



Department of Defense

DIRECTIVE

NUMBER 2000.12

August 18, 2003

Certified Current as of December 13, 2007

ASD(SO/LIC&IC)

SUBJECT: DoD Antiterrorism (AT) Program

References: (a) DoD Directive 2000.12, "DoD Antiterrorism/Force Protection (AT/FP) Program," April 13, 1999 (hereby canceled)
(b) Section 134 of title 10, United States Code
(c) Unified Command Plan, *March 1, 2005*¹
(d) DoD USS Cole Commission Report², January 9, 2001
(e) through (an), see *Enclosure 1*

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Changes the name of the DoD Antiterrorism/Force Protection (AT/FP) Program to the DoD Antiterrorism (AT) Program.

1.2. Reissues *Reference (a)* to update DoD policies and assigns responsibilities for implementing the procedures for the DoD AT Program, pursuant to 10 U.S.C. 134; Unified Command Plan; DoD USS Cole Commission Report, dated January 9, 2001; GAO Report, dated September 19, 2001; Secretary of Defense Memorandum, dated May 9, 2001; and Deputy Secretary of Defense Memorandum, dated August 14, 2001 (*References (b) through (g)*).

1.3. Continues to authorize the publication of DoD Instruction 2000.16 and DoD 2000.12-H (*References (h) and (i)*), pursuant to the requirements of DoD *Instruction 5025.015025.1-M* (*Reference (j)*).

¹ Unified Command Plan is available from the OASD(SO/LIC&IC) SO&CT/AT, Room 5E368, 2500 Defense Pentagon, Washington, DC 20301

² Report is available via <http://defenselink.mil/pubs/cole20010109.html>

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as "the DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, the Marine Corps, and the Coast Guard (when operating as a Military Service in the Navy). The term "commanders," as used in this Directive, refers to personnel assigned to command positions at all levels and the heads of the Defense Agencies and Field Activities.

2.2. This Directive also applies to DoD military and civilian personnel and their dependent family members; DoD contractors; DoD installations and facilities; DoD-owned, leased, or managed infrastructure and assets critical to mission accomplishment; and other DoD-owned, leased, or managed mission essential assets (hereafter referred to collectively as "DoD Elements and Personnel") overseas and in the United States, its territories, and possessions. DoD Elements and Personnel under the security responsibility of the Department of State (DoS) pursuant to 22 U.S.C. 4801 - 4805, DoD Instruction 5210.84, Memorandum of Understanding between the Department of Defense and the Department of State on Security of DoD Elements and Personnel in Foreign Areas dated December 16, 1997, and Memorandum of Understanding between the Department of State and the Department of Defense on Overseas Security Support, dated September 17, 1990 (*References (k) through (n)*) and other DoD-DoS Memoranda of Understanding (MOU) shall comply with Overseas Security Policy Board (OSPB) and DoS security standards instead of DoD standards prescribed by this Directive and *References (h) and (i)*.

2.3. The OSD Principal Staff Assistants (PSAs) and the DoD Components shall implement their AT responsibilities, functions, and authorities in compliance with this Directive. Nothing herein shall be interpreted to subsume or replace the functions, responsibilities, or authorities of the OSD PSAs or those of the DoD Components prescribed by law or other DoD guidance.

2.4. The scope of this Directive only addresses the AT element (defensive measures to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military forces) of the Department of Defense's combating terrorism (CbT) activities.

3. DEFINITIONS

Terms used in this Directive are defined in *Enclosure 2*.

4. POLICY

It is DoD policy that:

4.1. The DoD Components and the DoD Elements and Personnel shall be protected from terrorist acts through a high priority, comprehensive AT program. The Department of Defense's AT program shall be all encompassing using an integrated systems approach.

4.2. The Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DoD Elements and Personnel subject to their control and shall ensure the AT awareness and readiness of all DoD Elements and Personnel (including dependent family members) assigned or attached. Commanders must ensure appropriate AT protection and readiness of DoD Elements and Personnel while pursuing mission accomplishment.

4.3. The geographic Combatant Commanders' AT policies take precedence over all AT policies or programs of any DoD Component operating or existing in that command's area of responsibility (AOR) except for those under the security responsibility of a Chief of Mission (COM) (References (m) and (n)). All DoD Personnel traveling into a Combatant Commander's AOR will familiarize themselves with all AOR-specific AT policies and comply.

4.4. A Combating Terrorism Readiness Initiatives Fund (CbT-RIF) is maintained to provide a flexible means to respond to emergent and/or emergency AT requirements (Chairman of the Joint Chiefs of Staff Instruction 5261.01 *EB*, Reference (o)).

4.5. All DoD military, DoD civilians, DoD dependent family members, and DoD contractors shall comply with theater, country, and special clearance requirements (DoD Directive 4500.54 and DoD 4500.54-G (References (p) and (q)) before overseas travel.

4.6. The Commanders do not have the same legal responsibility to provide security for DoD contractors as that provided for military forces or direct-hire employees. Contractors remain private U.S. citizens. The Department of Defense shall assist the Department of State (DoS), where militarily feasible, in supporting efforts to protect U.S. citizens abroad. Contractors are required to contact the Combatant Command to obtain, and comply with, the specific AT guidance for that particular area. Commanders are required to offer AT training to contractors under the terms specified in the contract. Contractors working within a U.S. military facility or in close proximity of U.S. Forces shall receive incidentally the benefits of measures undertaken to protect U.S. Forces.

4.7. Compliance with the "No Double Standard" policy on dissemination of terrorist threat information is maintained. (See definition E2.1.29. at *Enclosure 2*.)

4.8. The Department of Defense's AT program is one of several security-related programs that fall under the overarching Combating Terrorism and Force Protection programs. The AT program shall be a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program shall be AT risk management, planning, training and exercises, resource generation, and a program review.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Special Operations ~~and~~/Low-Intensity Conflict and Interdependent Capabilities (ASD(SO/LIC&IC)), under the Under Secretary of Defense for Policy (USD(P)), shall:

5.1.1. Serve as the PSA and civilian advisor to the USD(P) and the Secretary of Defense to provide overall direction and supervision for policy, program planning and execution, and allocation of resources for the AT activities of the Department of Defense (*References* (b), (e), and (f)).

5.1.2. Establish AT standards and monitor DoD Component AT programs to reduce the vulnerability of the DoD Components and the DoD Elements and Personnel to terrorist attack in coordination with the Chairman of the Joint Chiefs of Staff and the other Heads of the DoD Components.

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

5.1.4. Through the DoD Antiterrorism Coordinating Committee (ATCC), its subcommittees (see *Enclosure 3*), and other organizations, provide policy oversight and guidance to the DoD Components in support of respective AT program efforts.

5.1.5. Develop, publish, and maintain *References* (h) and (i) and other appropriate issuances necessary to provide standards and guidance on protective measures that serve to reduce the vulnerability of the DoD Components and the DoD Elements and Personnel from terrorist acts.

5.1.6. Develop, publish, and update the DoD Antiterrorism Strategic Plan to provide an overarching framework to guide the DoD Components' long-term AT program efforts.

5.1.7. Sponsor the DoD Worldwide Combating Terrorism Conference as a continuing forum for DoD Components and interagency officials to provide guidance, exchange ideas, and generate policy recommendations that shall reduce DoD vulnerabilities to terrorism. The conference provides significant support to the ASD(SO/LIC&IC)'s efforts to maintain strategic direction and focus across the broad spectrum of CbT activities, including AT activities.

5.1.8. Coordinate DoD AT Program physical security issues with the Under Secretary of Defense for Intelligence (USD(I)), the DoD Physical Security Review Board, the DoD Physical Security Equipment Action Group (PSEAG), the Technical Support Working Group (TSWG), and other relevant security boards and committees.

5.1.9. Coordinate with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) on physical security technology development and the application of new technology to meet AT needs.

5.1.10. Coordinate with the Assistant Secretary of Defense for Homeland Defense *and Americas' Security Affairs* (ASD(HD&ASA)) regarding policy and oversight of the AT Program, as it affects the DoD Components and the DoD Elements and Personnel in the 50 United States, its territories, and possessions.

5.1.11. Coordinate with the Assistant Secretary of Defense for Health Affairs (ASD(HA)) on all medical and medically related aspects of DoD AT plans and programs.

