



Department of Defense INSTRUCTION

NUMBER 2000.12

March 1, 2012

Incorporating Change 2, Effective November 15, 2016

USD(P)

SUBJECT: DoD Antiterrorism (AT) Program

References: See Enclosure 1

1. PURPOSE. This Instruction:

a. Reissues DoD Directive (DoDD) 2000.12 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the authority in DoDD 5111.1 (Reference (b)) and Secretary and Deputy Secretary of Defense Memorandums (References (c) and (d)), to establish policy, assign responsibilities, and prescribe procedures for the DoD AT Program.

b. Implements in part section 134 of title 10, United States Code (U.S.C.) (Reference (e)), which provides that the Under Secretary of Defense for Policy (USD(P)) shall have overall direction and supervision for policy, program planning and execution, and allocation and use of resources for DoD combating terrorism (CbT) activities.

c. Incorporates the following actions from Acting Principal Deputy Under Secretary of Defense for Policy Memorandum (Reference (f)):

(1) Transfer of the DoD AT Program to the Assistant Secretary of Defense for Homeland Defense and ~~Americas' Security Affairs-Global Security~~ (ASD(HD&~~ASAGS~~)).

(2) Designation of ASD(HD&~~ASAGS~~) as the lead OSD official for implementation of the 1997 Memorandum of Understanding Between DoD and Department of State for Security of DoD Elements and Personnel in Foreign Areas (Reference (g)).

d. Replaces the Antiterrorism Coordinating Committee Senior Steering Group with the Mission Assurance Senior Steering Group (SSG). The Mission Assurance Coordination Board Terms of Reference (Reference (h)) describes the composition, roles, responsibilities, working groups, and procedures of the SSG.

e. Incorporates elements of and cancels DoD O-2000.12-H (Reference (~~ei~~)). Reference (~~ei~~) is replaced by the DoD Antiterrorism Officer Guide (Reference (~~bkbm~~)).

f. Incorporates and cancels the August 2010 Secretary of Defense Memorandum on DoD force protection (FP) responsibilities (Reference (~~sj~~)) by reinforcing the requirement for DoD Components to comply with geographic Combatant Commanders' authority to set FP conditions in their areas of responsibility (AOR), and requiring the geographic Combatant Commanders to share threat assessment requirements with DoD Components in their AORs, other geographic Combatant Commands, and the Defense Combating Terrorism Center (DCTC).

2. APPLICABILITY. This Instruction:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

(2) DoD military and civilian personnel, dependents of DoD military personnel (as defined in section 1072 of Reference (e)), family members of DoD civilian employees (as defined in section 040 of Department of State Standardized Regulations (Reference (~~ik~~))) outside the United States, DoD contractors (in accordance with the terms of applicable contracts, in accordance with DoDI 1100.22 (Reference (~~jl~~))), and when on DoD installations and facilities or when accompanying DoD forces outside the United States in areas designated for hostile fire pay or imminent danger pay in accordance with DoDI 1340.09 (Reference (~~km~~))), ~~and DoD installations and facilities (hereinafter referred to collectively as "DoD elements and personnel") worldwide, with the exception of DoD elements and personnel identified in paragraph 2.b. DoD military and civilian personnel listed on Annex B of a Memorandum of Agreement developed pursuant to Reference (g), and DoD installations and facilities (referred to collectively in this instruction as "DoD elements and personnel") worldwide, with the exception of DoD elements and personnel identified in paragraph 2.b.~~

b. Does NOT apply to DoD elements and personnel under the security responsibility of the Department of State (DOS) pursuant to Reference (g); sections 4801, 4802, and 4805 of title 22, U.S.C. (Reference (~~ln~~)); and DoDI 5210.84 (Reference (~~mo~~)), including those assigned to international organizations (except those assigned to United Nations or other multinational peace operations). The DoD elements and personnel under the security responsibility of DOS shall comply with Overseas Security Policy Board (OSPB) and DOS security standards instead of the DoD standards prescribed by this Instruction and DoDI 2000.16 (Reference (~~np~~)).

c. Does not subsume or replace the functions, responsibilities, or authorities of the OSD principal staff assistants or those of the Heads of the DoD Components prescribed by law or other DoD guidance.

d. Addresses only the AT element of DoD CbT activities, as defined in the Glossary.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy that:

a. DoD Components and DoD elements and personnel shall be protected from terrorist acts through a high-priority, comprehensive AT program using an integrated systems approach.

b. AT is one of many independent, yet mutually supporting enablers of the broader FP effort. Other enablers include programs such as physical security; emergency management; law enforcement; information security; operations security; ~~the Defense~~ Critical Infrastructure ~~Program Protection (DCIP)~~; continuity of operations (COOP); and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE). AT and FP are not synonymous.

(1) The DoD AT Program is an element of CbT and focuses on defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.

(2) The minimum elements of an AT program shall be AT risk management, planning, training and exercises, resource application, and comprehensive program review, as defined in the Glossary.

(3) All response planning undertaken pursuant to this Instruction will be consistent to the maximum extent possible with Secretary of Homeland Security Publications (References ~~(pq)~~ and ~~(qr)~~). As such, plans for response to a terrorist incident must be incorporated into and synchronized with incident response plans prepared in accordance with DoDI 6055.17 (Reference ~~(rs)~~) to ensure continued application of AT measures throughout the incident.

c. Commanders and DoD civilian managers and directors have the authority to enforce appropriate *FP* measures to ensure the protection of DoD elements and personnel subject to their control while pursuing mission accomplishment, and shall ensure the AT awareness and readiness of all DoD elements and personnel assigned or attached. *Commanders and DoD civilian managers and directors will not apply restrictions on non-official (personal) travel to DoD civilian employees, contractors, and dependents unless those restrictions are directly related to:*

(1) A commander's control over military installations (including access to those installations).

(2) Providing certain benefits to dependents (e.g., benefits related to command sponsorship).

(3) Conducting combat operations, advanced force operations, or similar DoD missions.

d. In addition to the potential restrictions described in paragraph 4.c., in appropriate situations, non-official travel restrictions may also be imposed by proper authority on the following personnel:

(1) Individuals briefed and indoctrinated for Sensitive Compartmented Information, pursuant to Intelligence Community Directive 703 (Reference (t)).

(2) Defense contractor personnel, if they are required by the terms of their contracts to comply with GCC FP policies.

(3) DoD civilian employees who are designated as emergency essential employees consistent with section 1580 of Reference (e), when necessary to meet expeditionary requirements pursuant to DoD Directive 1404.10 (Reference (u)).

e. The travel restrictions listed in paragraphs 4.c. and 4.d. may be included in the requirements for leave travel in the DoD Foreign Clearance Guide (Reference (v)).

~~df. Geographic Combatant Commanders have tactical control (TACON) for FP, as defined in the Glossary, over all DoD personnel within their geographic areas of responsibility (AORs), with the exception of DoD personnel for whom the chiefs of U.S. diplomatic missions (COMs) have security responsibility as described in References (g) and (m). Geographic Combatant Commanders have the authority to enforce appropriate FP measures to ensure the protection of all DoD elements and personnel subject to their control within their geographic areas of responsibility (AORs). This includes personnel on temporary duty, with the exception of DoD personnel for whom the chiefs of U.S. diplomatic missions (COMs) have security responsibility, as described in References (g) and (o). This authority includes tactical control (TACON) for FP, as defined in the Glossary, over military personnel within a geographic Combatant Commander's AOR.~~

eg. The Combatant Commander Initiative Fund (CCIF) or the Combating Terrorism Readiness Initiative Fund (CbT-RIF), if funded, will be maintained as a flexible means to respond to emergent and emergency AT requirements (as described in Chairman of the Joint Chiefs of Staff Instructions 7401.01E (Reference (tw)) and 5261.01F (Reference (ux))).

fh. The definitions provided in Reference (np) shall be used to guide the determination of the terrorist threat to DoD personnel, facilities, and interests and to establish terrorism threat levels (TTLs).

gi. DoD Components shall implement Force Protection Condition (FPCON) measures as outlined in Reference (np) in anticipation of or in response to a terrorist threat or attack. Commanders and civilian managers and directors at all levels must continually update risk assessments to ensure all appropriate measures are applied for the mitigation of terrorist threats.

hj. DoD elements and personnel shall comply with the theater, country, and special area clearance requirements in DoDD 4500.54E (Reference (vy)) and ~~the DoD Foreign Clearance Guide~~ (References (v) ~~and (w)~~) before traveling outside the United States on official travel.

ik. DoD shall assist DOS, when feasible and normally on a reimbursable basis, in supporting efforts to protect U.S. citizens abroad in accordance with section 4805 of Reference (~~ln~~) or other applicable provisions of law. DoD contract provisions shall be developed in accordance with Reference (~~ik~~) and shall require that contract firms, companies, and entities obtain AOR-specific AT guidance issued by the applicable geographic Combatant Commander, and require compliance by personnel performing DoD contracts outside the United States, consistent with the terms of the contract.

jl. DoD will comply with the No-Double-Standard Policy (as described in the Glossary) on the dissemination of terrorist threat information.

