Department of Defense

INSTRUCTION

NUMBER 5240.22
September 24, 2009
Incorporating Change 2, Effective April 3, 2019

USD(I)

SUBJECT: Counterintelligence Support to Force Protection

References: See Enclosure 1

1. PURPOSE. This Instruction implements policy, assigns responsibilities, and prescribes procedures in accordance with DoD Directive (DoDD) 5143.01 (Reference (a)) for conducting and managing counterintelligence (CI) support to force protection (FP), in accordance with DoDD O-5240.02 (Reference (b)); DoDD 2000.12 (Reference (c)); Memorandum of Understanding (MOU) (Reference (d)); DoD Instruction (DoDI) 2000.16 (Reference (e)); and DoD 5240 1-R (Reference (f)).

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 (CCMDs), 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 Department of Defense (hereafter referred to collectively as the "DoD Components").

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that there shall be comprehensive, aggressive, and integrated CI capabilities throughout the Department of Defense, using all CI functions and related activities to support the FP programs of the DoD Components and other supported elements within the Department of Defense, in accordance with References (b) and (f).

5. RESPONSIBILITIES. See Enclosure 2.

6. RELEASABILITY. **Cleared for public release.** This issuance is available on the DoD Issuances Website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 2. This issuance is updated to correct the office of primary responsibility and DoD Issuances Website address and remove expiration language in accordance with current Chief Management Officer of the Department of Defense direction.

8. EFFECTIVE DATE. This Instruction is effective September 24, 2009.

James R. Clapper, Jr.
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 Directive 2000.12, "DoD Antiterrorism (AT) Program," March 1, 2012
(d) Memorandum of Understanding (MOU) Between the Department of State, Bureau of Diplomatic Security and the DoD Counterintelligence Field Activity Regarding Force Protection Detachments, May 9, 2003[1]
(e) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006, as amended
(f) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 7, 1982, as amended
(g) DoD Instruction S-5240.15, "The Force Protection Response Group (FPRG) (U)," August 26, 2005[1]
(h) DoD Directive 5210.48, "Polygraph and Credibility Assessment Program," January 25, 2007, as amended
(i) Under Secretary of Defense for Intelligence Memorandum, "Operational Use of the Preliminary Credibility Assessment Screening System," October 29, 2007
(j) DoD Instruction 5240.6, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended
(k) DoD Instruction 5240.18, "Counterintelligence (CI) Analysis and Production," November 17, 2009, as amended
(l) DoD Instruction 3020.41, "Operational Contract Support (OCS)," December 20, 2011, as amended
(m) Title 22, United States Code
(n) DoD Directive 5105.75, "Department of Defense Operations at U.S. Embassies," December 21, 2007
(o) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," as amended
(p) DoD Instruction O-2000.22, "Designation and Physical Protection of DoD High Risk Personnel (HRP)," January 22, 2008, as amended
(r) DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended

[1] Contact USDI.Pubs@OSD.mil to obtain a copy.

ENCLOSURE 2

RESPONSIBILITIES

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

a. Monitor implementation of this Instruction and issue such additional direction and guidance as may be necessary in accordance with Reference (a).

b. Resolve any issue concerning CI support to FP that cannot be resolved by the DoD Components.

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

a. Advise the USD(I) and other OSD principal staff assistants on DoD CI support to FP policies and operational matters.

b. Provide policy oversight of DoD CI components to ensure compliance with DoD CI support to FP policy.

c. Represent the USD(I) at DoD and national-level forums concerning CI support to FP.

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. Oversee CI support to FP.

b. Manage CI support to FP implementation and resource planning, in accordance with References (b) and (c).

c. Support establishment of and oversee DoD Force Protection Detachment (FPDs).

d. Manage DoD participation in JTTFs.

e. Conduct program reviews of the DoD participation in the FPDs and JTTFs.

f. Manage the Force Protection Response Group (FPRG) in accordance with DoDI S-5240.15 (Reference (g)).

g. Determine common advanced training standards for CI support to FP skills and incorporate the standards into the training curriculum at the Joint Counterintelligence Training Academy.

4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff shall receive, validate, and prioritize requests for new FPD locations from the CCMDs (see Enclosure 3).

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

a. Integrate CI support into their respective Component FP programs.

b. Integrate CI support to FP when establishing priority intelligence requirements.

c. Integrate use of approved credibility assessment instruments, such as the polygraph and the PCASS, during contingency operations in accordance with DoDD 5210.48 and the USD(I) Memorandum (References (h) and (i)).

d. Implement the procedures in Enclosure 3.

6. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 5 of this enclosure, shall ensure their respective CI organizations:

a. Provide personnel to support FPDs and, when resources permit, JTTFs.

b. Consistent with Military Department policy, conduct liaison with Federal, State, and local agencies and foreign agencies for the collection and exchange of international terrorist threat information.

c. Collect, report, and disseminate time-sensitive terrorist threat information to supported commanders.

d. Provide supported commands with international terrorist threat analysis and production.

e. Provide tailored international terrorist briefings to supported commands as part of a CI awareness program in accordance with DoDI 5240.6 (Reference (j)).

f. Conduct the full range of CI activities as needed in support of Component force protection programs.

ENCLOSURE 3

PROCEDURES

1. GENERAL. DoD CI Components shall:

a. Notify the Director, DIA, of any significant terrorism-related information in accordance with References (b) and (j).

b. Ensure deploying CI personnel receive specialized training on CI support to FP.

c. Produce CI assessments in accordance with DoDI 5240.18 (Reference (k)) to meet combating terrorism and FP requirements of in-garrison and deployed forces.