5.1.12. Coordinate with the Chairman of the Joint Chiefs of Staff to validate submissions for CbT-RIF requests.

5.1.13. Monitor resource requirements resulting from Joint Staff Integrated Vulnerability Assessment (JSIVA) trends in coordination with the Chairman of the Joint Chiefs of Staff, the USD(AT&L), the Under Secretary of Defense (Comptroller) (USD(C)), and the Director, Defense Threat Reduction Agency (DTRA).

5.1.14. Review, in conjunction with the appropriate PSAs, the adequacy of the plans and programs of the DoD Components in meeting the requirements of the DoD AT Program and, in particular, the AT programs of the Combatant Commanders. In coordination with the Chairman of the Joint Chiefs of Staff, advise the Secretary of Defense and the USD(P) on changes needed to meet requirements.

5.1.15. Provide centralized policy and instruction for Protective Service Operations (PSO) assigned to dignitaries and personnel in high-risk billets.

5.2. The ~~Assistant Secretary of Defense for Homeland Defense (ASD(HD&ASA))~~, under the USD(P), shall:

5.2.1. Serve as the PSA and civilian advisor to the USD(P) and the Secretary of Defense to provide supervision for Domestic policy, program planning and execution, and allocation of resources for the Domestic AT activities of the Department of Defense.

5.2.2. Coordinate domestic DoD AT policy issues with the ASD(SO/LIC&IC) to ensure DoD policy consistency.

5.2.3. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.2.4. Serve as the DoD Domestic Incident Manager for DoD support to State and local civil authorities.

5.3. The ~~Assistant Secretary of Defense for Global Security Affairs (ASD(GSA))~~ ~~Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation (DUSD(TSP&C))~~, under the USD(P), shall:

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

5.3.2. Conduct regular reviews and assessments of the state of AT-focused export controls for their effectiveness and efficacy. The assessments shall include specific recommendations and action plans to remedy any deficiencies identified within domestic or international laws, regulations, and practices.

5.3.3. Provide a representative to the Interagency Intelligence Committee on Terrorism and an observer to the DoD ATCC and appropriate subcommittees as required under *Enclosure 3*.

5.4. The ~~Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))~~ shall:

5.4.1. In coordination with the ASD(SO/LIC&IC) and the Principal Deputy Under Secretary of Defense for Personnel and Readiness (PDUSD(P&R)), under the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), ensure that the Defense Federal Acquisition Regulation Supplement (DFARS) (*Reference (r)*) reflects current DoD AT security requirements for defense contractors. Specifically, pursuant to DoD Instruction 3020.37 (*Reference (s)*) establish requirements in the DFARS for defense contractors performing DoD contracts outside the United States to:

5.4.1.1. Affiliate with the Overseas Security Advisory Council (OSAC) (if the contractors are U.S. companies).

5.4.1.2. Ensure that their personnel who are U.S. citizens register with the U.S. Embassy and advise those who are third-country nationals to comply with the requirements of the embassy of their nationality.

5.4.1.3. Provide AT awareness information to personnel (before they travel outside the United States) commensurate with the information the Department of Defense provides to its military, DoD civilian personnel, and families (to the extent such information may be made available).

5.4.1.4. Receive the most current AT guidance for personnel and comply with *References* (p) and (q), as appropriate.

5.4.2. Be the DoD official responsible for AT technology development and expeditious application of new technology to meet AT needs.

5.4.3. Be the DoD official responsible for evaluating and testing commercial-off-the-shelf products to support the rapid acquisition and quick field integration of state-of-the-art AT technology.

5.4.4. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.5. The Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs (ATSD(NCB)), under the USD(AT&L), shall:

5.5.1. Serve as the PSA and advisor to the Secretary and Deputy Secretary of Defense and the USD(AT&L) for all matters concerning the formulation of policy and plans for nuclear weapons safety and security, chemical and biological defense programs, to include Chemical, Biological, Radiological, Nuclear material, and high-yield Explosives (CBRNE) protection programs in support of the Department of Defense's AT Program.

5.5.2. In coordination with the ASD(SO/LIC&IC) and the ASD(HD&ASA), develop and maintain CBRNE standards for installation protection efforts in support of the Department of the Defense's AT Program. These standards shall serve to supplement DoD AT Standards (*Reference* (h)) by synchronizing CBRNE protection with AT defensive measures.

5.5.3. Provide an observer to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.6. The Director, Defense Threat Reduction Agency (DTRA), under the USD(AT&L), pursuant to DoD Directive 5105.62, DoD Directive 5105.67 (*References (t) and (u)*), and the current MOU between the Chairman of the Joint Chiefs of Staff and DTRA, shall:

5.6.1. In coordination with the Chairman of the Joint Chiefs of Staff, conduct vulnerability assessments of DoD assets worldwide based on this Directive and *References (h) and (i)*. Also, support assessments of Combatant Command and Military Service headquarters' AT programs, Joint Chiefs of Staff exercises, air/sea ports of embarkation/debarkation, and in-transit forces. Provide copies of all vulnerability assessments conducted to the DoD Counterintelligence Field Activity (CIFA).

5.6.2. Provide assessment teams and maintain the necessary supporting resources as required per OSD direction.

5.6.3. Maintain a vulnerability assessment database interoperable with the DIA and the JITF-CT and provide periodic analytic products to the Chairman of the Joint Chiefs of Staff to support the AT readiness of the DoD Components.

5.6.4. Maintain the capability to provide follow-up assistance to assessed organizations; assist in training Combatant Commander, Military Service, and DoD Agency vulnerability assessment teams; conduct special, tailored Chairman of the Joint Chiefs of Staff-directed vulnerability assessments; and provide other specialized assistance within its area of expertise.

5.6.5. Provide an observer to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.7. The ~~Under Secretary of Defense (Comptroller)~~ (USD(C)) shall:

5.7.1. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.7.2. Provide information and guidance to the DoD Components on displaying AT resources within the Planning, Programming, ~~and Budgeting~~, *and Execution System* (PPBE) ~~system program~~ and budget submissions (DoD Directive 7045.14, *Reference (v)*).

5.7.3. Provide reports on AT funds as requested by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff.

5.8. The ~~Under Secretary of Defense for Intelligence (USD(I))~~ shall:

5.8.1. Provide policy, guidance, and oversight for information management, intelligence, counterintelligence, physical security, personnel security, operations security, critical infrastructure protection, information operations, technical security countermeasures, security and investigative matters, and information assurance to assist the ASD(SO/LIC&IC) on matters pertaining to the AT program.

5.8.2. Review the DoD intelligence, counterintelligence, security, and information operations support provided under this Directive for compliance with *References (l)*, DoD Directive 5240.2, DoD Directive ~~3020.405160.54~~, and DoD Directive 8500.1 (*References (w)*, through (*y*)).

5.8.3. Monitor Defense Intelligence Agency (DIA), National Security Agency (NSA), and Counterintelligence Field Activity (CIFA) execution of AT responsibilities. See *Enclosures 4, 5, and 6* for DIA, NSA, and CIFA responsibilities.

5.8.4. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*. Provide the senior DoD voting member to the OSPB.

5.8.5. Annually, as part of the PPBES cycle and in coordination with the Chairman of the Joint Chiefs of Staff, review the adequacy of physical security, counterintelligence, intelligence, and other security resources to determine whether they adequately support AT program objectives. Assist and support the Chairman of the Joint Chiefs of Staff in advising the Secretary of Defense of any changes that are needed to meet AT requirements.

5.8.6. Monitor the DIA's activities as the DoD Executive Agent for diplomatic security matters (*References (l)* through (*n*)).

5.9. The ~~Principal Deputy Under Secretary of Defense for Personnel and Readiness (PDUSD(P&R))~~, under the (USD(P&R)), shall:

5.9.1. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.9.2. Ensure the 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, and programs are synchronized with the appropriate Combatant Commander to provide AT protection for the DoD Elements and Personnel engaged in DoDEA-sponsored activities.

5.9.3. Coordinate with the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, and the Directors of the Defense Agencies concerning AT considerations in establishing tour lengths and determine whether restrictions should be placed on accompanying dependent family members for personnel assigned overseas. In coordination with the ASD(SO/LIC&IC), submit appropriate personnel and readiness recommendations to the Secretary of Defense.

5.10. The ~~Assistant Secretary of Defense for Health Affairs (ASD(HA))~~, under the USD(P&R), shall:

5.10.1. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.10.2. Support the DoD AT Program by interfacing with the National Disaster Medical System to ensure appropriate protection for the DoD Elements and Personnel.

5.10.3. Advise and provide recommendations to the Secretary of Defense and the Chairman of the Joint Chiefs of Staff on appropriate medical countermeasures to maximize Force Health Protection (FHP).

