. Counterintelligence (CI) Investigation. Includes inquiries and other activities undertaken to determine whether a particular person is acting for, or on behalf of, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

E2.1.5. Counterintelligence (CI) Operation. Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security.

E2.1.6. Counterintelligence (CI) Production. The process of analyzing all source information developed into final product and disseminated--irrespective of media--concerning espionage, other foreign intelligence collection threats, sabotage, terrorism, and other related threats, to U.S. military commanders, the Department of Defense, and the U.S. intelligence community.

E2.1.7. Counterintelligence (CI) Support to DoD HUMINT. The application of CI information, knowledge, and experience to prevent foreign intelligence or security services from detecting, neutralizing, or controlling DoD HUMINT plans and operations.

E2.1.8. Military Department Counterintelligence (CI) Agency. The Military Department CI Agencies include Army CI, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

### E3. ENCLOSURE 3

#### DEFENSE COUNTERINTELLIGENCE (CI) BOARD

##### E3.1. ORGANIZATION AND MANAGEMENT

E3.1.1. The DCIB shall be convened and chaired by the Director of CI, Office of the Deputy Assistant Secretary of Defense (Intelligence and Security). The DCIB membership shall include representatives from the OSD; Senior Deputy General Counsel (International Affairs and Intelligence); the Assistant to the Secretary of Defense (Intelligence Oversight); one representative from each of the Military Department CI Agencies; the Defense Investigative Service (DIS), the On-Site Inspection Agency (OSIA); and the Defense Intelligence Agency (DIA). Associate DCIB members are the National Security Agency/Central Security Service (NSA/CSS); the National Reconnaissance Office (NRO); Marine Corps Counterintelligence/Human Intelligence (HUMINT) Branch; Joint Staff, J-38/IW Special Technical Operations Division/TSB; DIA's Joint CI Support Branch; Counterintelligence Support Officers (CISOs), as described in DoD Instruction 5240.10 (reference (n)); and a representative of the C4I Integration Support Activity (CISA).

E3.1.2. The DCIB shall be supported by subcommittees or panels, with participation from those organizations represented on the DCIB. The subcommittee and panel chairs shall be appointed by the Chair, DCIB.

##### E3.2. FUNCTIONS

E3.2.1. The DCIB shall advise and assist the DASD(I&S) on CI matters within the purview of E.O. 12333 (reference (b)), PDD/NSC-24 (reference (c)), and this Directive; e.g., overseeing the implementation of CI policy; advising on the need for and allocation of CI resources; monitoring and evaluating support functions, such as automated data processing; carrying out specific tasks as outlined by the Chair; and reviewing and evaluating reforms of CI entities, to include functional consolidation, integration, and collocation.

E3.2.2. The DCIB membership will coordinate their respective CI activities, under the guidance of the DCIB Chairman.