km. Installation commanders will ensure non-DoD tenants comply with all aspects of the DoD AT program. Non-DoD tenant facilities on DoD property must comply with all applicable Unified Facilities Criteria (UFC) standards to ensure personnel in these facilities have the same level of protection as received by DoD members in other facilities on the installation.

ln. Non-DoD tenants on a DoD installation, facility, or other DoD-owned or -leased property shall be incorporated into the local AT plan using a memorandum of understanding (MOU) or memorandum of agreement (MOA) or similar support agreement. If not specified, non-DoD tenants shall be required to participate in the local DoD AT plans.

mo. Unit commanders or civilian managers and directors responsible for DoD elements occupying leased facility space, or space in buildings owned or operated by the U.S. General Services Administration (GSA) not located on DoD property, will comply with the applicable Federal Interagency Security Committee standards incorporated into the Unified Facilities Criteria pursuant to Deputy Secretary of Defense Memorandum (Reference (~~xz~~)), the Unified Facilities Criteria 4-010-01 (Reference (~~yaa~~)), and the Physical Security Criteria for Federal Buildings (Reference (~~zab~~)).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES

a. All DoD personnel traveling into a geographic Combatant Command AOR shall familiarize themselves and comply with all geographic Combatant Command-specific AT policies and requirements.

b. Enclosure 3 specifies the roles and requirements of the Defense Intelligence Agency (DIA), DCTC.

7. INFORMATION COLLECTION REQUIREMENTS. The DoD intelligence, counterintelligence, security, and information operations support activities described in this

Instruction ~~are exempt from licensing in accordance with paragraphs C4.4.1., C4.4.2., and C4.4.8. of DoD 8910.1-M does not require licensing with a report control symbol in accordance with paragraphs 1.b(3) and 1.b(4) of Enclosure 3 of Volume 1 of DoD Manual 8910.01 (Reference (aac)).~~

8. RELEASABILITY. ~~UNLIMITED~~ *Cleared for public release.* 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>.

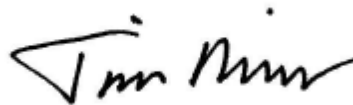
9. EFFECTIVE DATE. *This instruction is effective March 1, 2012.*

~~— a. This instruction is effective March 1, 2012.~~

~~— b. Change 1 is effective September 9, 2013. DoD Components have 180 days from this effective date to implement the programs described in this instruction.~~

~~— c. This instruction must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with in accordance with DoDI 5025.01 (Reference (bl)).~~

~~— d. This instruction will expire effective March 1, 2022 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (bl).~~



James N. Miller
Acting Under Secretary of Defense for Policy

Enclosures

1. References
2. Responsibilities
3. DCTC

Glossary

TABLE OF CONTENTS

| | |
|---|------|
| ENCLOSURE 1: REFERENCES..... | 78 |
| ENCLOSURE 2: RESPONSIBILITIES..... | 1011 |
| ASD(HD& ASAGS)..... | 1011 |
| ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT (ASD(SO/LIC))..... | 1011 |
| ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS (ASD(GSA))..... | 1011 |
| USD(AT&L)..... | 1112 |
| DEPUTY UNDERASSISTANT SECRETARY OF DEFENSE FOR <i>ENERGY</i> , INSTALLATIONS, AND ENVIRONMENT (DU ASD(<i>EI&E</i>))..... | 1112 |
| ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR, CHEMICAL, AND BIOLOGICAL DEFENSE PROGRAMS (ASD(NCB))..... | 1213 |
| DIRECTOR, DTRA..... | 1213 |
| USD(C)/CFO..... | 1213 |
| USD(I)..... | 1314 |
| DIRECTOR, DIA..... | 1314 |
| DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS)..... | 1415 |
| USD(P&R)..... | 1516 |
| ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA))..... | 1516 |
| ASSISTANT SECRETARY OF DEFENSE FOR <i>MANPOWER AND</i> RESERVE AFFAIRS (ASD(<i>M&RA</i>))..... | 1617 |
| ASSISTANT TO THE SECRETARY OF DEFENSE FOR INTELLIGENCE OVERSIGHT (ATSD(IO))..... | 1617 |
| DIRECTOR, PENTAGON FORCE PROTECTION AGENCY (PFPA)..... | 1617 |
| HEADS OF THE DoD COMPONENTS..... | 1617 |
| SECRETARIES OF THE MILITARY DEPARTMENTS..... | 1718 |
| CJCS..... | 1920 |
| COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS..... | 2122 |
| COMMANDERS OF THE FUNCTIONAL COMBATANT COMMANDS..... | 2425 |
| ENCLOSURE 3: DCTC..... | 2527 |
| GLOSSARY..... | 2729 |
| PART I. ABBREVIATIONS AND ACRONYMS..... | 2729 |
| PART II. DEFINITIONS..... | 2830 |

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003 (hereby cancelled)
- (b) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P)),", December 8, 1999
- (c) Secretary of Defense Memorandum, "Civilian Oversight of DoD Combating Terrorism and Consequence Management Activities," May 9, 2001¹
- (d) Deputy Secretary of Defense Memorandum, "Delegations of Authority," November 30, 2006
- (e) ~~Sections 134, 1072, 2801, 2859, and 2687 of title 10, United States Code~~
- (f) Acting Principal Deputy Under Secretary of Defense for Policy Approval, "Transfer of Antiterrorism (AT) Portfolio," March 23, 2009
- (g) Memorandum of Understanding between the Department of State and the Department of Defense, "Security of DoD Elements and Personnel in Foreign Areas," December 16, 1997²
- (h) DoD Mission Assurance Coordination Board Terms of Reference, current edition³
- (~~ei~~) DoD O-2000.12-H, "DoD Antiterrorism Handbook," February 1, 2004 (hereby cancelled)
- (~~sj~~) Secretary of Defense Memorandum, "DoD Force Protection Responsibilities – CORRECTED COPY," August 18, 2010 (hereby cancelled)
- (~~ik~~) Department of State Standardized Regulations, Section 040,⁴ current edition
- (~~jl~~) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
- (~~km~~) DoD Instruction 1340.09, "Hostile Fire Pay and Imminent Danger Pay," April 20, 2010
- (~~ln~~) Sections 4801, 4802, and 4805 of title 22, United States Code
- (~~mo~~) DoD Instruction 5210.84, "Security of DoD Personnel at U.S. Missions Abroad," January 22, 1992, *as amended*
- (~~np~~) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," October 2, 2006, *as amended*
- (~~pq~~) Secretary of Homeland Security Publication, "National Response Framework," January 2008
- (~~qr~~) Secretary of Homeland Security Publication, "National Incident Management System," December 2008
- (~~rs~~) DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," January 13, 2009, *as amended*
- (~~t~~) *Intelligence Community Directive 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information," June 21, 2013*
- (~~u~~) *DoD Directive 1404.10, "DoD Civilian Expeditionary Workforce," January 23, 2009*
- (~~wv~~) DoD Foreign Clearance Guide⁵

¹ Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

² Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

³ Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

⁴ Available on the Internet at http://aoprals.state.gov/content.asp?content_id=146&menu_id=81

⁵ Available at <https://www.fcg.pentagon.mil> and <https://www.fcg.pentagon.smil.mil>.

- (~~tw~~) Chairman of the Joint Chiefs of Staff Instruction 7401.01~~EG~~, “Combatant Commander Initiative Fund (CCIF),” ~~July 1, 2009~~ *September 21, 2015*
- (~~tx~~) Chairman of the Joint Chiefs of Staff Instruction 5261.01~~FG~~, “Combating Terrorism Readiness Initiatives Fund,” ~~October 21, 2008~~ *December 2, 2013*
- (~~vy~~) DoD Directive 4500.54E, “DoD Foreign Clearance Program (FCP),” December 28, 2009
- (~~xz~~) Deputy Secretary of Defense Memorandum, “Antiterrorism Building Standards for Leased Space,” December 7, 2012⁶
- (~~yaa~~) Unified Facilities Criteria 4-010-01, “DoD Minimum Antiterrorism Standards for Buildings,” ~~February 9, 2012~~ *as amended*
- (~~zab~~) Interagency Security Committee, “Physical Security Criteria for Federal Buildings: An Interagency Security Committee Standard,” April 12, 2010⁷
- (~~aac~~) ~~DoD 8910.1-M, “Department of Defense Procedures for Management of Information Requirements,” June 30, 1998-DoD Manual 8910.01, “DoD Information Collections: Procedures for DoD Internal Information Collections,” June 30, 2014, as amended~~
- (~~abd~~) DoD Directive 5111.13, “Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs (ASD(HD&ASA)),” January 16, 2009
- (~~ae~~) DoD Instruction 5200.08, “Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB),” December 10, 2005, *as amended*
- (~~af~~) DoD 5200.08-R, “Physical Security Program,” April 9, 2007, *as amended*
- (~~ag~~) DoD Instruction 3224.03, “Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E),” October 1, 2007
- (~~afh~~) Defense Federal Acquisition Regulation Supplement, current edition
- (~~agi~~) DoD Instruction C-4500.51, “DoD Commercially Procured and Leased Armored Vehicle Policy (U),” July 25, 2007
- (~~ahj~~) DoD Directive 5105.62, “Defense Threat Reduction Agency (DTRA),” April 24, 2013, *as amended*
- (~~aik~~) Memorandum of Agreement Between the Defense Threat Reduction Agency and the Joint Staff, “Higher Headquarters Antiterrorism Program Reviews and Joint Staff Integrated Vulnerability Assessment Support,” July 25, 2005⁸
- (~~ajl~~) Department of Defense Vulnerability Assessment Benchmarks, January 1, 2013⁹
- (~~akm~~) DoD Directive 7045.14, “The Planning, Programming, Budgeting, and Execution (PBBE) Process,” January 25, 2013
- (~~aln~~) DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” ~~November 23, 2005~~ *October 10, 2014, as amended*
- (~~amo~~) DoD Directive 5105.21, “Defense Intelligence Agency (DIA),” March 18, 2008
- (~~anp~~) DoD Directive 3025.18, “Defense Support of Civil Authorities (DSCA),” December 29, 2010, *as amended*
- (~~aeq~~) DoD Directive ~~5105.75~~ *5205.75*, “~~Department of Defense DoD~~ Operations at U.S. Embassies,” ~~December 21, 2007~~ *December 4, 2013*
- (~~apr~~) Title 36, Code of Federal Regulations
- (~~aqs~~) DoD 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons,” December ~~17~~, 1982, *as amended*