5.10.4. Provide policy, guidance, and oversight in setting requirements for CBRNE health and medical response, and related functions to include, but not limited to, vaccine protection, emergency decontamination at Medical Treatment Facilities, medical surveillance, medical management resulting from exposure to weapons of mass destruction, preventive medicine functions, and medical training.

5.11. The Assistant Secretary of Defense for Reserve Affairs (ASD(RA)), under the USD(P&R), shall:

5.11.1. Provide an observer to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.11.2. Monitor Military Departments' Reserve component readiness and training policies and funding to provide for domestic and overseas AT preparedness.

5.12. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) shall:

5.12.1. Pursuant to DoD Directive 5148.11 (*Reference (z)*), review the DoD intelligence and counterintelligence support provided under this Directive for compliance with DoD Directive 5240.1 and DoD 5240.1-R (*References (aa) and (ab)*).

5.12.2. Provide an observer to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.13. The Director, Program Analysis and Evaluation (Dir, PA&E) shall:

5.13.1. Serve as the PSA to the Secretary of Defense for program analysis and evaluation to analyze and evaluate the plans, programs and budgets of the DoD Components.

5.13.2. Provide a member to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.14. The Directors of the Defense Agencies and the DoD Field Activities, the OSD Principal Staff Assistants, and those who report directly to the Secretary or Deputy Secretary of Defense shall:

5.14.1. Support the geographic Combatant Commanders as they exercise overall responsibility for AT within their respective AOR. Pursuant to this Directive and *References* (c) and (h), institute AT Programs, ensure that Defense Agencies and Field Activities conduct vulnerability assessments that address terrorism as a potential threat to the DoD Elements and Personnel, and incorporate AT measures into contingency response plans.

5.14.2. Use *References* (h) and (i) for the AT planning and execution for their headquarters and all activities under their cognizance: consider mission, characteristics of the activity, geographic location, threat level, and Force Protection Condition (FPCON). Establish prescriptive AT standards for installations and facilities not located on U.S. military installations. Coordinate with the applicable Combatant Commander to ensure that AT plans and policies are in concert with the geographic Combatant Commanders' overall responsibility for the AOR.

5.14.3. Comply with *Reference* (h) requirements to maintain an AT training program. Ensure that all assigned personnel comply with *References* (p) and (q). Ensure that personnel are aware of any travel security advisories in effect at the time of travel. Ensure that all DoD Personnel (including dependent family members) scheduled for permanent changes of station to foreign countries receive required AT training or briefing specified in *Reference* (h).

5.14.4. Provide members to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.14.5. As part of the PPBES cycle, identify and document resource requirements necessary to implement and maintain AT programs. Submit AT requirements to the Secretary of Defense with an information copy to the Chairman of the Joint Chiefs of Staff and the appropriate Combatant Commanders. Include resource requirements in program and budget submissions. For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements through the appropriate Combatant Commander to the Chairman of the Joint Chiefs of Staff for CbT-RIF consideration. Implement accounting procedures to enable precise reporting of data submitted to Congress in the Congressional Justification Book (CJB), including the number and cost of personnel directly supporting the *Department of Defense DoD's* AT activities.

5.14.6. Identify and designate incumbents of high-risk billets and dependent family members requiring AT resident training. Ensure that AT resident training is provided to personnel assigned to high-risk billets and others, as applicable.

5.14.7. Ensure that current physical security technology and security requirements are incorporated into all new contracts, where appropriate.

5.14.8. Ensure AT protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects to mitigate AT vulnerabilities and terrorist threats (UFC 4-010-01, UFC 4-010-~~0210~~, and UFC-4-021-01, *References* (ac), through (ae)).

5.14.9. Develop an AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense's AT Strategic Plan.

5.15. The Secretaries of the Military Departments shall:

5.15.1. Support the geographic Combatant Commanders as they exercise overall responsibility for AT within their respective AOR. Pursuant to this Directive and *References* (c) and (h), institute AT Programs (to include Reserve components), ensure that installations conduct vulnerability assessments that address terrorism as a potential threat to DoD Elements and Personnel, and incorporate AT measures into contingency response plans.

5.15.2. Support the geographic and functional Combatant Commanders as they comply with DoD Directive 5100.1 and DoD Directive 5100.3 (*References* (af) and (ag)) by ensuring that sufficient resources are programmed in Military Department budgets to implement Combatant Commander AT Programs.

5.15.2.1. Ensure life-cycle costs are programmed and funded for CbT-RIF projects (*Reference* (o)). Ensure CbT-RIF projects are not programmed for funding through other sources and determine optimum technology available to meet requirements.

5.15.2.2. Maintain a centralized database of all vulnerability assessments. Prepare and disseminate analyses of Military Department-wide AT vulnerability trends as they relate to the PPBES process.

5.15.2.3. Implement accounting procedures to enable precise reporting of data submitted to Congress ~~in the CJB~~, including the number and cost of personnel directly supporting the Department of Defense's AT activities.

5.15.3. Institute AT training programs pursuant to *Reference* (h). Ensure doctrine developed for AT is compatible with joint doctrine and is incorporated in applicable Military Service schools. Ensure AT instruction is commensurate with the level of responsibility or the command for which the school is designed. Maximize the use of Advanced Distributed Learning technologies, when appropriate.

5.15.4. Identify and designate incumbents of high-risk billets and dependent family members requiring AT resident training. Provide AT resident training to those personnel assigned to high-risk billets and others, as applicable.

5.15.5. Implement procedures for Military Department personnel and their dependent family members to satisfy the requirements of *References* (p) and (q). Also implement procedures for the DoD Personnel (including dependent family members) scheduled for permanent change of station to foreign countries to receive required training specified in *Reference* (h).

5.15.6. Promptly disseminate information on terrorist threats, including specific warning of threats against the DoD Elements and Personnel pursuant to *References* (aa) and (ab), and the "No Double Standard" policy. (See definition at E2.1.29, *Enclosure 2*.)

5.15.7. Ensure current physical security technology and security requirements are incorporated into all new contracts, where applicable.

5.15.8. Ensure AT protective features for facilities and installations are included in the planning, design, and execution of military and minor construction projects to mitigate AT vulnerabilities and terrorist threats (*References* (ac), through (ae)).

5.15.9. Ensure that installations and activities develop, maintain, and implement AT plans and programs that incorporate AT measures in concert with DoD standards and conduct comprehensive AT program reviews and assessments (*Reference* (h)). Ensure AT program reviews include a validation of the thoroughness of the AT risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities. AT program reviews shall also evaluate installation and activity preparedness to respond to terrorist incidents (including CBRNE incidents), and the plans for managing the consequences of terrorist incidents and maintaining continuity of essential military operations. Ensure installations and activities coordinate AT plans with tenant units to incorporate tenant AT program requirements into the host AT plan.

5.15.10. Provide Military Department representatives as members of the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3*.

5.15.11. 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. Develop the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

5.15.12. Develop a Military Department AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense and Combatant Commanders' AT Strategic Plans.

5.16. The Chairman of the Joint Chiefs of Staff shall:

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

5.16.2. Prepare joint doctrine and assist the ASD(SO/LIC&IC) in the development and maintenance of AT standards and procedures. Review doctrine, standards, and procedures of the DoD Components. Review, coordinate, and oversee for the Secretary of Defense and in conjunction with the DoD Components, the AT training for all DoD Personnel (including their dependent family members).

5.16.3. Ensure the Chairman's Program Review and the Chairman's Program Assessment include a summary of AT requirements as determined by the Joint Requirements Oversight Council and derived from Combatant Commander Integrated Priority Lists.

5.16.4. Annually, as part of the DoD program and PPBES cycle, assist the Military Departments in determining the merit of AT requirement submissions. Review the adequacy of resources proposed by the Military Departments to determine whether they meet AT objectives and support Combatant Commanders' AT programs. Coordinate and make recommendations on unresolved AT requirements during programming and budget reviews. These reviews shall be done in conjunction with OSD PSAs having resource, program, and budget oversight responsibilities for the functional areas that comprise the AT budget aggregate. Advise the Secretary of Defense of any changes needed to meet AT requirements.

5.16.5. Assess the DoD Components' AT policies and programs for the protection of DoD Elements and Personnel, including DoD-owned, leased, or managed infrastructure and assets critical to mission accomplishment and other DoD-owned, leased or managed mission essential assets pursuant to this Directive and References (h) and (x). Ensure assessments are conducted of Joint Chiefs of Staff exercises, air/sea ports of embarkation/debarkation, and in-transit forces.

