



Department of Defense INSTRUCTION

NUMBER 5240.6

August 7, 2004

USD(I)

SUBJECT: Counterintelligence (CI) Awareness, Briefing, and Reporting Programs

- References:
- (a) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness and Briefing Program," July 16, 1996 (hereby canceled)
 - (b) Presidential Decision Directive/NSC No.12,¹ "Security Awareness and Reporting of Foreign Contacts," August 5, 1993
 - (c) [DoD Directive 5240.2](#), "DoD Counterintelligence (CI)," May 22, 1997
 - (d) Executive Order 12829, "National Industrial Security Program," January 6, 1993
 - (e) through (y), see enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues reference (a), implements reference (b) within the Department of Defense (DoD), and establishes procedures for conducting and administering DoD counterintelligence awareness, briefings and reporting as required by reference (c).

1.2. Provides procedures for the handling of other threat information affecting the security of DoD personnel, information, resources, installations, and operations.

1.3. Reaffirms the requirement for a foreign intelligence and international terrorist threat awareness and briefing programs for DoD military, civilian employee, and contractor personnel.

¹ Authorized users may contact the CI Directorate, DUSD(CI&S), USD(I), Room 3C260, Pentagon for a copy.

2. APPLICABILITY AND SCOPE

This Instruction applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of 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").

2.2. DoD contractor personnel with security clearances for their briefing and reporting requirements as specified under E.O. 12829 (reference (d)), (hereafter referred to collectively as "the DoD contractors").

2.3. Active and Reserve military personnel, DoD civilian employees, and DoD contractors (hereafter collectively referred to as "the DoD personnel").

3. DEFINITIONS

Definitions for this Instruction are in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The DoD personnel report any contact information or circumstances that could pose a threat to the security of U.S. personnel, DoD or other U.S. resources, and classified national security information (hereafter referred to as "classified information"), or controlled unclassified information under E.O. 12958, DoD Directive 5230.24, DoD 5400.7-R, and DoD Directive 5210.83 (references (e) through (h)) to an appropriate authority. Judicial and/or administrative action may be taken when DoD personnel fail to report such required information.

4.2. The DoD personnel shall receive periodic briefings on the threats posed by foreign intelligence services, international terrorists, computer intruders and unauthorized disclosures, and individual reporting responsibilities. This shall include insider threats and the crimes of spying and treason.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence (USD(I)) shall oversee the DoD Counterintelligence (CI) awareness, briefing, and reporting programs and ensure:

5.1.1. The Deputy Under Secretary of Defense (Counterintelligence and Security) (DUSD(CI&S)) shall establish and sustain the DoD CI awareness, briefing, and reporting programs.

5.1.2. The Director, Counterintelligence, under the DUSD(CI&S), shall:

5.1.2.1. Recommend policy on CI awareness, briefing, and reporting programs to the DUSD(CI&S) and the USD(I).

5.1.2.2. Provide oversight to the DoD CI Program.

5.1.2.3. Participate in DoD and national-level forums concerning CI awareness, briefing, and reporting programs.

5.1.2.4. Serve as the staff point of contact within OSD for issues related to CI awareness, briefing, and reporting programs.

5.1.3. The Director, Counterintelligence Field Activity (CIFA), under the DUSD(CI&S), shall:

5.1.3.1. Manage and provide functional oversight of the Department's CI awareness, briefing, and reporting programs.

5.1.3.2. Brief the USD(I) on significant CI investigative referrals received pursuant to this Instruction in accordance with DoD Directive 5105.67 (reference (i)).

5.1.3.3. Recommend policy changes through the DUSD(CI&S) to the USD(I).

5.1.3.4. Provide additional training to Component CI personnel on the skills required for the CI awareness, briefing, and reporting programs.

5.1.3.5. Represent the Department with other Government and management agencies regarding implementation of all DoD CI matters pursuant to reference (i).