⁶ Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

⁷ Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

⁸ Available from the Defense Threat Reduction Agency, 8725 John J. Kingman Road, MSC 6201, Fort Belvoir, VA 22080-6201

⁹ Available from J3 DDAT/HD (J34) ATRP, 3000 The Pentagon (MB917), Washington, DC 20318

- (~~arf~~) DoD Directive 6200.04, “Force Health Protection (FHP),” October 9, 2004
- (~~asu~~) DoD Directive 5148.11, “Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)),” April 24, 2013
- (~~atv~~) DoD Directive 5240.01, “DoD Intelligence Activities,” August 27, 2007, *as amended*
- (~~atw~~) DoD Instruction O-2000.22, “Designation and Physical Protection of DoD High-Risk Personnel (HRP),” ~~January 22, 2008~~ *June 19, 2014*
- (~~avx~~) Unified Facilities Criteria 4-020-01, “DoD Security Engineering Facilities Planning Manual,” September 11, 2008
- (~~awy~~) DoD Directive 5100.01, “Functions of the Department of Defense and its Major Components,” December 21, 2010
- (~~axz~~) DoD Directive 5100.03, “Support of the Headquarters of Combatant and Subordinate Unified Commands,” February 9, 2011
- (~~ayba~~) ~~DoD Directive 8500.01E, “Information Assurance (IA),” October 24, 2002~~ *DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014*
- (~~azbb~~) DoD Directive 3020.40, “DoD Policy and Responsibilities for Critical Infrastructure,” January 14, 2010, *as amended*
- (~~bac~~) DoD Directive ~~5240.02~~, “Counterintelligence (CI),” ~~December 20, 2007~~ *March 17, 2015*
- (~~bjd~~) DoD Directive 1400.31, “DoD Civilian Work Force Contingency and Emergency Planning and Execution,” April 28, 1995
- (~~bbe~~) DoD Instruction 2000.26, “Suspicious Activity Reporting (SAR),” ~~November 1, 2011~~ *September 23, 2014*
- (~~bef~~) Under Secretary of Defense for Intelligence Memorandum, “Designation of a Single Point of Contact for Defense Intelligence,” October 16, 2007¹⁰
- (~~bdg~~) Interagency Intelligence Committee on Terrorism, “Guidelines for Intelligence Community Terrorist Threat Warning System,” June 26, 2007¹¹
- (~~beh~~) Office of the Director of National Intelligence Memorandum E/S 00584, “Analytic Framework for Counterterrorism,” July 11, 2006¹²
- (~~bfi~~) Homeland Security Presidential Directive 6, “The Integration and Use of Screening Information to Protect Against Terrorism,” September 16, 2003¹³
- (~~bgj~~) National Security Presidential Directive–59/Homeland Security Presidential Directive–24, “Biometrics for Identification and Screening to Enhance National Security,” June 5, 2008¹⁴
- (~~bhk~~) Under Secretary of Defense for Intelligence Memorandum, “Designation of Joint Intelligence Task Force for Combating Terrorism (JITF-CT) as DoD Lead for Access to International Terrorism-related Information,” January 28, 2011¹⁵
- (~~bil~~) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” current edition
- (~~bkm~~) Office of the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs, “DoD Antiterrorism Officer Guide,” December 2012¹⁶
- (~~bl~~) ~~DoD Instruction 5025.01, “DoD Directives Program,” September 26, 2012, as amended~~

¹⁰ Available from usdi.pubs@osd.mil

¹¹ Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

¹² Available from OASD(HD&GS)/Room 3D247, 2600 Defense Pentagon, Washington, D.C. 20301

¹³ Available at <http://www.gpo.gov/fdsys/pkg/WCPD-2003-09-22/pdf/WCPD-2003-09-22-Pg1234-2.pdf>

¹⁴ Available at <http://www.gpo.gov/fdsys/pkg/WCPD-2008-06-09/pdf/WCPD-2008-06-09-Pg788-2.pdf>

¹⁵ Available from OUSD(I)/Room 3C1088, 2600 Defense Pentagon, Washington, D.C. 30301

¹⁶ Available from the Joint Staff, J-34 and the Office of the Assistant Secretary of Defense for Homeland Defense and Global Security

ENCLOSURE 2

RESPONSIBILITIES

1. ASD(HD&ASAGS). The ASD(HD&ASAGS), under the authority, direction, and control of the USD(P), shall:

a. Serve as the principal civilian advisor to the Secretary of Defense and the USD(P) to provide overall direction and supervision for policy development, program planning and execution, and allocation of resources for DoD AT activities (as described in References (c), (d), (f), and DoDD 5111.13 (Reference (abd))).

b. Coordinate with the Chair of the Under Secretary of Defense for Intelligence (USD(I)) Physical Security Review Board on physical security matters that affect DoD AT planning conducted in accordance with DoDI 5200.08 and DoD 5200.08-R (References (aee) and (adf)).

c. Coordinate with the Chair of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) Physical Security Equipment Action Group on physical security technology development and the application of new technologies to meet AT needs in accordance with DoDI 3224.03 (Reference (aeg)).

d. Coordinate with the CJCS to validate submissions for CCIF requests.

e. Monitor resource requirements resulting from ~~Joint Staff Integrated Vulnerability Assessment~~ *Joint Mission Assurance Assessment* trends in coordination with the CJCS; the USD(AT&L); the Under Secretary of Defense (Comptroller) (USD(C))/Chief Financial Officer (CFO), Department of Defense; and the Director of the Defense Threat Reduction Agency (DTRA).

2. ASSISTANT SECRETARY OF DEFENSE FOR SPECIAL OPERATIONS AND LOW-INTENSITY CONFLICT (ASD(SO/LIC)). The ASD(SO/LIC), under the authority, direction, and control of the USD(P), shall:

a. Coordinate with the ASD(HD&ASAGS) regarding policy and oversight of the DoD AT Program.

b. Provide an OSD representative to the Interagency Deputies Committee and the Counterterrorism Security Group (CSG).

3. ASSISTANT SECRETARY OF DEFENSE FOR GLOBAL STRATEGIC AFFAIRS (ASD(GSA)). The ASD(GSA), under the authority, direction, and control of the USD(P), shall:

a. Serve as the principal civilian advisor to the Secretary of Defense and the USD(P) on issues related to the proliferation of military and dual-use technology by terrorists, terrorist organizations or networks, and state sponsors of terrorism.

b. Provide a representative to the Interagency Intelligence Committee on Terrorism, as required.

4. USD(AT&L). The USD(AT&L) shall:

a. In coordination with the ASD(HD&~~ASAGS~~) and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), ensure that the Defense Federal Acquisition Regulation Supplement (Reference (~~a~~*fh*)) reflects current DoD AT requirements for defense contractors. Specifically, pursuant to Reference (e), establish requirements in Reference (~~a~~*fh*) for defense contractors performing DoD contracts outside the United States to:

(1) Ensure they subscribe to and monitor Overseas Security Advisory Council information and updates, and provide such information to employees overseas.

(2) Ensure their personnel who are U.S. citizens register with the relevant U.S. Embassy, and advise their personnel who are third-country nationals to contact the appropriate embassy for guidance on applicable requirements.

(3) Ensure that procedures are established requiring that DoD contractor personnel be provided AT awareness information before travelling outside of the United States that is commensurate with the information that DoD, including the geographic Combatant Commanders, provides to military and civilian personnel, to the extent such information may be made available.

(4) Comply with Reference (~~a~~*eg*) and DoDI C-4500.51 (Reference (~~a~~*gi*)) as appropriate.

b. Establish policy that encourages DoD Components to:

(1) Develop AT technology, and expeditiously apply new technology to meet AT needs.