5.16.6. Assess AT as an element of the overall force planning function of any force deployment decision. Periodically reassess AT posture of deployed forces. Review Reference (c), approved by the President, and the Secretary's "Forces for Unified Commands" Memorandum (Reference (ah)) to determine the impact on this Directive and the Department of Defense's AT Program. Recommend revisions to these plans or this Directive, as required. Review Combatant Commanders' joint operation plans (OPLANS, CONPLANS, and functional plans), deployment orders, and other relevant documents for AT considerations.

5.16.7. Assess the implementation of FPCONs for uniform implementation and dissemination as specified by this Directive and References (h) and (i).

5.16.8. Provide representatives to the DoD ATCC and appropriate subcommittees as required under *Enclosure 3*. Provide an observer to the OSPB. Appoint the Director for Operations, Joint Staff (J3) to co-chair the Antiterrorism Coordinating Committee - Senior Steering Group (ATCC-SSG) and the *Joint Staff* Deputy Director for ~~Global Operations~~ (~~Antiterrorism/Homeland Defense (DD AT/HD)Force Protection~~)-*Joint Staff* to co-chair the ATCC under *Enclosure 3*.

5.16.9. Coordinate with the USD(I) and the ASD(SO/LIC&IC) on sharing of terrorism intelligence and counterintelligence data and information on AT. This includes threats posed to the DoD Components and the DoD Elements and Personnel by domestic and foreign terrorists.

5.16.10. 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. Also assess the capability to fuse suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance and reconnaissance collection activities.

5.16.11. In coordination with the ASD(SO/LIC&IC), manage and administer the Chairman of the Joint Chiefs of Staff CbT-RIF pursuant to *Reference (o)*. Ensure out-year maintenance costs for CbT-RIF-funded projects are identified and coordinated with the Military Departments so that they are addressed during the PPBES cycle.

5.16.12. 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 PPBES process.

5.17. The Geographic Combatant Commanders have overall AT responsibility within their AOR (*Reference (c)*), except for those DoD Elements and Personnel for whom a COM has security responsibility pursuant to law (*Reference (k)*) or a Memorandum of Agreement (MOA) per *Reference (m)*. Accordingly, they shall:

5.17.1. Establish AT policies and programs for the protection of all DoD Elements and Personnel in their AOR, including those for whom the Combatant Commander assumes AT responsibility based on a MOA with a COM (*Reference (m)*). Coordinate with the COMs in the AOR to identify all non-Combatant Commander DoD Components and DoD Elements and Personnel. In instances where AT protection may be more effectively provided through the Combatant Commander, establish country-specific MOAs per *Reference (m)*.

5.17.2. Ensure AT policies and programs include specific prescriptive standards derived from *Reference (h)* to address specific terrorist threat capabilities and geographic settings, particularly regarding infrastructure critical to mission accomplishment and other DoD-owned, leased, or managed mission essential assets (*Reference (x)*).

5.17.3. Exercise tactical control (TACON) (for force protection) over all DoD Elements and Personnel (including force protection responsibility for DoD dependent family members) (except those under the security responsibility of a COM) within the Combatant Commander's AOR. TACON (for force protection) applies to all DoD personnel assigned permanently or temporarily, transiting through, or performing exercises or training in the Combatant Commander's AOR. TACON (for force protection) is in addition to a Combatant Commander's normal exercise of operational control (OPCON) over assigned forces.

5.17.4. Periodically, assess and review the AT programs of all Combatant Commander-assigned DoD Components in their AOR per this Directive and *Reference* (h). Also assess the AT programs of all DoD Components performing in their AOR that are not under the security responsibility of a COM. Military Service component commands or other subordinate commands reporting to the Combatant Commander may conduct the assessments. Ensure AT program reviews include a validation of the thoroughness of the AT risk management methodology used to assess asset criticality, terrorist threat, and vulnerabilities. AT program reviews shall also evaluate installation and activity preparedness to respond to terrorist incidents (including CBRNE incidents), and the plans for managing the consequences of terrorist incidents and maintaining continuity of essential military operations. Relocate forces as necessary and report to the Secretary of Defense through the Chairman of the Joint Chiefs of Staff pertinent actions taken for AT protection.

5.17.5. Consistent with *Reference* (l) and the MOUs (*References* (m) and (n)), serve as the DoD point of contact with host-nation officials on matters involving AT policies and measures.

5.17.6. Provide updates to *Reference* (p) and *Reference* (q) stating command travel requirements and theater entry requirements.

5.17.7. Ensure all assigned military, DoD civilians, Defense contractors, and their family members receive applicable AT training and briefings pursuant to *Reference* (h). Ensure personnel traveling in the AOR comply with *References* (p) and (q). Ensure personnel are aware of any Travel Warnings in effect at the time of travel. Ensure that all DoD Personnel (including dependent family members) scheduled for permanent change of station to the geographic Combatant Commander's AOR or to another geographic Combatant Commander's AOR receive required AT training and briefings (e.g., AOR Updates) in compliance with *Reference* (h). Identify and disseminate to deploying force providers specific AOR pre-deployment training requirements that all personnel must complete before arrival in theater.

5.17.8. Identify, document, validate, prioritize, and submit to the Joint Staff the resource requirements necessary to achieve the AT program objectives for each activity under the Combatant Commander or for which that Commander has AT responsibility. Work with the Joint Staff and the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to *PPBES* procedures.

5.17.9. 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.

5.17.10. Assess the terrorist threat for the AOR according to this Directive, and provide threat assessment information to the DoD Components and the COMs in the AOR. Develop risk mitigation measures and maintain a database of those measures and the issues that necessitated their implementation. On the basis of the threat assessment, identify and designate incumbents of high-risk billets and dependent family members to receive AT resident training.

5.17.11. Keep subordinate commanders informed of the nature and degree of the threat. Ensure that commanders are prepared to respond to changes in threats and local security circumstances. Ensure that the COMs are fully and currently informed of any threat information relating to the security of those DoD Elements and Personnel under their security responsibility, but not under the command of the Combatant Commander.

5.17.12. Ensure compliance with the "No-Double-Standard" policy. (See definition E2.1.29., *Enclosure 2.*)

5.17.13. Ensure that FPCONs are uniformly implemented and disseminated as specified by this Directive and *References (h) and (i).*

5.17.14. Provide a representative to the DoD ATCC and appropriate subcommittees, as required under *Enclosure 3.*

5.17.15. 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 suspicious activity reports from military security, law enforcement, and counterintelligence organizations with national-level intelligence, surveillance, and reconnaissance collection activities.

5.17.16. Submit to the Chairman of the Joint Chiefs of Staff emergent and/or emergency AT requirements that cannot be funded by the Military Departments for CbT-RIF funding consideration (*Reference (o).*)

5.17.17. Coordinate AT program issues with the functional Combatant Commanders, the COMs, the Defense Agencies/Activities, and the Military Departments, as appropriate.

5.17.18. Develop a geographic AOR, Combatant Commander-oriented AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense's AT Strategic Plan.

5.18. The Functional Combatant Commanders shall:

5.18.1. Establish AT policies and programs for assigned DoD Elements and Personnel including assessment and protection of facilities and appropriate level of AT training and briefings. Coordinate programs with the appropriate Combatant Commanders and the COMs.

5.18.2. Coordinate with the geographic Combatant Commanders to ensure adequate AT protection of forces (*References* (c) and (ah)).

5.18.3. Ensure that subordinate elements, which are tenant units on Military Service installations, coordinate their AT programs and requirements with the host installation commander. Differences shall be resolved through the applicable Combatant Commander and the Service component command chain of command.

5.18.4. Identify and designate incumbents of high-risk billets and dependent family members requiring AT resident training. Provide AT resident training to personnel assigned to high-risk billets and others, as applicable.

5.18.5. For emergent and/or emergency AT requirements that cannot be funded through other means, submit requirements to the Chairman of the Joint Chiefs of Staff for CbT-RIF consideration (*Reference* (o)).

5.18.6. Provide a representative to the DoD ATCC and appropriate subcommittees, as required under *Enclosure* 3.

5.18.7. Identify, document, and submit to the Joint Staff the resource requirements necessary to achieve AT program objectives for each activity under the Combatant Command or for which the Commander has AT responsibility. Work with the Service component commands to ensure that resource requirements to implement the AT programs are identified and programmed according to *PPBES* procedures.

