



Department of Defense INSTRUCTION

NUMBER 2000.16
October 2, 2006

USD(P)

SUBJECT: DoD Antiterrorism (AT) Standards

- References:
- (a) DoD Instruction 2000.16, "DoD Antiterrorism Standards," June 14, 2001 (hereby canceled)
 - (b) DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003
 - (c) DoD Instruction 2000.14, "DoD Combating Terrorism Program Procedures," June 15, 1994 (hereby canceled)
 - (d) DoD Instruction 2000.18, "DoD Installation Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Emergency Response Guidelines," December 4, 2002
 - (e) through (ag), see Enclosure 1

1. REISSUANCE AND PURPOSE

This Instruction:

1.1. Reissues Reference (a) to update policy implementation, responsibilities, and the antiterrorism (AT) standards for the DoD Components under the authority of Reference (b) for the protection of DoD elements and personnel from acts of terrorism. This update reorganizes the AT standards listed in Enclosure 3 according to the minimum required elements for an AT program: risk management, planning, training and exercises, resource application, and comprehensive program review. It also cancels Reference (c).

1.2. Expands protection of DoD installations to recognize the importance of defending against terrorist use of chemical, biological, radiological, nuclear and high explosive (CBRNE) weapons according to Reference (d).

1.3. Expands requirements to DoD Instruction 5200.08 and DoD 5200.8-R (References (e) and (f)) to address the linkages between AT and Physical Security Programs.

2. APPLICABILITY AND SCOPE

2.1. This Instruction 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 “commander(s),” as used herein, refers to personnel assigned to command positions at all levels and their civilian equivalents.

2.2. The standards prescribed in this Instruction apply only to the DoD AT Program.

3. DEFINITIONS

The terms used in this Instruction are defined in Joint Publication 1-02 (Reference (g)) or Enclosure 2.

4. POLICY

Under Reference (b), it is DoD policy:

4.1. To protect DoD personnel, their families, installations, facilities, information, and other material resources from terrorist acts.

4.2. To establish AT standards for the Department of Defense. The primary AT standards are contained in this Instruction and supplemented by guidance contained in References (e) and (f), and DoD O-2000.12-H (Reference (h)).

4.3. That commanders at all levels shall have the authority to enforce security measures and are responsible for protecting persons and property subject to their control.

4.4. That Geographic Combatant Commander AT policies and programs shall 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) pursuant to the Memorandums of Understanding (References (i) and (j)).

4.5. That the DoD elements and personnel not falling under the AT policies and programs of a geographic Combatant Commander, by law or under Reference (i), shall comply with the Overseas Security Policy Board Security Standards.

4.6. That non-DoD tenants on a DoD installation, facility, or other DoD property must comply with all aspects of the DoD AT program addressed in this Instruction and other AT guidance documents.

4.7. That functional Combatant Commanders will support geographic Combatant Commanders as they exercise overall AT responsibility within their AOR.

5. RESPONSIBILITIES

Under the authority in Reference (b):

5.1. The Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, under the Under Secretary of Defense for Policy, shall:

5.1.1. In coordination with the Under Secretary of Defense for Intelligence, the Assistant Secretary of Defense for Homeland Defense and the Assistant to the Secretary of Defense for Nuclear and Chemical and Biological Defense Programs, provide AT policy oversight and monitor compliance with this Instruction by the DoD Components, both within and outside the United States.

5.1.2. Develop, publish, and maintain this Instruction to provide standards for protective measures that serve to reduce the vulnerability of DoD personnel, their families, installations, facilities, information, and other material resources to terrorist acts. AT protective measures are an extension of the existing DoD Physical Security Program requirements.

5.1.3. Be the point of contact for the Department of Defense with the Department of State for the standards contained in this Instruction and be responsible at the departmental level for resolving any conflicts with the Department of State between the DoD Components and any United States Country Team with respect to such standards.

5.2. The Heads of the DoD Components shall:

5.2.1. Establish clear AT policies for all DoD elements and personnel that support the geographic Combatant Commanders as they exercise overall responsibility for AT within their AOR.

5.2.2. Develop and implement comprehensive AT programs pursuant to the requirements and standards established by this Instruction and References (b) and (i), and DoD O-2000.12-P (Reference (k)) and be responsible for the implementation of and compliance with DoD AT policies within their organizations.

5.2.3. Use the standards prescribed in this Instruction as baseline standards. The DoD Components may promulgate unique requirements to supplement the standards contained herein.