(2) Evaluate and test commercial-off-the-shelf products to support the rapid acquisition and quick field integration of state-of-the-art AT technology.

5. ~~DEPUTY UNDER ASSISTANT~~ SECRETARY OF DEFENSE FOR ~~ENERGY,~~ INSTALLATIONS, AND ENVIRONMENT (~~DUASD~~(*EI&E*)). The ~~DUASD~~(*EI&E*), under the authority, direction, and control of the USD(AT&L), shall advise and provide recommendations to the Secretary of Defense, the USD(AT&L), and the CJCS on appropriate installation emergency management efforts in support of the DoD AT Program.

6. ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR, CHEMICAL, AND BIOLOGICAL DEFENSE PROGRAMS (ASD(NCB)). The ASD(NCB), under the authority, direction, and control of the USD(AT&L), ~~shall~~:

a. Serves as the principal advisor to the Secretary of Defense and the USD(AT&L) for all matters concerning the formulation of policy and plans for nuclear weapons safety and security, *safety and security of chemical and biological agents*, and chemical and biological defense programs, including chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) protection programs, in support of the DoD AT Program.

b. Coordinates all other matters, including those related to chemical and biological security measures *and the safety and security of chemical and biological agents*, with the USD(I).

7. DIRECTOR, DTRA. Pursuant to DoDD 5105.62 (Reference (~~ahj~~)) and the MOA between DTRA and the Joint Staff (Reference (~~ai~~k)), the Director, DTRA, under the authority, direction, and control of the USD(AT&L), through the ASD(NCB), and in addition to the responsibilities in section 17 of this enclosure, shall:

a. As the technical and field agent for the CJCS, conduct vulnerability assessments of DoD elements and personnel worldwide in accordance with this Instruction and Reference (~~ap~~) and the DoD ~~Antiterrorism Vulnerability Mission Assurance~~ Assessment Benchmarks (Reference (~~aj~~l)). Support assessments of Combatant Command and Military Department headquarters AT programs, CJCS exercises, air and sea ports of embarkation and debarkation, and in-transit forces.

b. Maintain the capability to provide follow-up assistance to assessed organizations; assist in training vulnerability assessment teams for the Combatant Commands, Military Departments, and DoD agencies; conduct specialized CJCS-directed assessments; and provide other specialized assistance as appropriate.

c. Analyze information collected during assessments and coordinate with the ASD(HD&~~AS~~AGS) to provide recommendations regarding AT, and with the USD(I) regarding physical security, program procedures, best practices, lessons learned, and improvements to the assessment process.

8. USD(C)/CFO. The USD(C)/CFO shall:

a. Provide information and guidance to the DoD Components on displaying AT resources within the planning, programming, budgeting, and execution (PPBE) process (formerly referred to as the Planning, Programming, and Budgeting System) and budget submissions in accordance with DoDD 7045.14 (Reference (~~ak~~m)).

b. Provide reports on AT funds as requested by the Secretary of Defense and the CJCS.

9. USD(I). The USD(I), in accordance with DoD Directive 5143.1 (Reference (~~an~~)), shall:

a. Provide policy, guidance, and oversight for intelligence, counterintelligence, personnel security, physical security, information security, operations security, and chemical and biological security to assist the ASD(HD&~~ASAGS~~) on matters pertaining to the AT program.

b. Review the DoD intelligence and counterintelligence security policies and programs that affect or support the DoD AT program.

c. Monitor National Security Agency and DIA execution of AT responsibilities.

d. Annually, as part of the PPBE process and in coordination with the CJCS, review the adequacy of intelligence, counterintelligence, physical security, and other security resources to determine whether they adequately support AT program objectives. Assist and support the CJCS in advising the Secretary of Defense of any changes needed to meet AT requirements.

e. Monitor DIA activities as the DoD Lead Component for diplomatic security matters in accordance with References (g) and (~~mo~~) and DoDD 5105.21 (Reference (~~amo~~)).

f. Provide the senior DoD voting member to the OSPB.

10. DIRECTOR, DIA. The Director, DIA, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 17 of this enclosure, shall:

a. Operate the DCTC as the lead DoD organization for:

(1) Managing the collection, exploitation, analysis, fusion, coordination, and dissemination of all-source intelligence in support of DoD CbT operations, planning, and policy including DoD AT requirements.

(2) Representing DoD in discussions about and coordination of AT and CbT issues in the Intelligence Community.

b. Ensure the DCTC complies with the requirements of Enclosure 3.

c. Function as the DoD Lead Component for diplomatic security matters pursuant to Reference (~~ln~~). Establish, manage, and operate a DoD diplomatic security element that shall:

(1) Ensure compliance by DoD elements and personnel under the security responsibility of a COM with OSPB and DOS security standards at missions outside the United States.

(2) Ensure deficiencies in the diplomatic security support received from the COMs are addressed and DoD equities protected.

(3) Ensure DoD representation at the OSPB and other committees, subcommittees, and working groups, as appropriate, pursuant to this Instruction and References (g), (~~km~~), and (~~np~~).

d. Provide and conduct security assistance visits and vulnerability assessments for all DIA elements, as well as other DoD Components under COM security responsibility, in accordance with References (~~km~~), (~~mi~~), (~~np~~), (~~pq~~), (~~qr~~), DoDD 3025.18 (Reference (~~np~~)), and DoDD ~~51205~~.75 (Reference (~~aqq~~)).

e. Provide completed vulnerability assessments or security assistance visit reports to the USD(I), ASD(HD&~~ASAGS~~), CJCS, Combatant Commanders, DoD IG, DOS Inspector General, Combatant Commander Inspectors General, DOS Diplomatic Security Service, senior defense officials and defense attachés (SDOs and DATTs), and COMs.

f. Provide semi-annual updates to the ASD(HD&~~ASAGS~~), CJCS, and Combatant Commanders on trend items and lessons learned.

g. Maintain a centralized database of all vulnerability assessments conducted that concern DoD elements under COM security responsibility.

h. In coordination with the cognizant geographic Combatant Commander and DOS personnel, ensure that AT plans for all DoD elements under COM security responsibility comply with Reference (~~mo~~).

i. Maintain an international terrorism database that includes international counterterrorism policies and response capabilities.

j. Provide the senior DIA voting member and the alternate senior DoD voting member to the OSPB.

k. Ensure the databases listed in paragraphs 10.g. and 10.i. are properly scheduled for disposition in accordance with chapter XII, subchapter B of title 36, Code of Federal Regulations (Reference (~~aqr~~)).

11. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS). The DIRNSA/CHCSS, under the authority, direction, and control of the USD(I) and in addition to the responsibilities in section 17 of this enclosure, shall:

a. Disseminate signals intelligence (SIGINT) reports on international terrorist threats against U.S. interests globally to the intelligence community and other DoD Components on a timely basis. Ensure compliance with the No-Double-Standard Policy (as described in the Glossary).

b. Maintain an international terrorism communication profile database that shall include international terrorist group communications systems and international terrorist group profiles based on SIGINT. Ensure this database is properly scheduled for disposition in accordance with DoD 5240.1-R (Reference (~~aqs~~)).

- c. Produce and coordinate SIGINT-based international terrorist threat warnings.
- d. Through the Signals Intelligence Directorate, Counter Terrorism Mission Management Center, serve as the focal point for coordination of international terrorist issues with the intelligence community, the DoD, and non-DoD law enforcement elements, as required.
- e. Provide SIGINT support for AT aspects of major U.S. deployments, as required.
- f. Provide a representative to the OSPB.
- g. Provide defensive travel briefings to DoD personnel who have been approved for foreign travel as appropriate.

12. USD(P&R). The USD(P&R) shall:

- a. Ensure that Department of Defense Education Activity (DoDEA) AT programs are adequately resourced with AT-trained administrators and security personnel, effective AT protective measures are incorporated into daily operations, comprehensive AT Program Reviews or assessments are conducted, and programs are synchronized with the appropriate geographic Combatant Commander to provide AT protection for DoD elements and personnel engaged in DoDEA-sponsored activities.
- b. Coordinate with the Secretaries of the Military Departments, the CJCS, the geographic Combatant Commanders, and the Directors of the Defense Agencies concerning AT considerations in establishing tour lengths, and to determine whether dependents should accompany personnel assigned overseas. In coordination with the ASD(HD&ASAGS), submit appropriate personnel and readiness recommendations to the Secretary of Defense.

13. ASSISTANT SECRETARY OF DEFENSE FOR HEALTH AFFAIRS (ASD(HA)). The ASD(HA), under the authority, direction, and control of the USD(P&R), shall:

- a. Serve as the principal advisor to the Secretary of Defense and the USD(P&R) for all matters concerning the formulation of policy and plans for Force Health Protection ~~and Mission Assurance~~ programs in support of the DoD AT Program.
- b. Develop and implement a Force Health Protection Program in accordance with DoDD 6200.04 (Reference (a#)) and serve as the principal advisor to the Secretary of Defense, the USD(P&R), and the CJCS on appropriate preventive measures and medical countermeasures to maximize force health protection.
- c. Advise and provide recommendations on requirements for CBRNE health and medical response and related functions including but not limited to vaccine protection, emergency decontamination at medical treatment facilities, medical surveillance, medical management

relating to exposure to weapons of mass destruction (WMD), preventive medicine functions, and medical training.

