Department of Defense
DIRECTIVE

NUMBER 5240.06
May 17, 2011
Incorporating Change 2, July 21, 2017

USD(I)

SUBJECT: Counterintelligence Awareness and Reporting (CIAR)

References: See Enclosure 1

1. PURPOSE. This Directive:

a. Reissues DoD Instruction (DoDI) 5240.6 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (b)).

b. Establishes policy, assigns responsibilities, and provides procedures for CIAR in accordance with DoDD ~~O~~ 5240.02 (Reference (c)).

c. Lists reportable contacts, activities, indicators, and behaviors associated with foreign intelligence entities (FIEs), a term that includes international terrorists.

d. Establishes that persons subject to chapter 47 of title 10, United States Code, hereinafter referred to as the Uniform Code of Military Justice (UCMJ) (Reference (d)) who violate specific provisions of this issuance may be subject to punitive action under Article 92, UCMJ.

e. Establishes that civilian employees under their respective jurisdictions who violate specific provisions of this issuance may be subject to appropriate disciplinary action under regulations governing civilian employees.

f. Includes reportable FIE-associated cyberspace contacts, activities, indicators, and behaviors.

g. Establishes the CIAR Council (CIARC) in accordance with DoDI 5105.18 (Reference (e)).

2. APPLICABILITY. This Directive applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff

and the Joint 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 within the DoD (hereinafter referred to collectively as the "DoD Components").

b. Active and reserve military personnel, as well as DoD civilian employees (hereinafter referred to collectively as "DoD personnel").

c. The requirements of this Directive will be incorporated into DoD contracts, as appropriate, and made applicable to those contracts.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. Initial and annual CIAR training on the FIE threat, methods, reportable information, and reporting procedures shall be provided to DoD personnel as outlined in Enclosure 3.

b. Potential FIE threats to the DoD, its personnel, information, materiel, facilities, and activities, or to U.S. national security shall be reported by DoD personnel in accordance with Enclosure 4.

c. Failure to report FIE threats as identified in paragraph 3.a and section 5 of Enclosure 4 of this Directive may result in judicial or administrative action or both pursuant to applicable law or policy.

(1) Persons subject to the UCMJ who violate specific provisions of this issuance may be subject to punitive action under Article 92, UCMJ.

(2) Civilian employees under their respective jurisdictions who violate specific provisions of this issuance may be subject to appropriate disciplinary action under regulations governing civilian employees.

d. The collection, retention, and dissemination of U.S. person information shall be in accordance with DoD 5240.1-R (Reference (f)) and paragraph 3.e. of Enclosure 3 of this Directive.

e. CIAR records shall be maintained in accordance with ~~DoDD 5015.2~~ *DoDI 5015.02* (Reference (g)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosures 3 through 5.

7. INFORMATION COLLECTION*S* ~~REQUIREMENTS~~. The information requirement

contained in this Directive is exempt from licensing in accordance with ~~paragraphs C4.4.1., C4.4.7., and C4.4.8.~~ *Paragraphs 1.b.(3), 1.b.(6), and 1.b.(8) of Volume 1* of DoD *Manual* 8910.*0*1~~-M~~ (Reference (h)).

8. RELEASABILITY. ~~UNLIMITED. This Directive is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.~~ ***Cleared for public release***. *This directives is available on the Directives Division Website at http://www.esd.whs.mil/DD/.*

9. EFFECTIVE DATE. This Directive~~:~~ *is effective May 17, 2011.*

~~a. Is effective May 17, 2011.~~

~~b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DoD Instruction 5025.01 (Reference (i)). If not, it will expire effective May 17, 2021 and be removed from the DoD Issuances Website.~~

William J. Lynn III
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities
3. Awareness Training
4. Reporting
5. CIARC