5.18.8. Develop a functional Combatant Commander-oriented AT Strategic Plan that details the vision, mission, goals, and performance measures in support of the Department of Defense and geographic Combatant Commanders' AT Strategic Plans.

6. INFORMATION REQUIREMENTS

The DoD intelligence, counterintelligence, security, and information operations support activities described in this Directive are exempt from licensing in accordance with paragraphs C4.4.1., C4.4.2., and C4.4.8., of DoD 8910.1-M (*Reference* (ai)).

7. EFFECTIVE DATE

This Directive is effective immediately.



Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 6

- E1. References, continued
- E2. Definitions
- E3. ATCC and ATCC-SSG
- E4. DIA AT Responsibilities
- E5. NSA AT Responsibilities
- E6. CIFA AT Responsibilities

E1. ENCLOSURE 1

REFERENCES, continued

- (e) Secretary of Defense Memorandum, "Civilian Oversight of DoD Combating Terrorism and Consequence Management Activities,"³ May 9, 2001
- (f) Deputy Secretary of Defense Memorandum, "Civilian Oversight of DoD Combating Terrorism Activities,"⁴ August 14, 2001
- (g) GAO Report, "Combating Terrorism: Actions Needed to Improve DoD Antiterrorism Program Implementation and Management,"⁵ September 19, 2001
- (h) DoD Instruction 2000.16, "DoD Antiterrorism (AT) Standards," *October 2, 2006*
~~June 14, 2001~~
- (i) DoD Handbook 2000.12-H, "Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February ~~4, 2004~~~~19, 1993~~
- (j) *DoD Instruction 5025.1, "DoD Directives Program," October 28, 2007*
~~DoD 5025.1-M, "DoD Directives System Procedures," March 5, 2003~~
- (k) Sections 4801 - 4805 of title 22, United States Code
- (l) DoD Instruction 5210.84, "Security of DoD Personnel at U.S. Missions Abroad," January 22, 1992
- (m) Memorandum of Understanding between the Department of Defense and the Department of State on Security of DoD Elements and Personnel in Foreign Areas,⁶ December 16, 1997
- (n) Memorandum of Understanding between the Department of State and the Department of Defense on Overseas Security Support,⁷ September 17, 1990
- (o) Chairman of the Joint Chiefs of Staff Instruction 5261.01 ~~EB~~, "Combating Terrorism Readiness Initiative Fund," *April 27, 2007*~~July 1, 2001~~
- (p) DoD Directive 4500.54, "Official Temporary Duty Travel Abroad," May 1, 1991
- (q) DoD 4500.54-G, "DoD Foreign Clearance Guide (FCG),"⁸ current edition
- (r) Defense Federal Acquisition Regulation Supplement, ~~1998-~~ *current* edition
- (s) DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crisis," November 6, 1990
- (t) DoD Directive 5105.62, "Defense Threat Reduction Agency," *November 28, 2005*
~~September 30, 1998~~
- (u) DoD Directive 5105.67, "DoD Counterintelligence Field Activity," February 19, 2002
- (v) DoD Directive 7045.14, "The Planning, Programming, and Budgeting System (PPBS)," May 22, 1984
- (w) DoD Directive 5240.2, "DoD Counterintelligence," May 22, 1997
- (x) *DoD Directive 3040.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005*
~~DoD Directive 5160.54, "Critical Infrastructure Protection (CIP)," January 20, 1998~~

³ Copy of the memorandum available from OASD(SO/LIC&IC)

⁴ Copy of the memorandum available from OASD(SO/LIC&IC)

⁵ Copy of this report can be obtained via <http://gao.gov>

⁶ MOU available via <http://foia.state.gov/masterdocs/02fam/02m0110.pdf> (pages 48-58)

⁷ MOU available via <http://foia.state.gov/masterdocs/02fam/02m0110.pdf> (pages 17-35)

⁸ FCG available via <http://www.fcg.pentagon.smil.mil>

- (y) DoD Directive 8500.1E, "Information Assurance," October 24, 2002
- (z) DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO))," ~~July 1, 1994~~ *May 21, 2004*
- (aa) DoD Directive 5240.1, "DoD Intelligence Activities," ~~April 25, 1988~~ *August 27, 2007*
- (ab) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence" December 1, 1982
- (ac) Unified Facilities Criteria (UFC) 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings," ~~July 31, 2002~~ *October 8, 2003*
- (ad) Unified Facilities Criteria (UFC) 4-010-~~0210~~, "DoD Minimum Antiterrorism Standoff Distances for Buildings," July 31, 2002
- (ae) Unified Facilities Criteria (UFC) 4-021-01, "Design and O&M: Mass Notification Systems," December 18, 2002
- (af) DoD Directive 5100.1, "Functions of the Department of Defense and its Major Components," August 1, 2002
- (ag) DoD Directive 5100.3, "Support of the Headquarters of Unified, Specified, and Subordinate Joint Commands," November 15, 1999
- (ah) "Forces for Unified Commands Memorandum," current edition
- (ai) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (aj) Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms," May 7, 2002, *as amended*
- (ak) Section 1072(2) of title 10, Unites States Code
- (al) DoD Directive 3025.15, "Military Assistance to Civil Authorities," February 18, 1997
- (am) DoD Directive 5105.47, "US Defense Representatives (USDR) in Foreign Countries," September 20, 1991
- (an) DoD Instruction 5105.57, "Procedures for the US Defense Representative (USDR) in Foreign Countries," December 26, 1995

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Antiterrorism (AT). Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including limited response and containment by local military and civilian forces (Reference (i)).

E2.1.2. Antiterrorism (AT) Awareness. Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism (JCS Pub 1-02, Reference (aj)).

E2.1.3. Antiterrorism (AT) Program. The AT program is one of several security-related programs that fall under the overarching Combating Terrorism and Force Protection programs. The AT program is a collective, proactive effort focused on the prevention and detection of terrorist attacks against DoD personnel, their families, facilities, installations, and infrastructure critical to mission accomplishment as well as the preparation to defend against and planning for the response to the consequences of terrorist incidents. Although not elements of AT, plans for terrorism consequence management preparedness and response measures as well as plans for continuing essential military operations are important adjuncts to an effective AT program. The minimum elements of an AT program are AT risk management, planning, training and exercises, resource generation, and a program review.

E2.1.3.1. AT risk management is the process of systematically identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk cost with mission benefits. The end products of the AT program risk management process shall be the identification of areas and assets 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, asset criticality assessment, and vulnerability assessment), the Commander must determine which assets require the most protection and where future expenditures are required to minimize risk of attack or lessen the severity of the outcome of an attack. The Commander must decide on how best to employ given resources and AT force protection measures to deter, mitigate, or prepare for a terrorist incident.

E2.1.3.2. AT planning is the process of developing specific guidance and execution-oriented instructions for subordinates.

E2.1.3.3. AT training is the development of individual, leader, and collective skills as well as conducting comprehensive exercises to validate plans for antiterrorism, incident response, consequence management, and continuity of essential military operations.

E2.1.3.4. AT resource generation is the process of identifying and submitting requirements through existing PPBES, CbT-RIF, and other funding mechanisms. Central to success of resource generation is tracking, and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

E2.1.3.5. Comprehensive AT program review is the systematic assessment of the AT program against standards prescribed by DoD Instruction 2000.16 (Reference (h)).

E2.1.4. Chief of Mission (COM)/Diplomatic Security Responsibility. A COM is responsible for protecting all official U.S. personnel and facilities, except those under the security responsibility of the Combatant Commander. The COM administers the security programs through the regional security officer (RSO) in accordance with DoS and OSPB policies and standards. Depending on the local conditions, the COM may also elect to implement security procedures, as deemed necessary, that exceed required levels set forth by the OSPB. When a Combatant Commander agrees to relinquish, and the COM accepts "security responsibility" for DoD Elements and Personnel pursuant to the DoD-DoS MOU (Reference (m)), all DoS, OSPB, and locally implemented RSO security policies apply to the DoD elements under the COM's security responsibility. The security programs typically covered by the RSO include, but not are limited to: physical, personal, procedural, and residential security; technical security including computer security and protection of sensitive national security information and equipment; and new arrival briefing programs on crime, terrorism, and counterintelligence. They also include the conduct of criminal and personnel investigations, operational supervision of Marine Security Guard and local National Guard programs, surveillance detection operations and liaison activities with senior host-country security and law enforcement officials, and an official relationship (Overseas Security Advisory Council (OSAC)) with private U.S. businesses located abroad to provide security advice, threat warning, and other information, including suspicious activity reports. The RSO is the Ambassador's law enforcement and security advisor and represents the U.S. Federal, State, and local law enforcement authorities not resident in the country. All RSOs and assistant RSOs are special agents of the Diplomatic Security Service.