14. ASSISTANT SECRETARY OF DEFENSE FOR *MANPOWER AND* RESERVE AFFAIRS (ASD(*M&RA*)). The ASD(*M&RA*), under the authority, direction, and control of the USD(P&R), shall monitor Reserve Component readiness and training policies and funding allocated for domestic and overseas AT preparedness.

15. ASSISTANT TO THE SECRETARY OF DEFENSE FOR INTELLIGENCE OVERSIGHT (ATSD(IO)). Pursuant to DoDD 5148.11 (Reference (*asu*)), the ATSD(IO) will review, as appropriate, the DoD intelligence and counterintelligence support provided in accordance with this Instruction for compliance with DoDD 5240.01 (Reference (*atv*)) and Reference (*afs*). The ATSD (IO) will also assess compliance with References (*atv*) and (*afs*) as part of its inspection program.

16. DIRECTOR, PENTAGON FORCE PROTECTION AGENCY (PFPA). The Director, PFPA, under the authority, direction, and control of the Director of Administration and Management and in addition to the responsibilities in section 17 of this enclosure, shall develop and implement a comprehensive AT program in accordance with this Instruction and Reference (*ap*) for the people, facilities, infrastructure, and other resources located on the Pentagon Reservation and for the DoD elements and DoD-occupied facilities not under the jurisdiction of a Military Department within the National Capital Region or not part of any DoD Component that already has an AT program.

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

a. Support the geographic Combatant Commanders as they exercise TACON for FP responsibility within their respective AORs. Pursuant to this Instruction and Reference (*ap*), institute AT programs and incorporate appropriate AT standards into contingency response plans.

b. Use References (*ap*) and (*bkm*) for AT planning and execution.

c. Coordinate with geographic Combatant Commanders to ensure that AT plans and policies do not conflict with AT plans and policies of the geographic Combatant Commanders.

d. Ensure that:

(1) All personnel comply with References (v) and (*wy*).

(2) Personnel are aware of any theater travel security advisories in effect at the time of travel.

e. As part of the PPBE process, identify and document resource requirements necessary to implement and maintain AT programs.

(1) Submit AT requirements to the Secretary of Defense. Provide an information copy to ASD(HD&ASAGS) and the CJCS.

(2) Consider resource requirements in program and budget submissions. For emergent or emergency AT requirements that cannot be funded through other means, submit requirements through the appropriate geographic Combatant Commander to the CJCS for CCIF or, when funded, CbT RIF consideration.

(3) Implement accounting procedures to enable precise reporting of data submitted to Congress in the Congressional Budget Justification Book (CJB), including the number and cost of personnel directly supporting DoD AT activities.

f. Identify and recommend for designation high-risk personnel (HRP) in accordance with DoDI O-2000.22 (Reference (auw)). Ensure that AT training is provided to HRP and their dependents, as appropriate.

g. Incorporate current ~~physical~~ security requirements into all new contracts and leverage existing security technology to meet these requirements as appropriate.

h. Develop policy to ensure coordination with appropriate civil authorities as required, and as appropriate and permitted by law formalize these relationships through MOUs or MOAs.

i. Include AT protective features for facilities and installations in the planning, design, and execution of minor and military construction projects and leases to mitigate AT vulnerabilities and terrorist threats (protection requirements are described in Reference (yaa), Unified Facilities Criteria (UFC) 4-020-01 (Reference (avx)), and DoDD 5100.01 (Reference (awy))).

18. SECRETARIES OF THE MILITARY DEPARTMENTS. The Secretaries of the Military Departments, in addition to the responsibilities in section 17 of this enclosure, shall:

a. Support the geographic Combatant Commanders in exercising overall responsibility for AT within their respective AORs. Pursuant to this Instruction and Reference (h

), provide AT program policy that includes Reserve Component programs, to ensure that installation commanders (or other DoD officials responsible for installations) conduct vulnerability assessments that address terrorism as a potential threat to DoD elements and personnel.

b. Support the geographic and functional Combatant Commanders in complying with DoD Directive 5100.03 (Reference (axz)) by ensuring that sufficient resource requirements are considered in Military Department budget deliberations to implement Service Component AT or FP programs.

(1) Monitor all vulnerability assessments in the DoD-sponsored information system described in paragraph 10.g. of this enclosure. Prepare and disseminate analyses of Military Department-wide AT vulnerability trends as they relate to the PPBE process.

(2) Implement accounting procedures to enable precise reporting of data to the Office of the USD(AT&L) for inclusion in the CBJB, including the number and cost of personnel directly supporting DoD AT activities.

c. Coordinate with the appropriate Combatant Commander for intelligence that supports necessary protective measures for forces assigned to the geographic and functional Combatant Commands, or not under the authority of the geographic Combatant Commanders pursuant to References (g) and (mo).

d. Institute AT training programs pursuant to Reference (hp). Ensure doctrine developed for AT is compatible with joint doctrine and is incorporated in applicable curricula of Military Department schools. Ensure AT instruction is commensurate with the level of responsibility or command for which the school is designed. Maximize the use of advanced distributed learning technologies, as appropriate.

e. In coordination with the geographic Combatant Commander, promptly disseminate information on terrorist threats, including specific warning of threats against DoD elements and personnel pursuant to DoDD 8500.01E (Reference (ayba)) and the No-Double-Standard Policy (as described in the Glossary).

f. Implement procedures for Military Department personnel and their dependents to satisfy the requirements of References (vy) and (ayba). Implement procedures for DoD personnel and dependents scheduled for permanent change of station to foreign countries to receive the training required by Reference (hp).

g. Review AT programs and validate the thoroughness of the AT risk management methodology used to assess DoD elements and personnel criticality, terrorist threat, and vulnerabilities to make risk-based decisions for the application of appropriate countermeasures.

h. Integrate AT programs with relevant aspects of the Defense Critical Infrastructure Program in accordance with DoDD 3020.40 (Reference (azbb)) through the geographic Combatant Commands to address protection and assurance of critical infrastructure.

i. Ensure Service component commands have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

j. Monitor worldwide events for effects on AT and FPCONs in coordination with the Commanders of the Combatant Commands and the other Secretaries of the Military Departments. Assess the implementation and dissemination of FPCONs as specified by this Instruction and Reference (hp).

k. For AT program purposes, where the Military Department's supporting or subordinate Service component is designated as lead for a joint basing location, ensure that MOUs or MOAs address AT program coordination, particularly in regard to shared AT functions and responsibilities in order to maximize resource usage.

l. For AT program purposes, where the Military Department's supporting or subordinate Service component is not designated as lead for a joint basing location, ensure that Service commanders coordinate AT program execution with the designated joint base lead Service commander's AT program office.

m. Coordinate through the Joint Staff to provide assessments of DoD AT Programs at military installations worldwide, AT mobile training, and AT refresher courses, and to provide analytical support on AT issues as described in References (ahj) and (aik).

n. Ensure Service component commanders:

(1) Submit AT requirements to the Secretary of the Military Department concerned, and provide an information copy to the geographic Combatant Commander concerned.

(2) For emergent or emergency AT requirements that cannot be funded through other means, submit requirements through the appropriate Combatant Commander to the CJCS for CCIF consideration.

19. CJCS. The CJCS, in addition to the responsibilities in section 17 of this enclosure, shall:

a. Serve as the principal military advisor to the Secretary of Defense for all DoD AT issues.

b. Prepare joint doctrine for and assist the ASD(HD&ASAGS) in the development and maintenance of AT standards and procedures. Review DoD Component AT doctrine, standards, and procedures for compliance with this Instruction. Oversee, review, and coordinate AT Level I Awareness Training for all DoD personnel, including their dependents, in conjunction with the DoD Components. Conduct the Joint Staff Level IV AT Executive Seminar. Maintain a Web-based AT awareness training program that meets the requirements of Reference (hp).

c. Assess DoD Component AT policies and programs for the protection of DoD elements and personnel pursuant to this Instruction and References (mo), (hp), (zab), (aee), (aik), (ajl), (azbb), and DoDD O-5240.02 (Reference (bac)). Ensure such assessments are conducted for in-transit forces, air and sea ports of embarkation and debarkation, and CJCS exercises.

d. Review Combatant Commander joint operation plans, concept plans, functional plans, deployment orders, and other relevant documents for AT considerations.

e. Monitor worldwide events for effects on AT and FPCONs in coordination with the Commanders of the Combatant Commands and the Secretaries of the Military Departments.

