Department of Defense
INSTRUCTION

NUMBER 5240.26
May 4, 2012
Incorporating Change 1, Effective October 15, 2013

USD(I)

SUBJECT: Countering Espionage, International Terrorism, and the Counterintelligence (CI) Insider Threat

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Establishes policy, assigns responsibilities, and provides procedures for CI activities to counter espionage and international terrorist threats to DoD in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)).

b. Implements policy in DoDD O-5240.02 (Reference (b)) and DoD Instruction (DoDI) O-5100.93 (Reference (c)) to identify and counter foreign intelligence entities (FIEs).

c. Establishes policy and assigns responsibilities for the CI Insider Threat Program in support of other DoD Insider Threat programs consistent with the Secretary of Defense Memorandum (Reference (d)) and Executive Order 13587 (Reference (e)).

d. Establishes the Insider Threat CI Group (ITCIG).

2. APPLICABILITY. This Instruction applies to 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").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. In accordance with Reference (b) and DoDI 2000.12 (Reference (f)), countering espionage and international terrorism shall be an integrated CI mission to detect, identify, exploit, assess, and deny efforts by FIEs to recruit DoD-affiliated personnel.

b. Countering insider threats are coordinated CI, security, information assurance (IA), law enforcement (LE), and antiterrorism and force protection (AT/FP) activities that shall be accomplished in accordance with References (b) through (f) and DoDI 5240.05, DoDD 5240.06, DoDI 5240.16, DoDI 5240.19, DoDI O-5240.21, DoDD 5210.48, DoDD 8500.01E, the Assistant to the President for National Security Affairs Memorandum, and Intelligence Community Standard 700-2 (References (g) through (o)).

c. CI insider threat information shall be shared within the Intelligence Community (IC) and with other departments and agencies in accordance with Executive Order 12333 (Reference (p)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. INFORMATION COLLECTION REQUIREMENTS. The report of anomalies associated with CI insider threats referenced in paragraph 2.a. of Enclosure 3 of this Instruction is exempt from licensing requirements in accordance with C4.4.7. of DoD 8910.1-M and the Secretary of Defense Memorandum (References (q) and (r)).

8. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

9. EFFECTIVE DATE. *This instruction:*

a. ~~This Instruction is~~ *Is* effective May 4, 2012.

b. ~~This Instruction~~ ~~m~~*M*ust be reissued, cancelled, or certified current within 5 years of its publication *to be considered current* in accordance with DoDI 5025.01 (Reference (s)).

c. ~~If not, this Instruction w~~*W*ill expire effective May 4, 2022 and be removed from the DoD Issuances Website *if it hasn't been reissued or cancelled in accordance with Reference (s)*.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," November 23, 2005
(b) DoD Directive O-5240.02, "Counterintelligence," December 20, 2007, *as amended*
(c) DoD Instruction O-5100.93, "Defense Counterintelligence (CI) and Human Intelligence (HUMINT) Center (DCHC)," August 13, 2010
(d) Secretary of Defense Memorandum, "(U) Information Security and Assurance Measures to Mitigate Unauthorized Removal of Information from Classified Networks," February 10, 2011
(e) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011
(f) DoD Instruction 2000.12, "DoD Antiterrorism (AT) Program," March 1, 2012
(g) DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM) Program," February 22, 2006
(h) DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011*, as amended*
(i) DoD Instruction 5240.16, "~~DoD~~ Counterintelligence Functional Services *(CIFS*)," ~~May 21, 2005~~ *August 27, 2012*
(j) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program," August 27, 2007, *as amended*
(k) DoD Instruction O-5240.21, "Counterintelligence (CI) Inquiries," May 14, 2009, *as amended*
(l) DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007, *as amended*
(m) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(n) 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
(o) Intelligence Community Standard Number 700-2, "Use of Audit Data for Insider Threat Detection," June 2, 2011
(p) Executive Order 12333, "United States Intelligence Activities," December 4, 1981 (as amended)
(q) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
(r) Secretary of Defense Memorandum, "Track Four Efficiency Initiative Decisions," March 14, 2011
(s) DoD Instruction 5025.01, "DoD Directives Program," ~~October 28, 2007~~ *September 26, 2012, as amended*
(t) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1, 1982
(u) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," February 2, 2009

(v) DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004
(w) DoD Instruction 5240.10, "Counterintelligence (CI) in the Combatant Commands and Other DoD Components," October 5, 2011
(x) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(y) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, *as amended*

ENCLOSURE 2

RESPONSIBILITIES

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

a. Monitor implementation of this Instruction and establish additional policy and provide direction as necessary.

b. Oversee the integration of CI Insider Threat Program activities with other DoD insider threat programs.