5.1.4. The Director, Defense Security Service, under the DUSD(CI&S), shall recommend changes to DoD 5220.22-M (reference (j)) to the DUSD(CI&S), to implement this Instruction within cleared defense contractor facilities.

5.2. The Heads of the DoD Components shall:

5.2.1. Develop and implement CI briefing, awareness, and reporting programs within their organizations.

5.2.2. Promptly report any CI information developed from these programs to their organic or lead CI agency and to the CIFA pursuant to USD(I) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003 (reference (k)).

5.2.3. Establish time-sensitive reporting procedures pursuant to paragraph 6.3., below, for the DoD personnel during official or non-official overseas travel.

5.2.4. Ensure Component CI agencies report CI information through the Portico system.

5.2.5. Ensure Component CI agency CI information is appropriately documented in the Portico system. Information collected responsive to validated collection requirements shall be published via Intelligence Information Report on the Portico system.

5.3. The Director, Defense Intelligence Agency, shall, in addition to the responsibilities listed in paragraph 5.2., above, and in coordination with the Director, Joint Staff, develop and implement CI awareness, briefing, and reporting programs for the Chairman, Joint Chiefs of Staff.

5.4. Defense Agencies with organic CI organizations shall:

5.4.1. Ensure reported information regarding contractor personnel is referred to the Defense Security Service (DSS) and the Federal Bureau of Investigation (FBI).

5.4.2. Ensure reported information regarding military or DoD civilian personnel is referred to the appropriate Military Department CI agency or the FBI, as appropriate. Any information reported to the FBI shall also be reported to the CIFA pursuant to DoD Instruction 5240.4 (reference (l)).

5.5. The Secretaries of the Military Departments shall:

5.5.1. Ensure Department CI agencies refer reported information regarding contractor personnel to the DSS and the FBI.

5.5.2. Refer reported information regarding DoD civilian employees to the FBI for possible CI investigative or operational action where the Department does not otherwise have investigative authority. Any information reported to the FBI shall also be reported to the CIFA pursuant to reference (l).

6. PROCEDURES

6.1. Awareness and Briefing Programs

6.1.1. The DoD awareness and briefing programs shall promote threat and reporting awareness responsibility, enable DoD personnel to identify CI threats, and the reporting of suspicious situations and incidents to appropriate authorities.

6.1.2. Threat awareness may be enhanced through a variety of methods, including but not limited to publications, posters, live presentations, and recorded media.

6.1.3. CI Briefings shall include:

6.1.3.1. Information about early detection of espionage and other suspected foreign intelligence and international terrorist activities to include the crimes of sabotage, subversion, treason, and spying.

6.1.3.2. Comprehensive, tailored threat information focusing on foreign intelligence, international terrorism, and other threats to include insider threats relevant to the DoD Component's mission, functions, activities and locations.

6.1.3.3. Information addressing the DoD anomalies program pursuant to White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996 and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996 (references (m) and (n)), which remain in effect.

6.1.4. Briefings shall be presented at or near the time of initial entry or hire and thereafter at least every 12 months. More frequent briefing intervals should be instituted if conditions warrant. Some DoD Component organizations or personnel may require more frequent briefings predicated on the nature of their duties.

6.1.5. Briefings should be presented by the Component CI agency when feasible. If the servicing Component CI agency is not used, the briefings should be coordinated with them for content and accuracy.

6.1.6. Briefings conducted pursuant to this Instruction do not satisfy the requirement of DoD Directive 2000.12 (reference (o)).

6.2. Reporting Requirements

6.2.1. The DoD personnel shall report information pursuant to E.O. 12968 and DoD 5200.2-R (references (p) and (q)) concerning security violations and other information with potentially serious security significance regarding someone with access to classified information or who is employed in a sensitive position. Examples of information or observed behaviors that should be reported are listed in enclosure 3.

6.2.2. Pursuant to this Instruction, the DoD personnel shall expeditiously report any contacts or circumstances that could pose a threat to the security of U.S. personnel, DoD resources, and classified national security information or controlled unclassified information to an appropriate DoD authority.