Assess the implementation and dissemination of FPCONs as specified by this Instruction and Reference (~~np~~).

f. Coordinate with the USD(I), Director, DIA, ASD(HD&~~ASAGS~~), and ASD(SO/LIC) on sharing terrorism intelligence and counterintelligence data and terrorist threat information. This includes sharing data and information on threats posed to the DoD Components and DoD elements and personnel by domestic and international terrorists.

g. Coordinate with the Director, DIA, to assess the capability of the Military Departments, the Combatant Commands, and the defense intelligence and security organizations to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Assess the capability to fuse suspicious activity reports (SARs) from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

h. In coordination with the ASD(HD&~~ASAGS~~), manage and administer the CJCS CCIF pursuant to Reference (~~fw~~). Ensure that out-year maintenance costs for CCIF-funded projects are identified and coordinated with the Military Departments and that they are considered in the PPBE process.

i. Provide an observer to the OSPB.

j. Integrate AT programs with relevant aspects of the ~~DCIP~~CIP through the DoD Components in accordance with Reference (~~azbb~~) and other protection-related programs to address protection and assurance of critical infrastructure.

k. Provide, in coordination with the Director, DTRA, AT vulnerability assessments and training of DoD elements, installations, and personnel worldwide in accordance with this Instruction and References (~~np~~), (~~ak~~), and (~~ajl~~).

l. In coordination with the ASD(HD&~~ASAGS~~) and the Director, DTRA, develop and distribute DoD ~~Vulnerability-Mission Assurance~~ Assessment Benchmarks.

m. Maintain a centralized database of all vulnerability assessments conducted. Prepare and disseminate analysis of DoD-wide AT vulnerability trends correlated to Military Department efforts within the PPBE process.

n. Manage the tracking, scheduling, and risk management activities of the antiterrorism portion of ~~vulnerability-mission assurance~~ assessments for the Department (includes risk assessments, ~~mission assurance assessments~~, and other assessment programs that incorporate the AT Program elements with other protection programs). These activities will be coordinated through the Combatant Commands, Military Departments, and Defense Agencies and will include:

- (1) Developing, coordinating, and publishing annual assessment schedules.

(2) Integrating and deconflicting AT assessments with other protection assessment programs consistent with paragraph 19.j.

(3) Tracking Component-level assessments.

(4) Managing the AT risk management function and related data system for DoD as specified in paragraph 10.g of this enclosure.

(5) Publishing DoD Assessment Benchmarks for DoD-wide utilization.

(6) Coordinating with the Director, DTRA, for establishment of technical and field agency support to the CJCS for the scheduling and execution of assessments, AT training, and analytical support consistent with References (a**h**j) and (a**i**k).

(7) Publishing assessments guidance to the DoD Components.

20. COMMANDERS OF THE GEOGRAPHIC COMBATANT COMMANDS. The Commanders of the geographic Combatant Commands, through the CJCS as appropriate and in addition to the responsibilities in section 17 of this enclosure, shall:

~~—a. Exercise TACON for FP over all DoD personnel within their geographic AORs, with the exception of DoD personnel for whom DOS, through the COMs, has security responsibility as prescribed in References (g) and (m). TACON for FP applies to all DoD elements and personnel assigned permanently or temporarily to, transiting through, or performing exercises or training in the AOR, including forces or personnel assigned to United Nations or other multinational peace operations. TACON for FP is in addition to the normal exercise of command authority over assigned or attached forces.~~

a. Enforce appropriate FP measures to ensure the protection of all DoD elements and personnel subject to their control within their AORs, including personnel on temporary duty, with the exception of DoD personnel for whom the COMs have security responsibility, as described in References (g) and (o). Exercise TACON for FP over all DoD military personnel assigned permanently or temporarily to, transiting through, or performing exercises or training within their geographic AORs. This includes forces or personnel assigned to the United Nations or other multinational peace operations, with the exception of DoD personnel for whom DOS, through the COMs, has security responsibility, as prescribed in References (g) and (o). TACON for FP is in addition to the normal exercise of command authority over assigned or attached forces.

b. Establish AT policies and programs for the protection of all DoD elements and personnel in their AORs, including those for whom they assume AT responsibility based on an MOA with a COM in accordance with References (g), (a**h**n), and (a**m**o). Coordinate with the COMs in their AORs to identify all DoD Components and DoD elements and personnel. Develop and maintain MOAs with COMs that clearly delineate security responsibility for DoD personnel based on

whether the COM or the geographic Combatant Commander is in the best position to provide FP and in accordance with References (g), (h), and (mo).

c. Include in AT policies and programs specific prescriptive standards derived from Reference (np) to address specific terrorist threat capabilities and geographic settings.

d. Establish a comprehensive assessment program. Periodically assess and review the execution of AT standards and measures of all DoD elements and personnel for whom they exercise TACON for FP pursuant to this Instruction and Reference (np), either through their respective staffs, the Joint Staff/DTRA assessment program, or through Military Services, Military Service component commands, or other subordinate commands reporting to them. Report to the Secretary of Defense, through the CJCS, all pertinent actions taken for AT protection as a result of the AT program reviews. AT program reviews shall:

(1) Include a validation of the thoroughness of the AT risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities and to make risk-based decisions for the application of appropriate countermeasures.

(2) Evaluate installation and activity preparedness to respond to terrorist incidents and to manage the consequences of terrorist incidents. If deficiencies are identified, coordinate with appropriate Service component commanders to identify requirement and resource gaps.

e. Consistent with References (h) and (mo), serve as the DoD point of contact with host-nation officials on matters involving AT policies and measures.

f. Provide updates to References (v) and (wy) stating command travel requirements and theater entry requirements.

g. Provide all assigned and attached DoD elements and personnel, and DoD contractor personnel in accordance with paragraph 4.j. above the signature of this Instruction, with applicable AT training and briefings pursuant to Reference (np).

(1) Support the requirement for DoD personnel to comply with References (v) and (wy) when traveling in the AOR.

(2) Develop and implement policies and procedures that support and enforce the requirement for personnel to be aware of travel warnings in effect at the time of travel.

(3) Provide all assigned DoD personnel (including dependents) scheduled for permanent change of station with required AT training and briefings (e.g., AOR updates) in compliance with Reference (np). Provide threat assessments to transient (in-transit) forces in the AOR or planning to enter the AOR.

(4) Identify and disseminate or make available to deploying force providers relevant threat information and specific AOR pre-deployment training requirements that all personnel must complete before arrival in theater.

h. Identify, document, validate, prioritize, and submit to the Joint Staff, Director of Operations, the resource requirements necessary to achieve the AT program objectives for each activity assigned or attached under their command. Work with the Joint Staff and the Service component commands to ensure that resource requirements to implement AT programs are identified and considered in the PPBE process.

i. Develop, maintain, and implement AT plans and programs that incorporate AT measures at installations and activities consistent with DoD standards.

j. Coordinate AT plans of activities and tenant units with host installations, and ensure host installations incorporate activity and tenant requirements into the overall installation AT plan.

k. Establish command relationships and policies for subordinate commands, including joint task forces, to ensure that effective mechanisms are in place to maintain an AT protective posture commensurate with the terrorist threat.

l. Assess the terrorist threat for their AORs in accordance with Reference (np) and provide threat assessment information to the DoD Components and the COMs in their AORs. *DoDI 1400.31* (Reference (bjd)) can also be used as a guide for this function. Provide threat information requirements to the DoD Components in their AORs, other Combatant Commanders, and the DIA DCTC to enable threat information sharing.

m. Inform subordinate commanders (and appropriate DoD civilian managers and directors) of the nature and level of the terrorist threat. Ensure that:

(1) Commanders and DoD civilian managers and directors are prepared to respond to changes in threats and local security circumstances.

(2) COMs are informed on all issues affecting security, including threats and FPCON status, and that a full exchange of information affecting protective measures and TTLs for DoD elements and personnel is coordinated to reduce differences in standards of protection.

n. Coordinate as appropriate with the Secretaries of the Military Departments to ensure elimination of potential gaps in information sharing.

o. Comply with the No-Double-Standard Policy (as described in the Glossary).

p. Establish the baseline FPCON for the AOR and procedures to ensure that FPCONs and FPCON measures are disseminated and implemented as specified by this Instruction and Reference (np).

q. Ensure that a capability exists to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack. Develop the capability to fuse SARs from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities; disseminate these SARs as appropriate. Fusion of intelligence and law enforcement

information shall be accomplished pursuant to References (~~apr~~) and DoD Instruction 2000.26 (Reference (~~b~~)).

r. Submit to the CJCS priority emergent or emergency AT requirements that cannot be funded by the Military Departments for CCIF funding consideration (or through CbT RIF when available).

s. Coordinate AT program issues with the functional Combatant Commanders, the COMs, the Directors of the Defense Agencies and DoD Field Activities, and the Secretaries of the Military Departments, as appropriate.

t. Monitor worldwide events for effects on AT and FPCONs in coordination with the other Commanders of the Combatant Commands and the Secretaries of the Military Departments. Assess the implementation and dissemination of FPCONs as specified by this Instruction and Reference (~~pq~~).

u. Establish FP standards in their AORs for DoD civilian employees, family members of DoD civilian employees outside the United States, and dependents of DoD military personnel (these standards would not apply to persons under DOS security responsibility).