Glossary

TABLE OF CONTENTS

TABLES

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 5240.6, "Counterintelligence (CI) Awareness, Briefing, and Reporting Programs," August 7, 2004 (hereby cancelled)
(b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," ~~November 23, 2005~~ *October 29, 2014, as amended*
(c) DoD Directive ~~O~~ 5240.02, "Counterintelligence *(CI)*," ~~December 20, 2007, as amended~~ *March 17, 2015*
(d) Chapter 47 of title 10, United States Code (also known as "The Uniform Code of Military Justice")
(e) DoD Instruction 5105.18, "DoD Intergovernmental and Intragovernmental Committee Management Program," July 10, 2009
(f) DoD 5240.1-R, "Activities of DoD Intelligence Components that Affect United States Persons," December 1982
(g) ~~DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000~~ *DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015*
(h) ~~DoD 8910.1-M "Department of Defense Procedures for Management of Information Requirements," June 30, 1998~~ *DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collection," June 30, 2014, as amended*
~~(i) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012~~
(~~j~~*i*) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," ~~February 2, 2009~~ *April 1, 2016,*
(~~k~~*j*) DoD Instruction S-5240.09, "*(U)* Offensive Counterintelligence Operations (OFCO) ~~(U)~~," ~~October 29, 2008~~ *February 2, 2015, as amended*
(~~l~~*k*) DoD Instruction S-5240.17, "*(U)* Counterintelligence Collection *Activities (CCA)* ~~(U)~~," ~~January 12, 2009~~ *March 14, 2014*
(~~m~~*l*) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009*, as amended*
(~~n~~*m*) Assistant to the President for National Security Affairs Memorandum, "Early Detection of Espionage and Other Intelligence Activities Through Identification and Referral of Anomalies," August 23, 1996[1]
(~~o~~*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, 1996
(~~p~~*o*) DoD Instruction 3305.11, "DoD Counterintelligence (CI) Training *and Certification,"* ~~March 19, 2007, as amended~~ *August 13, 2015*
(~~q~~*p*) DoD Instruction 3305.12, "Intelligence and Counterintelligence (I&CI) Training of Non-U.S. Persons," ~~October 25, 2007, as amended~~ *October 14, 2016*
(~~r~~*q*) DoD Instruction 2000.12, "DoD Antiterrorism (AT) Program," March 1, 2012*, as amended*
(~~s~~*r*) DoD Instruction 5200.39, ~~"Critical Program Information (CPI) Protection Within the Department of Defense," July 16, 2008, as amended~~ *"Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015*

(~~t~~*s*) Director of Central Intelligence Directive 1/20P, "Security Policy Concerning Travel and Assignment of Personnel With Access to Sensitive Compartmented Information (SCI)," December 29, 1991[1]

(~~u~~*r*) Revision 1 to the DoD Overprint to the National Industrial Security Program Operating Manual Supplement, April 1, 2004

(~~v~~*u*) DoD Manual 5200.01, Volumes 1-4, "DoD Information Security Program," February 24, 2012

(~~w~~*v*) DoD Instruction ~~8500.2, "Information Assurance (IA) Implementation," February 6, 2003~~ *8500.01, "Cybersecurity," March 14, 2014*

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

[1] Copies are available to authorized users on the Internet at http://www.intelink.ic.gov/ppr/strategyplanspolicy.intell/

ENCLOSURE 2

RESPONSIBILITIES

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

a. Monitor implementation of this Directive and issue such additional direction and guidance as necessary.

b. Resolve issues concerning CIAR that cannot be resolved by the DoD Components.

2. DEPUTY UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (DUSD(I&S)). The DUSD(I&S), under the authority, direction, and control of the USD(I), shall:

a. Provide policy oversight of CIAR; develop and recommend CIAR policy to the USD(I).

b. Participate in DoD and national-level CIAR forums.

3. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). The Director, DIA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 5 of this enclosure, shall:

a. Provide for centralized management of CIAR.

b. Conduct analysis of FIE threats and disseminate finished products to the DoD Components.

c. Coordinate, deconflict, and centrally manage CIAR.

d. Appoint the CIAR functional manager and the Chair to the CIARC.

e. Report trends, anomalies, and other matters of counterintelligence (CI) interest to the DUSD(I&S) in accordance with DoDIs 5240.04, S-5240.09, S-5240.17, and O-5240.21 (References (~~j~~*i*) through (~~m~~*l*)); Assistant to the President for National Security Affairs Memorandum (Reference (~~n~~*m*)); and Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum (Reference (~~o~~*n*)).

f. Coordinate with the appropriate DIA analysis element to analyze information gleaned from CI investigations, operations, collection, and inquiries.

g. Assist the DoD Components in obtaining finished DIA products for use in Component CIAR training and provide materials to support CI training of DoD personnel in accordance with DoDI 3305.11 (Reference (~~p~~*o*)) and non-U.S. persons, in accordance with DoDI 3305.12 (Reference (~~q~~*p*)).

4. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). The Director, DSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 5 of this enclosure, shall provide CIAR advice and assistance to cleared contractors, in accordance with applicable contracts.

5. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Establish and implement a CIAR program within their respective Components.

b. Provide finished intelligence materials to trainers in support of CIAR.

c. Maintain CIAR training records in accordance with Enclosure 3 of this Directive to document participation in annual CIAR training requirements.

d. Report potential FIE threats to their organization's CI element or their supporting Military Department CI Organization (MDCO).

e. Administer judicial or administrative action, as appropriate, pursuant to applicable law or policy when DoD personnel fail to report FIE threats. Persons subject to the UCMJ who violate specific provisions of this Directive may be subject to punitive action under Article 92, UCMJ. Civilian employees under their respective jurisdictions who violate specific provisions of this Directive may be subject to appropriate disciplinary action under regulations governing civilian employees.

ENCLOSURE 3

AWARENESS TRAINING

1. GENERAL. CIAR training shall include instruction on:

a. The threat from FIEs.

b. The methods, also known as "modus operandi," of FIEs.

c. FIE use of the Internet and other communications including social networking services (SNS).

d. The CI insider threat.

e. Anomalies in accordance with References (~~m~~*l*) and (~~n~~*m*).

f. Reporting responsibilities regarding foreign travel and foreign contacts.

g. The reporting requirements in Enclosure 4.

2. INDIVIDUAL TRAINING REQUIREMENTS

a. All DoD personnel shall receive CIAR training in accordance with this Directive.

b. Failure to receive training does not relieve individuals from their reporting responsibilities in Enclosure 4 of this Directive.

3. DoD COMPONENT TRAINING REQUIREMENTS. DoD Components shall:

a. Provide CIAR training to DoD personnel within 30 days of initial assignment or employment to the Component and every 12 months thereafter.

b. Provide CIAR training with a CI-experienced person in a classroom environment.

(1) When a CI-experienced person is not available, an individual knowledgeable of CIAR may conduct the training; however, the Component shall provide the training materials to the organizational CI element or supporting MDCO for review.

(2) When classroom training is not feasible, provide CIAR training through other media.

c. Provide CIAR training tailored to their Component's mission, functions, activities, and locations.

d. Record CIAR training in a DoD Component or USD(I)-approved CI information system~~s~~ in accordance with Reference (c) and, upon request, make the record available to the supporting MDCO and the CIAR functional manager. The record shall identify the:

(1) Organization receiving the training.

(2) Attendees.

(3) Trainer and his or her organization.

(4) Date(s) of training.

(5) Subject of the training and a summary of the training content.

e. Maintain training records for a period of 5 years in accordance with Reference (e) and other applicable records management policy.

f. Conduct training in compliance with this Directive in addition to the antiterrorism training requirements of DoDI 2000.12 (Reference (~~r~~*q*)).

4. CI SUPPORT TO CIAR TRAINING. The MDCOs and organizational CI elements shall:

a. Provide their supported Components with assistance to establish and maintain CIAR training.

b. Upon request and when possible, provide their supported Components with a CI-experienced person to conduct the CIAR training.

c. When unable to provide a CI-experienced person to conduct training, review Component CIAR training materials for accuracy and completeness.

5. FOREIGN TRAVEL. DoD personnel with access to:

a. Critical program information shall notify their security personnel of all projected foreign travel in accordance with DoDI 5200.39 (Reference (~~s~~*r*)). Personnel who travel to overseas locations shall receive foreign intelligence threat briefings and anti-terrorism briefings prior to their departure.

b. Sensitive compartmented information shall meet their special security obligations, including advance foreign travel notification for official and unofficial travel and receipt of defensive travel briefings, in accordance with Director of Central Intelligence Directive 1/20P (Reference (~~t~~*s*)).

c. Special access program information shall notify their security personnel of all projected foreign travel. Such personnel shall receive foreign intelligence threat briefings and anti-

terrorism briefings prior to overseas travel in accordance with the DoD Overprint to the National Industrial Security Program Operating Manual Supplement (Reference (~~ut~~*t*)).