6.2.2.1. Appropriate authorities for active duty and Reserve military personnel and DoD civilians and DoD contractors working in DoD Component facilities include security officers, supervisors, commanders, and organic or lead CI agencies. Security officers, supervisors, and commanders shall expeditiously refer any information they receive pursuant to this Instruction to their supporting CI agency.

6.2.2.2. Appropriate authorities for DoD contractors at cleared contractor facilities shall include Facility Security Officers, Military Department CI Agencies, the FBI, or the DSS pursuant to reference (1).

6.2.3. The DoD personnel shall report contacts pursuant to the following situations:

6.2.3.1. A request by anyone, regardless of nationality, for unauthorized access to classified information under DoD 5200.1-R (reference (r)); controlled unclassified information under references (f), (g), and DoD Directive 5230.25 (reference (s)); or information systems containing such information.

6.2.3.2. Contact with an individual, regardless of nationality, under circumstances that suggest the DoD personnel may be the target of an attempted exploitation by a foreign intelligence service or international terrorist organization.

6.2.3.3. Contact with a known or suspected intelligence officer from any country.

6.2.3.4. Contact with anyone receiving information of planned, attempted, actual, or suspected international terrorism, espionage, sabotage, subversion, or other intelligence activities against the Department of Defense, other U.S. facilities, U.S. organizations, or U.S. citizens.

6.2.3.5. Actual or attempted unauthorized access into U.S. automated information systems and/or unauthorized transmissions of classified or controlled unclassified information over on-line computer services and telephones.

6.2.3.6. Close and continuing associations with foreign nationals may also be reportable under Director of Central Intelligence Directive (DCID) 6/1, reference (t) and DCID 6/4, reference (u).

6.2.3.7. In addition to the aforementioned reporting requirements, personnel who occupy positions designated by their DoD Component as sensitive shall apprise their commanders or supervisors of the nature and purpose of any intended contact with any foreign diplomatic establishment whether in the United States or abroad.

6.3. Sanctions. The DoD personnel who fail to report information required by this Instruction may be subject to judicial and/or administrative action under applicable law and regulations, including the Uniform Code of Military Justice (reference (v)), and other applicable sections of the United States Code.

6.4. Other

6.4.1. DoD acquisition program personnel working with Critical Program Information pursuant to DoD Directive 5200.39 (reference (w)) shall notify their servicing security personnel of all projected foreign travel. Such personnel shall

receive foreign intelligence threat briefings and anti-terrorism briefings prior to overseas travel.

6.4.2. The DoD personnel with access to Sensitive Compartmented Information (SCI) pursuant to DCID 1/20 (reference (x)) incur special security obligations that include advance foreign travel notification for official and/or unofficial travel and defensive travel briefings.

7. EFFECTIVE DATE

This Instruction is effective immediately.



Stephen A. Cambone
Under Secretary of Defense for Intelligence

Enclosures - 3

- E1. References, continued
- E2. Definitions
- E3. Examples of Reportable Employee Behaviors

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Executive Order 12958, "Classified National Security Information," April 17, 1995
- (f) [DoD Directive 5230.24](#), "Distribution Statements on Technical Documents," March 18, 1987
- (g) [DoD 5400.7-R](#), "DoD Freedom of Information Act Program," September 4, 1998
- (h) [DoD Directive 5210.83](#), "Department of Defense Unclassified Nuclear Information (DoD UCNI)," November 15, 1991
- (i) [DoD Directive 5105.67](#), "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002
- (j) [DoD 5220.22-M](#), "National Industrial Security Program Operating Manual," January 1999
- (k) Under Secretary of Defense (Intelligence) Memorandum, "Reporting Significant Counterintelligence Activity," July 19, 2003
- (l) [DoD Instruction 5240.4](#), "Reporting of Counterintelligence and Criminal Violations," September 22, 1992
- (m) White House Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996²
- (n) Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," October 15, 1996³
- (o) [DoD Directive 2000.12](#), "DoD Antiterrorism (AT) Program," August 18, 2003
- (p) Executive Order 12968, "Access to Classified Information," August 2, 1987
- (q) [DoD 5200.2-R](#), "Personnel Security Program," January 1987
- (r) [DoD 5200.1-R](#), "DoD Information Security Program," January 16, 1997
- (s) [DoD Directive 5230.25](#), "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984
- (t) Director of Central Intelligence Directive 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual," March 1, 1995⁴

² Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

³ Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

⁴ Available to authorized users via DoD Secure Internet Protocol Route Network (SIPRNET).

- (u) Director of Central Intelligence Directive 6/4, "Personnel Security Standards," July 2, 1998⁵
- (v) Section 801-940, Chapter 47, of title 10, United States Code, "Uniform Code of Military Justice"
- (w) [DoD Directive 5200.39](#), "Security, Intelligence and Counterintelligence Support to Acquisition Program Protection," September 10, 1997
- (x) Director of Central Intelligence Directive 1/20, "Security Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI)," December 29, 1991⁶
- (y) Sections 792-799, Chapter 37 of title 18, United States Code

⁵ Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

⁶ Contact the Counterintelligence Directorate, DUSD(CI&S), USD/I, Room 3C260, 6000 Defense Pentagon, Washington DC 20301-6000 to obtain a copy.

E2. ENCLOSURE 2

DEFINITIONS

E2.1. DEFINED TERMS

E2.1.1. Anomalies. Foreign power activity or knowledge suggesting foreign knowledge of U.S. national security information, processes or capabilities.

E2.1.2. Classified Information. Information requiring protection in the interest of national security, classified "TOP SECRET, SECRET, or CONFIDENTIAL" according to reference (x).

E2.1.3. Contact. Any form of meeting, association, or communication in person; by radio, telephone, letter, computer; or other means, regardless of who initiated the contact for social, official, private, or other reasons.

E2.1.4. Controlled Unclassified Information. Data bearing distribution limitation statements such as "For Official Use Only" in accordance with reference (g) and other information marked under references (f) and (g).

E2.1.5. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

E2.1.6. Counterintelligence Investigations. Are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow Defense Agency and Military Department directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve the security posture of threatened interests.

E2.1.7. Defensive Travel Briefings. Formal advisories alerting personnel of the potential for harassment, exploitation, provocation, capture, or entrapment while traveling. These briefings, based on actual experience when available, include information on courses of action helpful in mitigating adverse security and personnel consequences and advise of passive and active measures that personnel should take to avoid becoming targets or inadvertent victims as a consequence of hazardous travel.

E2.1.8. DoD Component CI Organizations. The organic CI elements of the Army, the Navy, the Air Force, the Marine Corps, the Joint Staff, the Combatant Command Staffs, the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, the Defense Security Service, the Defense Threat Reduction Agency, and the Missile Defense Agency and the CIFA.

E2.1.9. Espionage. Defined under Sections 792-799, Chapter 37, title 18, United States Code (reference (y)) and Article 106a, Uniform Code of Military Justice (UCMJ) (reference (v)).

E2.1.9.1. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies during war or peace.

E2.1.9.2. Reference (y) makes it an offense to gather, with the requisite intent or belief, national defense information, by going on, entering, flying over, or obtaining access by any means to any installation or place used by the United States for national defense. The method of gathering that information is immaterial.

E2.1.9.3. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense, which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it may be punished under reference (y).

E2.1.9.4. Anyone entrusted with or having lawful possession or control of information about national defense, who through gross negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of that trust may be punished under reference (y).

E2.1.9.5. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of reference (y).

E2.1.10. Foreign Diplomatic Establishment. Any embassy, consulate, or interest section representing a foreign country.

E2.1.11. Lead CI Agency. A Military Department CI Agency that has been designated by the USD(I) to provide defined levels of CI support to one or more of the DoD Components.