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. Develop and recommend CI and security policy to counter espionage, international terrorism, and the CI insider threat.

b. Provide policy oversight of all activities covered by this Instruction.

c. Represent the USD(I) at DoD and national-level forums concerning countering espionage, international terrorism, and the CI insider threat.

d. Ensure CI insider threat education is within security policy and training programs in coordination with the ~~Defense Counterintelligence and Human Intelligence Center (DCHC),~~ *Defense Intelligence Agency (DIA).*

e. Oversee security policy and a system to record and analyze security incidents and violations by a current DoD-affiliated person.

f. Oversee security policy and a system allowing analytical assessments of administrative and security anomalies and threats of DoD-affiliated persons.

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 of section ~~8~~ *7* of this enclosure, shall:

a. Incorporate CI insider threat information requirements into other intelligence collection requirements.

b. ~~Oversee Director, DCHC, i~~*I*mplement~~ation of~~ the procedures in Enclosure 3.

~~4. DIRECTOR, DCHC. The Director, DCHC, under the authority, direction, and control of the Director, DIA, shall:~~

~~a~~ *c.* Serve as the functional manager for the CI Insider Threat Program.

~~b~~ *d.* Serve as the functional manager for the DoD CI Enterprise to identify and neutralize FIEs.

~~c~~ *e.* In coordination with the DoD CI Enterprise, establish an overall CI Insider Threat Program strategy and implementation plan.

~~d~~ *f.* Ensure the CI Insider Threat Program is aligned with national strategies and objectives.

~~e~~ *g.* Establish CI Insider Threat Program standards.

~~f~~ *h.* Identify CI requirements and expectations from the security, IA, LE, and AT/FP disciplines, and provide CI support to those disciplines.

~~g~~ *i.* Assist in the development of CI insider threat policy, doctrine, and identification of emerging capabilities, as well as tactics, techniques, and procedures.

~~h~~ *j.* Ensure alignment to the CI Insider Threat Program of elements defined in Enclosure 3.

~~i~~ *k.* Identify best practices and disseminate across the DoD CI Enterprise.

~~j~~ *l.* Represent the DoD CI Insider Threat Program to the IC.

~~k~~ *m.* Develop and implement, with input from the DoD Chief Information Officer (DoD CIO), tactics, techniques, and procedures for CI analysis of IA auditing and monitoring capabilities.

~~l~~ *n.* Establish and maintain the ITCIG.

~~m~~ *o.* Ensure the CI, security, IA, LE, and AT/FP communities are represented in CI insider threat working groups, meetings, and symposia.

~~n~~ *p.* Incorporate CI insider threat training into the Joint CI Training Academy curriculum.

~~o~~ *q.* Coordinate with the DoD Cyber Crime Center to implement CI insider threat training into the technical analysis curriculum.

~~p~~ *r.* Incorporate CI insider threat awareness into CI awareness and reporting training in accordance with Reference (h).

~~q~~ *s.* Review and evaluate reports that indicate a CI insider threat from an unknown DoD-affiliated person in accordance with Enclosure 3.

~~r~~ *t.* Conduct analysis of anomalies as reported by the DoD Components in support of the CI Insider Threat Program in accordance with Enclosure 3 and Reference (n).

~~s~~ *u.* Develop procedures for the exchange of information on insider threat activities, anomalies, and other applicable areas of interest to the DoD Components, Military Department Counterintelligence Organizations (MDCOs), and Military Departments.

~~5~~*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 ~~8~~ *7* of this enclosure, shall:

a. Ensure CI insider threat awareness and counter-measures information is included within security training.

b. Provide instruction and assistance to DoD-cleared defense contractors regarding CI insider threat awareness and reporting procedures.