ENCLOSURE 4

REPORTING

1. GENERAL. DoD personnel shall report, in accordance with section 3 of this enclosure, the contacts, activities, indicators, and behaviors in section 5 of this enclosure.

2. FAILURE TO REPORT. DoD personnel who fail to report information as required in paragraph 3.a and section 5 of this enclosure that identifies reportable contacts, activities, indicators and behaviors, may be subject to judicial or administrative action, or both, pursuant to applicable law and regulations.

a. Persons subject to the UCMJ who violate the referenced specific provisions of this Directive may be subject to punitive action under Article 92, UCMJ.

b. Civilian employees under their respective jurisdictions who violate the referenced specific provisions of this Directive may be subject to appropriate disciplinary action under regulations governing civilian employees.

3. REPORTING REQUIREMENTS

a. DoD personnel shall report the contacts, activities, indicators, and behaviors stated in section 5 of this enclosure as potential FIE threats against the DoD, its personnel, information, materiel, facilities, and activities, or against U.S. national security.

b. DoD personnel shall report potential FIE threats to their organization's CI element or their supporting MDCO.

(1) When CI support is not available, DoD personnel shall report the threat without delay to their security officer, supervisor, or commander.

(2) Security officers, supervisors, and commanders shall forward reported information to their organizational CI element or their supporting MDCO within 72 hours.

c. DoD personnel, and their security officers, supervisors, and commanders, shall also comply with all other applicable reporting requirements, including those in accordance with DoD Manual 5200.01 (Reference (~~v~~*u*) and DoDI ~~8500.2~~ *8500.01* (Reference (~~w~~*v*)).

4. ACTIONS ON REPORTED INFORMATION. Upon receiving information on reportable contacts, activities, indicators, and behaviors, the MDCOs and organizational CI elements shall:

a. Take appropriate and authorized action in accordance with References (~~j~~*i*) through (~~o~~*n*).

b. In the event a contact, activity, indicator, or behavior is not associated with FIE, report such contacts, activities, indicators, and behaviors, to include self-radicalization, to the appropriate law enforcement or command authorities.

c. Inform the DoD Components about reported incidents, as appropriate, to allow the DoD Components to implement protection measures.

5. REPORTABLE CONTACTS, ACTIVITIES, INDICATORS, AND BEHAVIORS. Tables 1 through 3 contain reportable contacts, activities, indicators, behaviors, and cyber threats associated with FIEs.

a. Table 1. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 22 may be subject to judicial and/or administrative action in accordance with section 2 of this enclosure. The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action under Article 92, UCMJ.

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors

1.	When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through SNS that is not related to official duties.
2.	Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.
3.	Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.
4.	Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.
5.	Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.
6.	Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.
7.	Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.
8.	Discovery of suspected listening or surveillance devices in classified or secure areas.
9.	Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.
10.	Discussions of classified information over a non-secure communication device.

Table 1. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors, continued

11.	Reading or discussing classified or sensitive information in a location where such activity is not permitted.
12.	Transmitting or transporting classified information by unsecured or unauthorized means.
13.	Removing or sending classified or sensitive material out of secured areas without proper authorization.
14.	Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
15.	Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.
16.	Improperly removing classification markings from documents or improperly changing classification markings on documents.
17.	Unwarranted work outside of normal duty hours.
18.	Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.
19.	Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.
20.	Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.
21.	Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.
22.	Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or SNS.
23.	Trips to foreign countries that are: a. Short trips inconsistent with logical vacation travel or not part of official duties. b. Trips inconsistent with an individual's financial ability and official duties.
24.	Unexplained or undue affluence. a. Expensive purchases an individual's income does not logically support. b. Attempts to explain wealth by reference to an inheritance, luck in gambling, or a successful business venture. c. Sudden reversal of a bad financial situation or repayment of large debts.

b. Table 2. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 9 may be subject to judicial and/or administrative action in accordance with section 2 of this enclosure. The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action under Article 92, UCMJ.