E2.1.12. Military Department CI Agencies. The Military Department CI Agencies include the U.S. Army Counterintelligence, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

E2.1.13. National Security. A collective term encompassing both national defense and foreign relations of the United States.

E2.1.14. Portico. A program managed by the CIFA to provide automation support, through web-enabled software hosted on a robust infrastructure, to the DoD CI Community. Portico enables CI enterprise business processes; facilitates information sharing, and coordination across DoD Services and Agencies; and provides management tools for each CI functional area, as well as supporting tools and services for managing the CI process in the functional areas of Collection; Investigations; Analysis and Production; Operations; and CI Functional Services.

E2.1.15. Sabotage. An act or acts with the intent to injure or interfere with, or obstruct the national defense of a country by willfully injuring, destroying, or attempting to destroy any national defense or war materiel, premises or utilities to include human or natural resources, under reference (y).

E2.1.16. Spying. During wartime, any person who is found lurking as a spy or acting as a spy in or about any place, vessel or aircraft, within the control or jurisdiction of any of the Armed Forces or in or about any shipyard, any manufacturing or industrial plant, or any other place or institution engaged in work in aid of the prosecution of the war by the United States, or elsewhere.

E2.1.17. Subversion. An act or acts inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities with the willful intent thereby to interfere with, or impair the loyalty, morale, of discipline, of the Military Forces of the United States.

E2.1.18. Terrorism. The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

E2.1.19. Treason. Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason (see Section 2381 of title 18, U.S. Code, reference (y)).

E2.1.20. Unauthorized Disclosure. A communication or physical transfer of classified information to an unauthorized recipient.

E3. ENCLOSURE 3

EXAMPLES OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1. LIST OF REPORTABLE EMPLOYEE BEHAVIORS

E3.1.1. Unauthorized contact with an individual who is known or suspected of being associated with a foreign intelligence, security, or terrorist organization.

E3.1.2. Illegal activity, conduct or requests for participation in illegal activities or other conduct that might make someone susceptible to blackmail or result in a security violation.

E3.1.3. Reading or discussing classified or controlled unclassified information in an unauthorized location, such as while using public transportation.

E3.1.4. Attempts to obtain classified or other protected information in any format to which the requesting person does not have authorized access.

E3.1.5. Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

E3.1.6. Unauthorized possession and/or operation of cameras, recording devices, computers, or modems in areas wherein classified information and data are stored, discussed, or processed.

E3.1.7. The existence or use of any unauthorized listening or surveillance devices in sensitive or secure areas.

E3.1.8. Keeping classified material at home or any other unauthorized place.

E3.1.9. Acquiring access to classified or unclassified automated information systems without proper authorization.

E3.1.10. Transmitting classified material over unclassified FAX or computer.

E3.1.11. Seeking to obtain access to sensitive information inconsistent with present duty requirements.

E3.1.12. Removing classified or controlled unclassified material from work areas without appropriate authorization by any means.

E3.1.13. Improperly removing security classification markings from documents.

E3.1.14. Discussing classified information on a non-secure, unencrypted telephone.

E3.1.15. Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities.

E3.1.16. Extensive use of copy, facsimile, or computer equipment to reproduce or transmit classified material that may exceed job requirements.

E3.1.17. Repeated or un-required work outside of normal duty hours, especially unaccompanied.

E3.1.18. Unexplained or undue affluence, including sudden purchases of high value items (i.e., real estate, stocks, vehicles, or vacations) where no logical income source exists. Attempts to explain wealth by reference to inheritance, luck in gambling, or some successful business venture.

E3.1.19. Sudden reversal of a bad financial situation or repayment of large debts.

E3.1.20. Attempts to entice DoD personnel into situations that could place them in a compromising position.

E3.1.21. Attempts to place DoD personnel under obligation through special treatment, favors, gifts, money or other means.

E3.1.22. Short trips to foreign countries or travel within the United States to cities with foreign diplomatic activities for reasons that appear unusual or inconsistent with a person's interests or financial means.