2. JTTF

a. DoD CI personnel participating on JTTFs shall work in partnership with other JTTF members to detect and neutralize terrorists, terrorist-enabling individuals, and organizations threatening DoD interests.

b. DoD CI personnel assigned to a JTTF shall ensure timely and appropriate dissemination to the Department of Defense of developing threat information affecting DoD equities through the most effective means possible.

3. FPRG

a. DoD Component CI organizations, CCMDs, and Defense Agencies shall use FPRG capabilities whenever appropriate in their CI support to FP missions in accordance with References (f) and (g).

b. DoD Components shall submit requests for FPRG operational support in accordance with Reference (g).

4. CONTINGENCY CONTRACTING

a. The Military Department CI organizations shall provide foreign intelligence and international terrorist threat awareness information to component security organizations that screen employees of contractors supporting military or contingency operations described in DoDI 3020.41 (Reference (l)). When information of potential CI interest is uncovered during the screening process, the CI Component shall assist the security organization to resolve the matter.

b. The Military Department CI organization shall conduct CI awareness reporting briefings for employees of contractors supporting military or contingency operation per Reference (j).

5. FPD

a. The Military Departments shall assign CI personnel to FPDs pursuant to Reference (d).

b. The Military Department CI organization is responsible for administrative control of their assigned FPDs.

c. The FPD primary mission is to detect and warn of threats to DoD personnel and resources in-transit at overseas locations without a permanent DoD CI presence. The mission further includes serving as a force multiplier for the American Embassy Country Team in support of the DoD presence and mission, which include, but are not limited to:

(1) Liaison.

(2) Defense threat assessments.

(3) Route and/or travel threat assessments.

(4) Foreign intelligence and international terrorist threat briefings.

(5) DoD investigative lead reporting.

(6) Intelligence report production.

(7) Conducting or assisting in vulnerability assessments of ports, airfields, and routes used by in-transit forces.

d. CCMDs shall prioritize requests for new FPD locations within their area of responsibility and submit the requests to the Joint Staff. The Joint Staff shall consolidate the requests and establish a single priority list. The Joint Staff/J-34, in conjunction with the Joint Staff/J-2, shall coordinate with DIA and the Military Department CI organizations to fulfill the prioritized list based upon available resources.

e. The Joint Staff shall evaluate, on a case-by-case basis, CCMD requests to establish an FPD not included in the priority list. The evaluation determines validity for the requirement over those submitted on the priority list. If found valid and based upon available resources, the Joint Staff/J-34 shall coordinate with DIA and the Military Department CI organizations to fulfill the request.

f. Under section 3927 of title 22, United States Code (Reference (m)), FPD members fall under the direction, coordination, and supervision of the Chiefs of Mission (COM) except when they are under the command of a Combatant Commander. FPDs shall maintain close operational

synchronization with the Regional Security Officer (RSO), the Defense Attaché, and other country team members as appropriate.

g. The CCMDs shall work through the senior defense official for tasking the FPD pursuant to DoDD 5105.75 (Reference (n)).

h. FPDs shall maintain liaison contact with host nation officials to assess an operational picture of the local intelligence, terrorist, and criminal threat.

i. FPDs shall expeditiously communicate threat information directly to transiting units via established communication channels. FPDs shall provide assessment findings and reports, threat information, vulnerability assessment data, and related FP information to the CCMD.

j. The RSO has primacy for addressing all security issues affecting DoD personnel who are operating in-country under COM authority. The RSO is responsible for oversight, i.e., ensuring the FPD operates within the security guidelines and procedures established by the Department of State as outlined by the COM and in Reference (d).

6. CI ANALYTICAL SUPPORT. Military Department CI organizations shall conduct assessments and publish appropriate CI analytical products in accordance with Reference (k) to meet the FP requirements of in-garrison and deployed forces required by Reference (c).

7. POLYGRAPH AND PRELIMINARY CREDIBILITY ASSESSMENT SCREENING SYSTEM (PCASS) EXAMINATIONS. Military Department CI organizations authorized to use polygraph and/or PCASS may use the credibility assessment technologies as a tool to enhance CI support to FP in accordance with Reference (h). Only certified operators shall employ PCASS. Certified operators may use PCASS as a field expedient credibility assessment tool during the initial screening of non-U.S. persons of interest for intelligence and security purposes in accordance with Reference (i).

8. BIOMETRICS. Wherever possible, CI organizations within the DoD Components should incorporate the latest advances in biometrics capabilities into their operational planning. Biometrics technology should be brought to bear in source validation and assessment, as well as in identifying personnel who may pose a threat to DoD forces.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CI	counterintelligence
COM	Chief of Mission
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DUSD(I&S)	Deputy Under Secretary of Defense (Intelligence and Security)
FP	force protection
FPD	Force Protection Detachment
FPRG	Force Protection Response Group
JTTF	joint terrorism task force
MOU	memorandum of understanding
PSD	protective security detail
PCASS	Preliminary Credibility Assessment Screening System
RSO	Regional Security Officer
USD(I)	Under Secretary of Defense for Intelligence

PART II. DEFINITIONS

ADCON. Defined in Joint Publication 1-02 (Reference (o)).

FP. Defined in Reference (o).

PSD. Defined in DoDI O-2000.22 (Reference (p)).