21. COMMANDERS OF THE FUNCTIONAL COMBATANT COMMANDS. The Commanders of the functional Combatant Commands, through the CJCS as appropriate and in addition to the responsibilities in section 17 of this enclosure, shall:

a. Establish AT policies and programs for assigned DoD elements and personnel, including policies and programs for assessment and protection of facilities and for providing the appropriate level of AT training and briefings. Coordinate these programs with the appropriate geographic Combatant Commanders and with their COMs.

b. Coordinate with the geographic Combatant Commanders and Service component commanders to ensure adequate AT protection of forces.

c. Ensure that subordinate elements that are tenant units on DoD installations and facilities coordinate their AT programs and requirements with their respective host installation commanders. Ensure they resolve any differences through the applicable Combatant Command and Service component command chains of command.

d. For priority emergent or emergency AT requirements that cannot be funded through other means, submit requirements to the CJCS for CCIF consideration (or through CbT RIF when available) and provide a copy of the submission to the appropriate geographic Combatant Commander.

e. Identify, document, and submit to the Joint Staff the resource requirements necessary to achieve AT program objectives for each activity under their command or for which they have FP responsibility. Work with the Service component commands to ensure that resource

requirements needed to implement their AT programs are identified and considered in the PPBE process.

ENCLOSURE 3

DCTC

The DCTC shall:

- a. In accordance with USD(I) Memorandum (Reference (b~~ef~~)), serve as the lead national-level, all-source international terrorism intelligence effort within DoD and as the analytical lead and the mission manager for combating terrorism issues pertaining to domestic and international terrorist threats to DoD elements and personnel (excluding threats posed by U.S. persons who have no foreign connection as defined in Reference (a~~qs~~)).
- b. Operate the Defense Terrorism Threat Warning System to provide prompt dissemination of intelligence on international terrorist threats including specific warning of threats against DoD elements and personnel pursuant to Reference (b~~ef~~) and the Interagency Intelligence Committee on Terrorism Guidelines (Reference (b~~dg~~)). Warnings to DoD personnel and their dependents shall be in accordance with the No-Double-Standard Policy (as described in the Glossary). The Defense Terrorism Threat Warning System includes:
 - (1) Producing all DoD terrorist threat warnings and providing DoD input for all intelligence community alerts, advisories, and assessments.
 - (2) Providing the support to the Combatant Commands and other key DoD elements as described in Office of the Director of National Intelligence Memorandum (Reference (b~~eh~~)).
 - (3) Implementing Reference (b~~dg~~).
 - (4) Setting DoD TTLs for all countries. TTLs shall be established as the result of all-source analysis and incorporation of Combatant Command and Military Department input. The DCTC shall coordinate country TTLs with the appropriate Combatant Commands, Military Departments, and DATT offices.
- c. Operate a 24-hour terrorism intelligence Warning and Fusion Center within the DCTC as the counterterrorism adjunct to the National Joint Operations and Intelligence Center, and ensure terrorist threat intelligence is disseminated to the appropriate DoD Components.
- d. Provide the DoD representative to, and provide Defense Intelligence Enterprise input to, the Interagency Intelligence Committee on Terrorism.
- e. Maintain a CbT knowledge base including information on international terrorist groups, capabilities, facilities, incidents, biographies, and biometrics.
- f. Subject to the provisions of References (a~~qs~~) and (b~~eh~~), assess the international terrorist threat worldwide, ensure dissemination of threat information to the DoD Components, and produce daily international terrorist threat awareness reports.

g. Serve as the lead DoD official for, and provide the DoD and the intelligence communities with, analytical products, studies, and analyses that pertain to international terrorist threats to the DoD Components and DoD elements and personnel. These products shall be consistent with the principles established in References (b(6)) and (b(7)).

h. Function as the Defense Intelligence Enterprise primary intelligence mission manager for CbT issues, and serve as the intelligence point of contact for the National Counterterrorism Center in accordance with Reference (b(7)).

i. Function as the DoD intelligence lead for the intelligence community terrorist watchlist effort in support of Homeland Security Presidential Directive (HSPD) 6 (Reference (b(7))) and National Security Presidential Directive 59/HSPD-24 (Reference (b(6))).

j. Monitor the Defense Intelligence Enterprise to ensure the Combatant Commands and Military Departments have the capability to collect, receive, evaluate, analyze, and disseminate all relevant data on terrorist activities, trends, and indicators of imminent attack.

k. Provide defense intelligence subject matter expertise for AT and CbT issues to OSD, the Joint Staff, and DIA, as required.

l. Attend CSG meetings pertaining to terrorism in coordination with the ASD(SO/LIC) and the Joint Staff Director of Operations.

m. In accordance with USD(I) Memorandum (Reference (b(6))), serve as the DoD lead to facilitate selective access to international terrorism-related information that might indicate a threat to DoD personnel, official visitors, facilities, information systems, or infrastructure.

GLOSSARYPART I. ABBREVIATIONS AND ACRONYMS

| | |
|----------------------------|--|
| AOR | area of responsibility |
| ASD(EI&E) | Assistant Secretary of Defense for Energy, Installations, and Environment |
| ASD(GSA) | Assistant Secretary of Defense for Global Strategic Affairs |
| ASD(HA) | Assistant Secretary of Defense for Health Affairs |
| ASD(HD& ASAGS) | Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs <i>Global Security</i> |
| ASD(NCB) | Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs |
| ASD(RA) | Assistant Secretary of Defense for Reserve Affairs |
| ASD(SO/LIC) | Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict |
| AT | antiterrorism |
| ATSD(IO) | Assistant to the Secretary of Defense for Intelligence Oversight |
| CBJB | Congressional Budget Justification Book |
| CBRNE | chemical, biological, radiological, nuclear, and high-yield explosive |
| CbT | combating terrorism |
| CbT-RIF | Combating Terrorism Readiness Initiative Fund |
| CCIF | Combatant Commander Initiative Fund |
| CJCS | Chairman of the Joint Chiefs of Staff |
| COM | Chief of U.S. Diplomatic Mission |
| CIP | critical infrastructure protection |
| CSG | Counterterrorism Security Group |
| DATT | Defense Attaché |
| DCIP | Defense Critical Infrastructure Program |
| DCTC | Defense Combatting Terrorism Center |
| DHS | Department of Homeland Security |
| DIA | Defense Intelligence Agency |
| DIRNSA/CHCSS | Director, National Security Agency/Chief, Central Security Service |
| DoDD | DoD Directive |
| DoDEA | Department of Defense Education Activity |
| DoDI | DoD Instruction |
| DOS | Department of State |
| DTRA | Defense Threat Reduction Agency |
| DUSD(I&E) | Deputy Under Secretary of Defense for Installations and Environment |

| | |
|------------|---|
| FP | force protection |
| FPCON | force protection condition |
| HRP | high-risk personnel |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| OSPB | Overseas Security Policy Board |
| PFFPA | Pentagon Force Protection Agency |
| PPBE | planning, programming, budgeting, and execution |
| RSO | Regional Security Officer |
| SAR | suspicious activity report |
| SDO | senior defense official |
| SIGINT | signals intelligence |
| TACON | tactical control |
| TTL | terrorism threat level |
| U.S.C. | United States Code |
| USD(AT&L) | Under Secretary of Defense for Acquisition, Technology, and Logistics |
| USD(C)/CFO | Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense |
| USD(I) | Under Secretary of Defense for Intelligence |
| USD(P) | Under Secretary of Defense for Policy |
| USD(P&R) | Under Secretary of Defense for Personnel and Readiness |
| WMD | weapons of mass destruction |

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this Instruction.

AT. Defined in Joint Publication 1-02 (Reference (b*i*)).

AT awareness. Fundamental knowledge of both the terrorist threat and the measures to reduce personal vulnerability to terrorism.

AT planning. The process of developing specific AT guidance and execution-oriented instructions for subordinates. AT planning is one of the five minimum elements of an AT program.

AT program review. The process of developing specific guidelines used to evaluate an AT program in order to assess and evaluate its effectiveness and adequacy satisfactorily. AT program review is one of the five minimum elements of an AT program.

AT resource application. The process of identifying and submitting requirements through existing PPBE process, CbT-RIF, and other funding mechanisms. AT resource application is one of the five minimum elements of an AT program. Tracking is central to the success of resource generation, as is ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

AT risk management. The process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits. AT risk management is one of the five minimum elements of an AT program. The end products of the AT program risk management process shall be the identification of DoD elements and personnel that are vulnerable to the identified threat attack means. From the assessment of risk based upon the three critical components of AT risk management (threat assessment, criticality assessment, and vulnerability assessment), the commander or DoD civilian manager or director must determine which DoD elements and personnel are at greatest risk and how best to employ given resources and FP measures to deter, mitigate, or prepare for a terrorist incident.

AT training and exercises. The process of developing individual, leader, and collective skills and of conducting comprehensive exercises to validate plans for AT incident response, consequence management, and continuity of essential military operations. AT program training and exercises is one of five minimum elements of an AT program.

CbT. Within DoD, encompasses all actions taken to oppose terrorism throughout the entire threat spectrum including terrorist use of CBRNE devices. Actions taken include AT, counterterrorism, terrorism consequence management, and intelligence support (collection, analysis, and dissemination of terrorism-related information).