E2.1.5. Combatant Command. Nontransferable command authority established by Section 164 of title 10, United States Code ("Armed Forces"), exercised only by the Commanders of Combatant Commands unless otherwise directed by the President or the Secretary of Defense. Combatant Command (command authority) cannot be delegated and is the authority of a Combatant Commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction of all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant Command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate Joint Force Commanders and Service and/or Functional Component Commanders. Combatant Command (command authority) provides full authority to organize and employ commands and forces as the Combatant Commander considers necessary to accomplish assigned missions. Operational control is inherent in Combatant Command (command authority) (Reference (aj)).

E2.1.6. Combating Terrorism (CbT). Combating terrorism within the Department of Defense encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of chemical, biological, radiological, nuclear materials, or high-yield explosive (CBRNE) devices.

E2.1.7. Consequence Management (CM). Those measures taken to protect public health and safety, restore essential Government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of a CBRNE situation. For domestic consequence management, the primary authority rests with the States to respond and the Federal Government through the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA), as the Lead Federal Agency (LFA), to provide assistance as required. The Department of State is the LFA for Foreign Consequence Management.

E2.1.8. Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (*Reference (aj)*).

E2.1.9. Counterterrorism (CT). Offensive measures taken to prevent (preempt), deter (disrupt), and respond to terrorism (*Reference (aj)*).

E2.1.10. Crisis Management. Measures to resolve a hostile situation and investigate and prepare a criminal case for prosecution under Federal law. Crisis Management shall include a response to an incident involving a weapon of mass destruction, special improvised explosive device, or a hostage crisis that is beyond the capability of the LFA (*Reference (aj)*).

E2.1.11. Critical Asset. Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and its timely restoration. Critical assets may be DoD assets or other Government or private assets, (e.g., industrial or infrastructure critical assets), domestic or foreign, the disruption or loss of which would render DoD critical assets ineffective or otherwise seriously disrupt DoD operations. Critical assets include traditional "physical" facilities and equipment, non-physical assets (such as software systems), or "assets" that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks) (*Reference (i)*).

E2.1.12. Critical Infrastructure. Infrastructure deemed essential to DoD operations or the functioning of a Critical Asset (*Reference (x)*).

E2.1.13. Criticality Assessment. Identifies key assets and infrastructure that support DoD missions, units, or activities and are deemed mission critical by military commanders or civilian agency managers. It addresses the impact of temporary or permanent loss of key assets or infrastructures to the installation or a unit's ability to perform its mission. It examines costs of recovery and reconstitution including time, dollars, capability, and infrastructure support.

E2.1.14. DoD Civilian Work Force. U.S. citizens or foreign nationals working for the Department of Defense and paid from appropriated or non-appropriated funds under permanent or temporary appointment. This includes employees filling full-time, part-time, intermittent, or on-call positions. Specifically excluded are all Government contractor employees.

E2.1.15. Defense Contractor. Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the Department of Defense to furnish services, supplies, or both, including construction. Thus, Defense contractors may include U.S. nationals, local citizens, or third country nationals. Defense contractors do not include foreign governments or representatives of foreign governments that are engaged in selling to the Department of Defense or a DoD Component, or foreign corporations wholly owned by foreign governments (*Reference (i)*).

E2.1.16. Domestic Terrorism. Terrorism perpetrated by the citizens 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 not the principal or intended target.

E2.1.17. Emergency (CbT-RIF Requirement). An unanticipated 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 (o)* for a detailed discussion of CbT-RIF request procedures.)

E2.1.18. Emergent (CbT-RIF Requirement). Newly formed, unexpected requirement resulting as a logical consequence of unforeseen circumstances and calling for prompt action. (See *Reference (o)* for a detailed discussion of CbT-RIF request procedures.)

E2.1.19. Family Member. Individuals defined as "Dependent" in Section 1072(2) of title 10 U.S.C. (*Reference (ak)*). Includes spouses; unmarried widows; unmarried widowers; unmarried legitimate children, including adopted children or stepchildren, who are under 21, incapable of self support; or under 23 and enrolled in a full-time institution of higher learning. Also, the family members of DoD civilian employees, particularly as it pertains to those assigned overseas. The DoD standard for family members requiring Level I AT awareness training is 14 years or older (or younger at discretion of the DoD sponsor, *Reference (h)*).

E2.1.20. Food and Water Security. The protection of food and water sources from disruption and contamination or other terrorist acts that could severely impact 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.

E2.1.21. Force Health Protection (FHP). All services performed, provided, or arranged by the Services to promote, improve, conserve, or restore the mental or physical well-being of personnel. These services include, but are not limited to, the management of health services resources, such as manpower, monies, and facilities; preventive and curative health measures; evacuation of the wounded, injured, or sick; selection of the medically fit and disposition of the medically unfit; blood management; medical supply, equipment, and maintenance thereof; combat stress control; and medical, dental, veterinary, laboratory, optometry, medical food, and medical intelligence services (Reference (aj)).

E2.1.22. Force Protection (FP). Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the Joint Force while degrading the opportunities of the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease (Reference (aj)).

E2.1.23. Force Protection Condition (FPCON). A DoD-approved system standardizing the Department's identification, recommended preventive actions, and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities. (See Reference (i) for a detailed description of the five progressive levels within the DoD FPCON System.)

E2.1.24. High-Risk Billet. Authorized personnel billet (identified and recommended by the appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make a person filling it an especially attractive or accessible terrorist target (Reference (h)).

E2.1.25. High-Risk Personnel. Personnel who, by their grade, assignment, symbolic value or relative isolation, are likely to be attractive or accessible terrorist targets (Reference (aj)).

E2.1.26. Intelligence

E2.1.26.1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

E2.1.26.2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding (Reference (aj)).

E2.1.27. Military Department. One of the Departments within the Department of Defense created by the National Security Act of 1947, as amended: the Department of the Army, the Department of the Navy, and the Department of the Air Force (Reference (aj)).

E2.1.28. Military Service. The Military Services are the United States Army, United States Navy, United States Air Force, United States Marine Corps, and the United States Coast Guard (when operating as a Military Service in the Navy) (*Reference (aj)*).

E2.1.29. "No Double Standard Policy"

E2.1.29.1. It is the policy of the U.S. Government that no double standard shall exist regarding the availability of terrorist threat information and that terrorist threat information be disseminated as widely as possible. Officials of the U.S. Government shall ensure that information that might equally apply to the public is readily available to the public. The Department of Homeland Security (DHS) is responsible for the release of information to the public in the 50 United States, its Territories, and Possessions. The Department of State (DoS) is responsible for release of terrorist threat information to the public in foreign countries and areas. Threats directed against or affecting the public (in the 50 United States, its Territories, and Possessions) or U.S. citizens abroad shall be coordinated with the DHS, the DoS, or the appropriate U.S. Embassy before release.

E2.1.29.2. Commanders may disseminate terrorist threat information immediately to DoD Elements and Personnel for threats directed solely against the Department of Defense. In foreign countries and areas, the threat information also shall be passed up the chain of command to the lowest level that has direct liaison with the DoS or the appropriate U.S. Embassy(ies) (or for non-Combatant Commander assigned forces, the U.S. Defense Representative (USDR)). Within the 50 United States, its Territories, and Possessions, the threat information shall be passed up the chain of command to the lowest level that has direct liaison with the DHS. Except when immediate notice is critical to the security of DoD Elements and Personnel, the appropriate DoS/U.S. Embassy(ies)/DHS should be informed 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 may immediately disseminate the information to, and implement appropriate AT protective measures for, DoD Elements and Personnel; and as soon as possible, inform the DoS/U.S. Embassies or the DHS, as appropriate, through the chain of command.

E2.1.29.3. Commanders also shall inform the DoS/U.S. Embassy(ies) or the DHS of any changes to FPCON Levels or the security posture that significantly affects the host nation/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 the DoS/U.S. Embassy(ies) (or for non-Combatant Command assigned forces, the USDR) or the DHS. Coordination and cooperation with the DoS/U.S. Embassy or the DHS in these cases is NOT a request for concurrence. Rather, it is informing the COM or Secretary of Homeland Security of the DoD response to a given terrorist threat. Although the COM or 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 in the chain of command. In areas outside the purview of

the DHS, the DoS is responsible to determine whether to release the threat information to U.S. citizens abroad and to deal with the sensitivities of the host nation(s). In the areas under the purview of the DHS, the Secretary of Homeland Security is responsible to determine whether to release the threat information to the U.S. public.