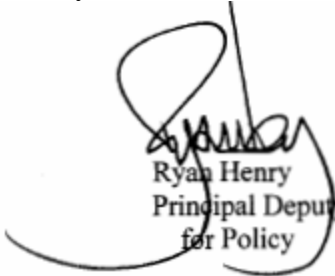
5.2.4. Identify the level of command (e.g., the specific subordinate commanders) responsible for meeting the standards prescribed in this Instruction.

6. INFORMATION REQUIREMENTS

The review, assessment, and reporting of AT programs is exempt from licensing in accordance with paragraphs C4.4.1., C4.4.2., C4.4.7., and C4.4.8. of DoD 8910.1-M (Reference (1)).

7. EFFECTIVE DATE

This Instruction is effective immediately.



Ryan Henry
Principal Deputy Under Secretary of Defense
for Policy

Enclosures – 4

- E1. References, continued
- E2. Definitions
- E3. DoD Antiterrorism (AT) Standards
- E4. DoD FPCON

E1. ENCLOSURE 1

REFERENCES, continued

- (e) DoD Instruction 5200.08, "Security of DoD Installations and Resources," December 10, 2005
- (f) DoD 5200.8-R, "Physical Security Program," May 1991
- (g) Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms", 12 April 2001
- (h) DoD O-2000.12-H, "DoD Antiterrorism Handbook,"¹ February 9, 2004
- (i) Memorandum of Understanding Between DOS and DoD on Security of DoD Elements and Personnel in Foreign Areas, December 16, 1997
- (j) Memorandum of Understanding between the Department of State and the Department of Defense on Security on the Arabian Peninsula, September 16, 1996,
- (k) DoD O-2000.12-P, "DoD Antiterrorism Strategic Plan," June 15, 2004
- (l) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," June 30, 1998
- (m) Section 1072(2) of title 10, United States Code
- (n) DoDI 5240.10, "Counterintelligence Support to the Combatant Commands and The Defense Agencies," May 14, 2004
- (o) DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense," January 7, 1980
- (p) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982
- (q) Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "DoD Policy on Drinking Water Vulnerability Assessments and Emergency Response Plans," July 3, 2003
- (r) Defense Threat Reduction Agency JSIVA Security Classification Guide,¹ February 2001
- (s) Joint Requirements Oversight Council Memo, JROCM 180- 3, "Chemical, Biological, Radiological, and Nuclear (CBRN) Defense Baseline Capabilities Assessment,"² September 11, 2003.
- (t) Unified Facilities Criteria (UFC) 4-010-01, "DoD Minimum Antiterrorism Standards for Buildings,"¹ October 8, 2003
- (u) DoD Directive C-4500.51, "DoD Non-Tactical Armored Vehicle Policy,"¹ May 4, 1987
- (v) Unified Facilities Criteria 4-010-02, "DoD Minimum Antiterrorism Standoff Distances for Buildings,"¹ October 8, 2003
- (w) Unified Facilities Criteria 4-021-01, "Design and O&M: Mass Notification Systems¹," December 18, 2002
- (x) Defense Federal Acquisition Regulation Supplement (DFARS)
- (y) DoD Directive 6490.2, "Comprehensive Medical Surveillance," October 21, 2004
- (z) CJCS Instruction 3121.01B, Standing Rules of Engagement / Standing Rules For the Use of Force For US Forces³, June 13, 2005

¹ A copy of this document is available via Secure Internet Protocol Router Network at www.atep.smil.mil

² The JROCM 180-3 is available via Secure Internet Protocol Router Network at <http://j8.js.smil.mil>

³ The CJCSI 3121.01B is available via Secure Internet Protocol Router Network at <http://js.smil.mil>.

- (aa) DoD Directive 5210.56, "Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties," November 1, 2001
- (ab) CJCS Instruction 3150.25B, "Joint Lessons Learned Program, February 15, 2005⁴
- (ac) CJCS Guide 5260, "Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism", October 14, 2005⁴
- (ad) CJCS Pocket Card 5260, "Antiterrorism Individual Protective Measures", October 1, 2001⁴
- (ae) DoD 4500.54-G, "DoD Foreign Clearance Guide (FCG)⁵," current edition
- (af) CJCS Instruction 5261.01D, "Combating Terrorism Readiness Initiatives Fund", December 16, 2005
- (ag) Defense Threat Reduction Agency (DTRA) Antiterrorism Vulnerability Assessment Team Guidelines,⁶ March 1, 2002

⁴ Unclassified CJCS Instructions, Guides, and Pocket Cards are available at www.dtic.mil/cjcs_directives/index.htm

⁵ The FCG is available via <http://www.fcg.pentagon.smil.mil>

⁶ The DTRA Vulnerability Assessment Team Guidelines are available at www.dtra.mil

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Antiterrorism (AT). See Joint Publication 1-02 (Reference (g)).