~~6~~*5*. DoD CIO. The DoD CIO shall:

a. Develop IA policies to support the CI Insider Threat Program.

b. Ensure CI insider threat education is within IA training policy and programs in coordination with ~~DCHC~~ *DIA*.

c. Participate in CI insider threat forums.

~~7~~*6*. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND AMERICAS' SECURITY AFFAIRS (ASD(HD&ASA)). The ASD(HD&ASA), under the authority, direction, and control of the Under Secretary of Defense for Policy, shall:

a. Develop AT policies to support the CI Insider Threat Program.

b. Participate in CI insider threat forums.

~~8~~*7*. HEADS OF THE DoD COMPONENTS. The Heads of the DoD Components shall:

a. Conduct authorized CI activities to detect, identify, assess, exploit, and deny FIE and the insider threat in accordance with this Instruction and DoD 5240.1-R (Reference (t)).

b. Share information provided by CI, security, IA, LE, and AT/FP working groups to effectively counter the CI insider threat.

c. Notify the appropriate MDCO or the Federal Bureau of Investigation (FBI) when there is a reasonable belief that a clandestine relationship exists or has existed between an FIE and an unidentified current or former DoD-affiliated individual in accordance with Enclosure 3, Reference (k), and DoDI 5240.04 (Reference (u)).

d. Incorporate CI insider threat information into CI, security, IA, LE, and AT/FP training in accordance with Reference (h) and DoDD 8570.01 (Reference (v)).

e. Establish and maintain the capability to support CI analysis of audit and monitoring data.

f. Consistent with authorized activities, implement CI insider threat initiatives to identify DoD-affiliated personnel suspected of or actually compromising DoD information on behalf of an FIE.

g. Report anomalies to the Director, ~~DCHC~~ *DIA*, in accordance with Enclosure 3 and Reference (n).

h. Ensure notification to DSS when cleared contractor locations or personnel are involved, and that notification is coordinated with the FBI or applicable MDCO.

~~9~~*8.* SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities of section ~~8~~ *7* of this enclosure, through their MDCO, shall:

a. Integrate and validate CI insider threat information requirements into other intelligence collection requirements

b. Provide supported organizations with CI insider threat briefings as part of the existing CI awareness program in accordance with Reference (h) and DoDI 5240.10 (Reference (w)).

c. Establish and implement CI initiatives to identify and counter espionage, international terrorism, and the CI insider threat.

d. Conduct information exchanges with Federal, State, local, tribal, and foreign agencies on CI insider threats in accordance with Reference (b).

e. Conduct anomaly-based detection activities in accordance with Reference (n).

f. Develop CI policy, programming, and resource requirements to implement a comprehensive insider threat program.

ENCLOSURE 3

PROCEDURES

1. UNKNOWN SUBJECT LEADS. Information based on a reasonable belief that a clandestine relationship exists or has existed between an FIE and an unidentified current or former DoD-affiliated individual shall be immediately reported and handled as follows:

a. DoD personnel shall immediately report such information to their organizational CI element, supporting MDCO, the FBI, or other appropriate authority in accordance with Reference (h).

b. Organizational CI elements that receive such information or develop the information during the course of a CI inquiry shall immediately notify ~~DCHC~~ *DIA* and the supporting MDCO or the FBI in accordance with Reference (k).

c. MDCOs shall report such information to ~~DCHC~~ *DIA*. This information supports the ~~DCHC~~ *DIA* requirement to serve as the focal point and central repository for unknown subject leads, reports, and information in accordance with Reference (u).

d. ~~DCHC~~ *DIA* personnel shall review and evaluate reports that indicate a CI insider threat from an unknown DoD-affiliated person. ~~DCHC~~ *DIA* personnel shall attempt to identify the unknown individual's organizational affiliation and refer developed information to the appropriate MDCO or the FBI in accordance with Reference (u).

2. ANOMALIES

a. The DoD Components report anomalies to ~~DCHC~~ *DIA* in accordance with Reference (n). This is done by memorandums within 5 working days, using the procedures established for CI inquiries and referrals in accordance with Reference (k).

b. ~~DCHC~~ *DIA* shall share CI insider threat trends within the CI enterprise.

c. If no FIE connection is found, threat information shall be forwarded to the applicable law enforcement organizations.

d. If ~~DCHC~~ *DIA* determines an anomaly warrants investigation, ~~DCHC~~ *DIA* shall refer the matter to the appropriate MDCO or the FBI in accordance with Reference (u).