Table 2. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors

1.	Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.
2.	Advocating support for a known or suspected international terrorist organizations or objectives.
3.	Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.
4.	Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.
5.	Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.
6.	Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.
7.	Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.
8.	Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.
9.	Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.
10.	Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

c. Table 3. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 10 may be subject to judicial and/or administrative action in accordance with section 2 of this enclosure. The indicators in items 11 through 19 are reportable, but failure to report these indicators may not alone serve as the basis for punitive action under Article 92, UCMJ.

Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors

1.	Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2.	Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3.	Network spillage incidents or information compromise.
4.	Use of DoD account credentials by unauthorized parties.

Table 3. Reportable FIE-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors, continued

5.	Tampering with or introducing unauthorized elements into information systems.
6.	Unauthorized downloads or uploads of sensitive data.
7.	Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8.	Downloading or installing non-approved computer applications.
9.	Unauthorized network access.
10.	Unauthorized e-mail traffic to foreign destinations.
11.	Denial of service attacks or suspicious network communications failures.
12.	Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13.	Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14.	Data exfiltrated to unauthorized domains.
15.	Unexplained storage of encrypted data.
16.	Unexplained user accounts.
17.	Hacking or cracking activities.
18.	Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19.	Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

ENCLOSURE 5

CIARC

1. PURPOSE. The CIARC shall serve as the principal forum for sharing information on CIAR training programs, lessons learned, courses of action, and the FIE threat.

2. MEMBERSHIP. The Director, DIA, shall appoint the CIARC Chair. Core membership shall consist of a CI representative from the USD(I) staff, the Joint Staff, MDCOs, and the Marine Corps CI. The Chair may expand membership to include security and information assurance personnel and other full-time or permanent part-time Federal employees or military personnel.

3. MEETINGS. The CIARC shall convene at least quarterly to discuss CI issues. At the discretion of the Chair, it may meet by video teleconference or other electronic media. The Chair shall set the agenda with input provided by the members.

4. ACTIVITIES. The CIARC shall:

a. Seek to identify best practices for CIAR.

b. Provide advice to the DoD Components on CIAR training.

c. Identify emerging trends in CIAR and assist the DoD Components in incorporating new information into CIAR training. Trends and new information shall include, but not be limited to:

(1) Targets of foreign collection.

(2) FIE modus operandi.

(3) Cyberspace trends.

(4) CI insider threat.

d. Serve as the principal advisory body to the Director, DIA, on CIAR issues, identify gaps in or issues with current policy, and recommend courses of action.

e. Promote information sharing and collaboration on CIAR training throughout the DoD.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CI	counterintelligence
CIAR	CI awareness and reporting
CIARC	CIAR Council
DIA	Defense Intelligence Agency
DoDD	DoD Directive
DoDI	DoD Instruction
DSS	Defense Security Service
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
FIE	foreign intelligence entity
MDCO	Military Department Counterintelligence Organization
SNS	social networking services
UCMJ	Uniform Code of Military Justice
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

These terms and their definitions are for the purposes of this Directive.

anomaly. Activity or knowledge, outside the norm, that suggests a foreign entity has foreknowledge of U.S. information, processes, or capabilities.

CI. Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

CI awareness. An individual's level of comprehension as to the FIE threat, methods, indicators, and reporting requirements.

CI insider threat. A person who uses their authorized access to DoD facilities, systems, equipment, information or infrastructure to damage, disrupt operations, compromise DoD information or commit espionage on behalf of an FIE.

FIE. Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorist organizations.

MDCO. Elements of the Military Departments authorized to conduct CI investigations, i.e., Army CI, Naval Criminal Investigative Service, and the Air Force Office of Special Investigations. The term "supporting MDCO" replaces "Lead CI Agency" as defined in DoDI 5240.10 (Reference (~~x~~*w*)).

self-radicalization. Significant steps an individual takes in advocating or adopting an extremist belief system for the purpose of facilitating ideologically-based violence to advance political, religious, or social change. The self-radicalized individual has not been recruited by and has no direct, personal influence or tasking from other violent extremists. The self-radicalized individual may seek out direct or indirect (through the Internet for example) contact with other violent extremists for moral support and to enhance his or her extremist beliefs.