E2.1.30. Operational Control (OPCON). Transferable command authority that may be exercised by commanders at any echelon at or below the level of Combatant Command. Operational control is inherent in Combatant Command (command authority) and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control includes authoritative direction over force protection (*Reference (aj)*).

E2.1.31. Overseas Security Advisory Council (OSAC). The OSAC was established by the 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 OSAC as a forum to produce a series of publications providing guidance, suggestions, and planning techniques on a variety of security-related issues, including terrorism.

E2.1.32. Overseas Security Policy Board (OSPB). The OSPB is a National Security Council body established 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 U.S. Chief of Mission abroad. The DoS Director for Diplomatic Security chairs the OSPB.

E2.1.33. Physical Security. That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft (*Reference (aj)*).

E2.1.34. Protective Service Operations (PSO). Protective Service Operations entail the protection of dignitaries and other high-risk personnel in the Combatant Commander's AOR where significant threats exist. Those threats include assaults, kidnappings, assassinations, and attempts to embarrass the U.S. Government. This condition may result in the requirement to provide increased safety and security through the assignment of protective service details.

E2.1.35. Reserve Components (RC). The RC of the Armed Forces of the United States are those Reserve members, units, and full-time support personnel of the Army National Guard of the United States, the Army Reserve, the Naval Reserve, the Marine Corps Reserve, the Air National Guard of the United States, the Air Force Reserve, and during time of war when directed by the President, the Coast Guard Reserve. Within each RC, a Reserve member is placed in one of three Reserve categories: Ready Reserve, Standby Reserve, or Retired Reserve (*Reference (aj)*).

E2.1.36. Security

E2.1.36.1. Measures taken by a military unit, activity, or installation, to protect against all acts designed to, or that may, impair its effectiveness.

E2.1.36.2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences (*Reference (aj)*).

E2.1.37. Security Organizations. Military law enforcement, military criminal investigative organizations, and DoD-contracted security personnel.

E2.1.38. Service Component Command. A command consisting of the Service component command and all those Service forces, such as individuals, units, detachments, organizations, and installations under that command, including the support forces that have been assigned to a Combatant Command or further assigned to a subordinate unified command or joint task force (*Reference (aj)*).

E2.1.39. Tactical Control (TACON). Command authority over assigned or attached forces or commands or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task (*Reference (aj)*).

E2.1.40. TACON (for force protection). TACON (for force protection) enables the geographic Combatant Commander to order implementation of force protection measures (of which AT measures are integral) and to exercise the security responsibilities outlined in any respective MOA concluded under the December 1997 Department of State/Department of Defense MOU on the Security of DoD Elements and Personnel in Foreign Areas (known as the Universal MOU) (*Reference (m)*). Further, TACON (for force protection) authorizes the geographic Combatant Commander to change, modify, prescribe, and enforce force protection measures for covered forces. This relationship includes the authority to inspect and assess security requirements and direct DoD activities to identify the resources required to correct deficiencies and to submit budget requests to parent organizations to fund identified corrections. The geographic Combatant Commander can also direct immediate force protection measures (including temporary relocation and departure) when, in his judgment, such measures must be accomplished without delay to ensure the safety of the DoD Personnel involved. Persons subject to the geographic Combatant Commander's TACON (for force protection) authority include not only active duty and Reserve component personnel in the Commander's AOR, but also, all DoD civilian employees and all family members in the AOR.

E2.1.41. Terrorism. The calculated use of unlawful violence or threat of unlawful violence to inculcate fear and intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological (*Reference (aj)*).

E2.1.42. Terrorist Threat Level. An intelligence threat 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 threat levels: LOW, MODERATE, SIGNIFICANT, and HIGH. Threat levels should not be confused with Force Protection Conditions (FPCON). Threat-level assessments are provided to senior leaders to assist them determining the appropriate local FPCON.

E2.1.43. Threat Analysis. In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target the DoD Components or the DoD Elements and Personnel. A threat analysis shall review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as 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.

E2.1.44. Threat Assessment. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity (*Reference (h)*).

E2.1.45. U.S. Defense Representative (USDR). The USDR is the in-country representative of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Combatant Commander for coordination of security matters for all in-country noncombat DoD Elements and Personnel (those personnel and organizations not assigned to, or attached to, or under the command of a Combatant Commander). The USDR shall act as the Department of Defense's single point of contact for security issues relating to the Combatant Commander/COM MOU (*References (l) and (m)*).

E2.1.46. Vulnerability

E2.1.46.1. In antiterrorism, a situation or circumstance, if left unchanged and taken advantage of by terrorists, that may result in the loss of life or damage to mission-essential resources.

E2.1.46.2. 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.

E2.1.46.3. 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.

E2.1.46.4. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (*References (h) and (aj)*).

E2.1.47. Vulnerability Assessment. An evaluation (assessment) to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. Identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism (*Reference (aj)*). The process the commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, family members, and facilities, which provide a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks (*Reference (h)*).

E3. ENCLOSURE 3

ANTITERRORISM COORDINATING COMMITTEE (ATCC) AND SENIOR STEERING GROUP (ATCC-SSG)

E3.1. PURPOSE

E3.1.1. Enable expeditious resolution of AT issues affecting the Department of Defense.

E3.1.2. Serve as a forum for the exchange of AT information to assist OSD staff elements with their oversight roles.

E3.1.3. Act as a clearinghouse for policy recommendations to the Secretary of Defense concerning protection of DoD personnel and their family members, facilities, critical infrastructure, and other material resources from terrorist acts.

E3.1.4. Facilitate coordination of AT actions and taskings.

E3.1.5. Review AT reports to the Secretary of Defense on the status of AT activities undertaken in support of this Directive.

E3.2. LEADERSHIP

E3.2.1. The ASD(SO/LIC&IC) under the USD(P) shall:

E3.2.1.1. Co-chair the ATCC-SSG.

E3.2.1.2. Appoint the Deputy Assistant Secretary of Defense for Special Operations and Combating Terrorism (DASD(SO/CT)) to co-chair the ATCC.

E3.2.2. The Chairman of the Joint Chiefs of Staff shall:

E3.2.2.1. Appoint the Director for Operations, Joint Staff (J3) to co-chair the ATCC-SSG.

E3.2.2.2. Appoint the Deputy Director for ~~Global Operations~~ (Antiterrorism/~~Homeland Defense Force Protection~~), Joint Staff to co-chair the ATCC.

E3.3. MEMBERSHIP

E3.3.1. Membership in the ATCC-SSG shall consist of the following principals: the Secretaries of the Military Departments, the USD(AT&L), the USD(C), the USD(P&R), the DoD GC, the DoD IG, the USD(I), the PDUSD(P&R), the ASD(HA), the ASD(HD&ASA), the ASD(LA), the ASD(PA), the ASD(SO/LIC&IC), the Director, PA&E, the Joint Staff (J3), the Director of the DIA, the Director of the DSCA, the Director of the CIFA, and the Commandant, U.S. Marine Corps, or their senior representative.

E3.3.2. Membership in the ATCC shall consist of one representative from each office as identified by the ATCC-SSG principals listed in paragraph E3.3.1. above, and representatives from the Combatant Commands. Observers from other OSD offices may be authorized on an as required basis.

E3.4. SUBCOMMITTEES

E3.4.1. Subcommittees shall be chaired by the Office of Primary Responsibility for the particular AT activity being addressed and shall consist of representatives from those offices that have clear responsibilities with regard to that particular AT activity.

E3.4.2. Standing subcommittees are Intelligence; Doctrine and Training; Operations; Overseas Security; Requirements, Programs, and Budget; Technology; and Congressional Liaison. Other subcommittees may be established as needed.

All Federal Agencies are required to take all steps necessary to reduce vulnerabilities to terrorist attacks. The ATCC and ATCC-SSG were established to meet this requirement and to support the Secretary of Defense and the Chairman of the Joint Chiefs of Staff in fostering cooperation and coordination for AT activities within the Department of Defense and among the Department of Defense and other U.S. Government Agencies and organizations.