E2.2. AT Awareness. Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorism.

E2.3. 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 application, and a program review.

E2.3.1. AT Risk Management. The process of systematically identifying, assessing, and managing risks arising from operational factors and making decisions that balance risk cost with mission benefits. The end products of the AT 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, 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 shall decide on how best to employ given resources and FP measures to deter, mitigate, and prepare for a terrorist incident.

E2.3.2. AT Planning. The process of developing specific guidance and execution-oriented instructions for subordinates. An AT Plan contains command-specific guidance for the establishment of an AT program and the implementation of the AT standards prescribed by this Instruction.

E2.3.3. AT Training and Exercises. The development of individual, leader, and collective skills, and the conduct of comprehensive exercises to validate plans for AT, incident response, terrorism consequence management, and continuity of essential military operations.

E2.3.4. AT Resource Application. The process of applying risk management to vulnerabilities, and where the resultant risk is not acceptable after applying mitigation measures, elevate the vulnerability with a resource request using the existing Planning, Programming, Budgeting, and Execution (PPBE) system, the Combating Terrorism Readiness Initiative Fund (CbT-RIF), the Physical Security Program, and other funding mechanisms. Central to success in

resource application is tracking and ensuring sufficient funding for identified AT program life-cycle costs and assessed shortfalls to mitigate risk associated with terrorist capabilities.

E2.3.5. Comprehensive AT Program Review. The systematic assessment of the AT program against the standards prescribed by this Instruction.

E2.4. Antiterrorism Officer (ATO). The principal military or civilian advisor charged with managing the AT Program for the commander or DoD civilian exercising equivalent authority.

E2.5. Combating Terrorism (CbT). For the purpose of this Instruction, CbT within the Department of Defense encompasses all actions, including AT (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event), and terrorism intelligence support (collection and dissemination of terrorism-related information) taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of CBRNE.

E2.6. Counterterrorism. See Reference (g).

E2.7. Criminal Intelligence (CRIMINT). Law enforcement information derived from the analysis of information collected through investigations, forensics, crime scene and evidentiary processes to establish intent, history, capability, vulnerability, and modus operandi of threat and criminal elements.

E2.8. Criticality Assessment. A criticality assessment addresses the effect of temporary or permanent loss of key assets or infrastructures on the installation or a unit's ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability, and infrastructure support.

E2.9. Defense Critical Asset. An asset of such extraordinary importance to DoD operations in peace, crisis, and war that its incapacitation or destruction would have a very serious, debilitating effect on the ability of the Department of Defense to fulfill its mission.

E2.10. DoD 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. 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.

E2.11. DoD Elements and Personnel. 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.

E2.12. DoD Personnel. Uniformed Military Service members and DoD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.

E2.13. Emergency Responders. Firefighters, law enforcement, security personnel, emergency medical technicians, emergency management and operations personnel, Explosive Ordnance Disposal personnel, physicians, nurses, medical treatment providers at medical treatment facilities, disaster preparedness officers, public health officers, bio-environmental engineers, and mortuary affairs personnel.

E2.14. Family Member. Individuals defined as “Dependent” in Section 1072(2) of Title 10 U.S.C. (Reference (m)). 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 the discretion of the DoD sponsor).

E2.15. Force Protection. See Reference (g).

E2.16. Force Protection Condition (FPCON). A DoD-approved system standardizing DoD’s identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates coordination among DoD Components and support for antiterrorism activities.

E2.17. Force Protection Detachment (FPD). A Counterintelligence (CI) element that provides comprehensive CI support to transiting ships/personnel/aircraft in regions of elevated threat.

E2.18. High-Risk Billet (HRB). Authorized personnel billet (identified and recommended by appropriate authority) that because of grade, assignment, travel itinerary, or symbolic value may make personnel filling them an especially attractive or accessible terrorist target.