COM diplomatic security responsibility. The responsibility of a COM for protecting all official U.S. personnel and facilities within the host country except those under the security responsibility of the geographic Combatant Commander. The COM administers the security program through the DOS Regional Security Officer (RSO) in accordance with DOS and OSPB policies and standards. The RSO is the COM's law enforcement and security advisor and represents the U.S. Federal and local law enforcement authorities not resident in the country. Depending on the local conditions and needs, the COM may also elect to implement security procedures that exceed required levels set forth by the OSPB. When a COM has security responsibility for DoD elements and personnel, all DOS, OSPB, and locally implemented RSO security policies apply to DoD elements under the COM's security responsibility.

Combatant Command. Defined in Reference (b*if*).

consequence management. Defined in Reference (b*if*).

counterintelligence. Defined in Reference (b*if*).

counterterrorism. Defined in Reference (b*if*).

crisis management. Those measures taken to resolve a hostile situation and to investigate and prepare a criminal case for prosecution under Federal law. Crisis management shall include a response to an incident involving WMD, a special improvised explosive device, or a hostage crisis that is beyond the capability of the lead Federal agency.

criticality assessment. Defined in Reference (b*if*).

DATT. Defined in Reference (a*oq*).

~~DCIP. Defined in Reference (a*z*).~~

defense critical infrastructure. Defined in Reference (b*if*).

dependents. Defined in section 1072 of Reference (e).

DoD civilian work force. Defined in DoD Directive 1400.31 (Reference (b*if*)).

DoD contractor. Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the DoD to furnish services, supplies, or both, including construction. DoD contractors may include U.S. nationals, local citizens, or third-country nationals. DoD contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the DoD (including selling to the DoD Components) or foreign corporations wholly owned by foreign governments.

DoD installations and facilities. Includes any base, camp, post, station, yard, center, homeport facility for any ship, or other activity under the jurisdiction of DoD and, in the case of an activity in a foreign country, under the operational control of the Secretary of a Military Department or the Secretary of Defense, without regard to the duration of operational control.

domestic. Of or relating to the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, the Federated States of Micronesia, the Republic of the Marshall Islands, and any other U.S. possessions or territories, or any political subdivision thereof.

domestic terrorism. Terrorism perpetrated by the citizens or legal residents of one country against persons in that country. This includes acts against citizens of a second country when they are in the host country and are not the principal or intended target.

emergency CCIF requirement. An unanticipated CCIF requirement created by a combination of circumstances or the resulting state that requires immediate action to prevent, deter, or respond to a terrorist act. (See Reference (t) for a detailed discussion of CCIF request procedures.)

emergent CCIF requirement. A newly formed unexpected CCIF requirement resulting as a logical consequence of unforeseen circumstances and calling for prompt action. (See Reference (~~t~~w) for a detailed discussion of CCIF request procedures.)

food and water security. The protection of food and water sources from disruption and contamination or other terrorist acts that could severely affect operations. Food and water security measures include those actions taken to detect, prevent, and mitigate the effects from intentional acts designed to disrupt or contaminate food and water sources.

force health protection. Defined in Reference (b*i*l).

foreign connection. A foreign connection is established by a reasonable belief that a U.S. person is or has been in contact with, or has attempted to contact, a foreign person or a representative of a foreign power, or a reasonable belief that a U.S. person is acting or encouraging others to act to further the goals or objectives of a foreign person or foreign power.

foreign power. A foreign government or non-state entity, or any component thereof, whether or not recognized by the United States; a faction of a foreign nation or nations, not substantially composed of U.S. persons; an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by that foreign government or governments; a group or person engaged in or in activities in preparation for international terrorism; a group engaged in or in activities in preparation for international narcotics, weapons, or human trafficking; a foreign based political organization not substantially composed of U.S. persons; or an entity that is directed and controlled by a foreign government or governments.

FP. Defined in Reference (b*i*l).

FPCON. Defined in Reference (b*i*l).

HRP. Defined in Reference (b*i*l).

imminent. Ready to take place.

intelligence. Defined in Reference (b*i*l).

lead Federal agency. Defined in Reference (b*i*l).

Military Department. Defined in Reference (b*i*l).

Military Service. Defined in Reference (b*i*l).

No-Double-Standard Policy. The policy that no double standard shall exist regarding the availability of terrorist threat information and that terrorist threat information shall be disseminated as widely as possible within applicable law and regulations. This policy includes these requirements, responsibilities, and procedures:

For threats directed solely against the DoD in foreign countries and areas, the threat information shall be passed up the chain of command to the lowest level that has direct liaison with DOS or the appropriate U.S. embassies (or for non-Combatant Commander-assigned forces, the SDOs and DATTs). Within the United States, including its territories and possessions, the threat information shall be passed up the chain of command to the lowest level that has direct liaison with Department of Homeland Security (DHS), the Department of Justice, and other Federal law enforcement agencies. Except when immediate notice is critical to the security of DoD elements and personnel, DOS, the U.S. embassy(ies), or DHS shall be informed, as appropriate, of the threat information before release to DoD elements and personnel. When immediate notice is critical to the security of DoD elements and personnel, commanders and DoD civilian managers and directors may immediately disseminate the information to and implement appropriate AT protective measures for DoD elements and personnel; under such circumstances they shall as soon as possible inform DOS, the U.S. embassy(ies), or DHS, as appropriate, through the chain of command.

Commanders (and authorized DoD civilian managers and directors) also shall inform DOS, U.S. embassy(ies), or DHS of any changes to FPCON levels or the security posture that significantly affect the host nation or U.S. public. When FPCONs are changed based upon received threat information, both the threat information and notice of the changed FPCON shall be passed up the chain of command to the lowest level that has direct liaison with DOS, the U.S. embassies (or for non-Combatant Command-assigned forces, the SDOs and DATTs), or DHS. Coordination and cooperation with DOS, the U.S. embassy, or the DHS in these cases is NOT a request for concurrence. Rather, it is informing the COM or the Secretary of Homeland Security of the DoD response to a given terrorist threat. Although the COM or the Secretary of Homeland Security may not agree with the commander's assessment, the ultimate responsibility for protection of DoD elements and personnel rests with the commanders (and DoD civilian managers and directors) in the chain of command.

operational control. Defined in Reference (b)(1).

Overseas Security Advisory Council. A council established by DOS in 1985 to foster the exchange of information between American companies with overseas operations and the U.S. Government. Government and business representatives have joined to use the Council as a forum to produce a series of publications providing guidance, suggestions, and planning techniques on a variety of security-related issues including terrorism.

OSPB. An interagency organization established by the President to consider, develop, coordinate, and promote security policies, standards, and agreements on overseas security operations, programs, and projects that affect all U.S. Government agencies under the authority of a COM abroad. The DOS Director for Diplomatic Security chairs the OSPB.

physical security. Defined in Reference (b*1*).

protective service detail. Trained and armed protective security officials capable of providing continuous protection for a designated individual.

reasonable belief. Defined in Reference (a*es*).

Reserve Components. Defined in Reference (b*1*).

RSO. Defined in Reference (b*1*).

risk. Probability and severity of loss linked to hazards.

SAR. Official documentation of behavior that may be indicative of preoperational planning related to terrorism or criminal intentions.

SDO. Defined in Reference (a*eq*).

security. Defined in Reference (b*1*).

security organizations. Military law enforcement, military criminal investigative, and defense criminal investigative organizations and DoD-contracted security personnel tasked with providing protection for personnel or resources.

Service component command. Defined in Reference (b*1*).

TACON. Defined in Reference (b*1*).

TACON for FP. TACON that enables the geographic Combatant Commander to order implementation of FP measures and to exercise the security responsibilities outlined in any MOA concluded pursuant to Reference (g) (known as the “Universal MOU”). Further, TACON for FP authorizes the geographic Combatant Commander to change, modify, prescribe, and enforce FP measures for covered forces. This relationship includes the authority to inspect and assess security requirements, and submit budget requests to parent organizations to fund identified corrections. The geographic Combatant Commander may also direct immediate FPCON measures (including temporary relocation and departure) when in his or her judgment such measures must be accomplished without delay to ensure the safety of the DoD personnel involved. Persons subject to TACON for FP of a geographic Combatant Commander include Active and Reserve Component personnel (including National Guard personnel in a title 10 status) in the AOR.

terrorism. Defined in Reference (b*1*).

terrorism threat analysis. In AT, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DoD Components or DoD elements and personnel. A threat analysis shall review the factors of a

terrorist group's operational capability, intentions, activity, and the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment.

terrorism threat assessment. Includes:

The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat.

The product of a threat analysis for a particular unit, installation, or activity.

terrorist threat. An expression of intention, by an individual or group, to commit an act or acts of violence to inflict injury or damage in pursuit of political, religious, or ideological objectives.

TTL. An intelligence assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity, and operational environment. There are four TTLs: Low, Moderate, Significant, and High. Threat levels should not be confused with FPCONs. Threat-level assessments are provided to senior leaders to assist them in determining the appropriate local FPCON.

vulnerability. In AT, a situation or circumstance that if left unchanged and taken advantage of by terrorists may result in the loss of life or damage to mission-essential resources. This includes:

The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished.

The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment.

The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

vulnerability assessment. Defined in Reference (b)(1).