3. CI INSIDER THREAT PROGRAM ELEMENTS. The CI Insider Threat Program shall include:

a. CI Analysis of Information Technology Auditing and Monitoring. Mitigation tools are a collection of IA tools or a single application that provides standard on-line behavioral monitoring of prohibited activities, anomalous behavior, and suspicious actions. These automated systems shall have a standard data sharing capability to ease interoperability within DoD and the IC. The tools shall be supported by technical and analytical resources.

b. CI Insider Threat Awareness and Training. Awareness and training shall consist of integrated CI, security, IA, and AT/FP education programs addressing threats to personnel within the DoD Component in accordance with Reference (h). Education programs shall be mandatory, interactive, and address current and real threats in the work and personal environment.

c. Foreign Travel and Contact Reporting and Analysis. A process for DoD personnel, including contractor support, to report foreign travel and foreign contacts. The process includes foreign national visits to DoD and contractor facilities. The process shall be in accordance with Reference (h) and DoDD 5230.20 (Reference (x)). The process shall be integrated into component travel systems, as appropriate, to ensure proper notifications and that pre- and post-travel briefings are conducted.

d. Polygraph and Credibility Assessment. Polygraph and approved credibility assessment tools shall be used in accordance with Reference (l) to identify and resolve CI insider threat issues.

(1) Favorable CI scope polygraph (CSP) and expanded-scope screening exams shall be entered into the Joint Personnel Adjudication System and Scattered Castle system, to allow information to be shared with components and the IC, unless inputting the data will compromise the status or affiliation of the concerned individual.

(2) DoD Polygraph Program personnel shall report the results of unfavorable CSP examinations to the responsible authority for determination of access suitability, CI analysis, and further investigation, as appropriate.

e. Personnel Security, Evaluation, Analysis, and Reporting. In accordance with DoD Manual 5200.01-V-3 (Reference (y)), both personnel security and CI professionals shall coordinate within their authorities when CI concerns are developed through the adjudicative process.

f. Security Incident Reporting and Evaluation. CI and security professionals shall coordinate to obtain records of security incidents, violations, suspicious incidents, and anomalies by DoD-affiliated persons in accordance with Reference (t).

g. Proactive CI Initiatives. The implementation of innovative activities to identify CI insider threats is a shared responsibility and mission for CI, security, IA, and AT/FP, while working in concert with the MDCOs and, as appropriate, the FBI, in accordance with existing policies and laws. Components shall coordinate innovative activities with their respective legal advisors before implementing.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(HD&ASA)	Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
AT/FP	antiterrorism and force protection
CI	counterintelligence
CSP	CI scope polygraph
~~DCHC~~	~~Defense Counterintelligence and Human Intelligence Center~~
DIA	Defense Intelligence Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DSS	Defense Security Service
DUSD(I&S)	Deputy Under Secretary of Defense for Intelligence and Security
FBI	Federal Bureau of Investigation
FIE	foreign intelligence entity
HUMINT	human intelligence
IA	information assurance
IC	Intelligence Community
ITCIG	Insider Threat Counterintelligence Group
LE	law enforcement
MDCO	Military Department CI Organization
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

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

anomaly-based detection. The process of comparing CI, security, IA, LE, and AT/FP behaviors and activities that are deemed normal against other observed events to identify significant deviations and or anomalous behavior.

anomaly. Defined in Reference (b).

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

DoD personnel. Active and reserve military personnel, as well as DoD civilian employees.

DoD-affiliated personnel. DoD active and reserve personnel, DoD civilian employees, retired military and DoD civilian employees, contractors and their employees, inactive reservists, National Guard members, family members of active duty and civilian personnel, persons residing on or having access to DoD facilities, persons under consideration for DoD employment, and former DoD employees and contractors.

FIE. Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, blocks or impairs U.S. intelligence collection, influences U.S. policy, or disrupts U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorists.

insider. Anyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

insider threat. A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.