E4. ENCLOSURE 4

DEFENSE INTELLIGENCE AGENCY ANTITERRORISM (AT) RESPONSIBILITIES

E4.1.1. Establish and operate a Joint Intelligence Task Force for Combating Terrorism (DIA/JITF-CT) to direct collection, exploitation, analysis, fusion, and dissemination of all-source intelligence in support of DoD combating terrorism operations, planning, and policy, including DoD AT requirements. The JITF-CT serves as the single national-level, all-source foreign terrorism intelligence effort within the Department of Defense. The JITF-CT is designated to serve as the central repository of all foreign terrorism-related intelligence for the Department of Defense. Military Department Secretaries and Service Chiefs shall conduct terrorism intelligence activities as a component of or in consonance with the JITF-CT.

E4.1.2. DIA/JITF-CT shall provide prompt dissemination of intelligence on foreign terrorist threats, including specific warning of threats against DoD Personnel (including family members), facilities, and other DoD material resources to comply with DoD Directive 5240.1 and DoD 5240.1-R (*References (aa) and (ab)*). Warnings to DoD Personnel (including family members) shall be in accordance with the "No Double Standard" policy as defined in *Enclosure 2*. The DIA/JITF-CT is the focal point within the Department of Defense for the analysis of data and information pertaining to domestic and foreign terrorist threats to DoD Personnel (excluding threats posed by U.S. persons who have no discernable foreign control or connections).

E4.1.3. Operate a 24-hour terrorism intelligence Warning and Fusion Center within the JITF-CT; ensure terrorist threat intelligence is disseminated to the appropriate DoD Components.

E4.1.4. Send a representative to the Interagency Committee on Terrorism, and provide the DoD input to the national intelligence foreign terrorism warning process.

E4.1.5. Maintain a foreign terrorism database, which includes information on foreign terrorist groups, capabilities, facilities, incidents, biographies, and foreign counterterrorism policies and response capabilities.

E4.1.6. Subject to the provisions of *References (aa) and (ab)*, assess the foreign terrorist threat worldwide, ensure dissemination to the DoD Components, and produce daily foreign terrorist threat awareness reports.

E4.1.7. Provide a member to the DoD Antiterrorism Coordinating Committee (ATCC) and subcommittees, as required under *Enclosure 3*.

E4.1.8. Function as the DoD Executive Agency for diplomatic security matters, pursuant to DoD Instruction 5210.84 (*Reference (1)*). Establish, manage, and operate a DoD diplomatic security element that shall:

E4.1.8.1. Ensure the Department of Defense's compliance with the Overseas Security Policy Board (OSPB) and DoS security standards.

E4.1.8.2. Ensure that deficiencies and equities in the diplomatic security support received from the COMs are addressed.

E4.1.8.3. Ensure DoD representation at the National Security Council's OSPB and other committees, subcommittees, and working groups, where appropriate pursuant to this Directive and *References* (h), (i), and (k) through (n)).

E4.1.9. Provide the senior DIA voting member to the OSPB and provide the alternate DoD senior-voting member to the OSPB.

E4.1.10. Provide and conduct security assistance visits and vulnerability assessments for all DIA elements, as well as other defense component offices under the security responsibility of the Chiefs of Mission (COMs) on a routine and emergency basis (*References* (h), (l) through (n), DoD Directive 3025.15, DoD Directive 5105.47, and DoD Instruction 5105.57 (*References* (al) through (an))). Provide completed vulnerability assessments or security assistance visit reports to the ASD(SO/LIC&IC), the geographic Combatant Commanders, the Director of the CIFA, the DoD Inspector General, the DoS Inspector General, the Unified Commands' Inspector Generals, the DoS Diplomatic Security Services, the U.S. Defense Representatives (USDRs), and the respective COMs. Provide semi-annual updates to the Combatant Commanders and the ASD(SO/LIC&IC) on trend items and lessons learned.

E4.1.11. Maintain a centralized database of all vulnerability assessments conducted concerning DoD Elements under COM security responsibility.

E4.1.12. In coordination with the cognizant Combatant Commander and DoS personnel, ensure that the appropriate reference is used to plan and execute AT for all DoD activities under the security responsibility of the COMs.

E4.1.13. Ensure DIA personnel are aware of DoD travel security policy and required actions for travelers enroute to, or through, DoD-designated high potential physical threat countries.

E4.1.14. Ensure DIA personnel assigned to high-risk billets and to others, as recommended by appropriate authority to the Military Departments, receive appropriate AT training.

E4.1.15. Provide the Combatant Commanders with tailored analytical products, studies, and analyses pertaining to foreign terrorist threats to the DoD Components, Elements and Personnel.

E4.1.16. Set DoD terrorist threat levels by country worldwide. Terrorism threat levels shall be established as the result of all-source analysis and incorporation of Combatant Command and Military Department input.

E4.1.17. Attend Counterterrorism Security Group (CSG) meetings pertaining to terrorism, in conjunction with the ASD(SO/LIC&IC) and the Joint Staff (J3).

E4.1.18. Provide Protective Service Operations (PSOs) for DIA personnel assigned to high-risk billets and to others as recommended by appropriate DoD and DIA counterintelligence and security authority.

E5. ENCLOSURE 5

NATIONAL SECURITY AGENCY ANTITERRORISM (AT) RESPONSIBILITIES

E5.1.1. Disseminate, on a timely basis to the intelligence community and the Department of Defense, signals intelligence (SIGINT) reports on foreign terrorist threat against U.S. interests globally. Ensure compliance with the "No Double Standard" policy. (See definition E2.1.29., *Enclosure 2.*)

E5.1.2. Operate a 24-hour foreign terrorism desk within the National Security Operations Center. This desk shall provide cryptologic support to combat terrorism.

E5.1.3. Maintain a foreign terrorism communication profile database, which shall include foreign terrorist group communications systems and foreign terrorist group profiles based on SIGINT.

E5.1.4. Produce and coordinate SIGINT-based foreign terrorist threat warnings.

E5.1.5. Through the Signals Intelligence Directorate, Counter Terrorism Product Line, serve as the focal point for coordination of foreign terrorist issues with the Intelligence Community, the Department of Defense, and Law Enforcement elements.

E5.1.6. Provide AT SIGINT support to major U.S. deployments, as required.

E5.1.7. Provide a representative to the Overseas Security Policy Board (OSPB).

E5.1.8. Provide defensive travel briefings, when appropriate, to affiliates who have been approved for foreign travel.

E6. ENCLOSURE 6

DEPARTMENT OF DEFENSE COUNTERINTELLIGENCE FIELD ACTIVITY
ANTITERRORISM RESPONSIBILITIES

E6.1.1. Establish a threat analysis capability designed to collect, fuse and analyze domestic law enforcement information with foreign intelligence and counterintelligence information in support of the DoD CbT mission. As a designated DoD law enforcement and counterintelligence activity, CIFA shall support the efforts of the JITF-CT, serving as the bridge between intelligence related to international terrorism and domestic law enforcement information.

E6.1.2. Maintain a domestic law enforcement database that includes information related to potential terrorist threats directed against the Department of Defense.

E6.1.3. Support the JITF-CT, the Combatant Commands, and the Military Services in preparing threat assessments and advisories.

E6.1.4. Conduct specific risk assessments in support of the *Defense* Critical Infrastructure Protection Program. Identify and maintain a database of critical DoD assets and infrastructure. This database shall include vulnerability assessments of all DoD facilities.

E6.1.5. Support DoD counterintelligence components in preparing threat assessments by providing tailored analytical and data-mining services.

E6.1.6. Establish and manage DoD Force Protection Detachments at high-threat in-transit locations overseas, ensuring required counterintelligence and force protection support is provided to DoD Elements transiting these locations.

E6.1.7. Assign DoD counterintelligence and criminal investigative personnel to the National Joint Terrorism Task Force and designated Joint Terrorism Task Forces within CONUS. Provide program oversight and coordination for assigned counterintelligence assets and serve as the repository for information obtained.

E6.1.8. Provide countersurveillance support to the Combatant Commands upon request, subject to the approval of the Chairman of the Joint Chiefs of Staff.

E6.1.9. Provide a member to the DoD ATCC and subcommittees as required pursuant to *Enclosure 3* of this Directive.

E6.1.10. Assist the DIA in the execution of its diplomatic security function. Such assistance shall include:

E6.1.10.1. Representation at the National Security Council's Overseas Security Policy Board and other related committees, subcommittees, and working groups.

E6.1.10.2. Support the DIA security assistance visits and vulnerability assessments for all DoD Elements under the security responsibility of the COMs.