E2.19. High-Risk Personnel (HRP). Personnel who, by their grade, assignment, symbolic value, or relative isolation are likely to be attractive or accessible terrorist targets.

E2.20. Higher Headquarters Assessment (HHA). An overall assessment by a higher headquarters of how an organization is managing its AT program, to include management and compliance effort by subordinate organizations.

E2.21. Joint Staff Integrated Vulnerability Assessment (JSIVA). A JSIVA is a “vulnerability-based” evaluation of an installation's ability to deter and/or respond to a terrorist incident. A “vulnerability-based” assessment considers both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, both in terms of their mobility and the types of weapons historically employed.

E2.22. Overseas Security Policy Board (OSPB). The OSPB was 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 COM abroad. The Department of State Director for Diplomatic Security chaired the OSPB. National Security Presidential Directive (NSPD) 1, February 13, 2001, disestablished the OSPB and assigned the duties to various Policy Coordination Committees. However, the OSPB continues in its charter and is a sub-group of the Records and Access Information Security Policy Committee of the National Security Council. The Secretary of State has designated the Assistant Secretary, Bureau of Diplomatic Security, to chair the OSPB.

E2.23. 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.

E2.24. Security

E2.24.1. Measures taken by a military unit, activity, or installation, to protect against all acts designed to, or that may, impair its effectiveness.

E2.24.2. A condition that results from establishing and maintaining protective measures that ensure a state of inviolability from hostile acts or influences.

E2.25. Special Event. An activity characterized by a large concentration of personnel and/or a gathering where distinguished visitors are involved, often associated with a unique or symbolic event.

E2.26. Terrorism. See Reference (g).

E2.27. Terrorism Consequence Management. DoD preparedness and response for mitigating the consequences of a terrorist incident including the terrorist use of a Weapon of Mass Destruction (WMD). DoD consequence management activities are designed to support the Lead Federal Agency (domestically, Department of Homeland Security; overseas, Department of State) and include measures to alleviate damage, loss of life, hardship or suffering caused by the incident; protect public health and safety; and restore emergency essential government services.

E2.28. Terrorism Incident Response Measures. A set of procedures established for response forces to deal with the effects of a terrorist incident.

E2.29. Terrorism Threat Assessment

E2.29.1. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat.

E2.29.2. The product of a threat analysis for a particular unit, installation, or activity.

E2.30. Terrorism Threat Level. See Reference (g).

E2.31. Terrorism Vulnerability Assessment

E2.31.1. An assessment to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. It identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism.

E2.31.2. 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 AT measures that can protect personnel and assets from terrorist attacks.

E2.31.3 A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities.

E2.32. Vulnerability

E2.32.1. In AT, a situation or circumstance, which if left unchanged, may result in the loss of life or damage to mission essential resources.

E2.32.2. The susceptibility of a nation or military force to any action by any means through which its war fighting potential or combat effectiveness may be reduced or will to fight diminished.

E2.32.3. 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.

E.2.32.4. The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

E2.33. Weapons of Mass Destruction (WMD). See Reference (g).

E3. ENCLOSURE 3

DoD ANTITERRORISM (AT) STANDARDS

E3.1. DoD STANDARD 1: AT Program Elements. The minimum required elements of a DoD Component AT program shall be: risk management (STANDARD 3); planning (including the AT Plan) (STANDARD 7); training and exercises (STANDARD 23); resource application (STANDARD 30); and comprehensive program review (STANDARD 31). The development and maintenance of the AT program elements should be ongoing and continuously refined to ensure the relevance and viability of all defensive measures employed to reduce vulnerabilities to terrorist capabilities.

E3.2. DoD STANDARD 2: Intelligence Support to the DoD AT Program

E3.2.1. The Director, Defense Intelligence Agency (DIA), sets the DoD Terrorism Threat Level identifying the potential threat to DoD interests in a particular country, including the United States. The Director, DIA, shall coordinate, if necessary, with the Department of State to minimize conflicting classification of threat levels for the affected country. The DoD Terrorism Threat Level applies whether or not U.S. personnel are present in the country. The Geographic Combatant Commanders may also set Terrorism Threat Levels for specific personnel, family members, units, installations, or geographic regions in countries within the Geographic Combatant Commander's AOR, using the definitions and criteria established by the Director, DIA.

E3.2.2. The Heads of the DoD Components shall:

E3.2.2.1. Task the appropriate officials under their command or control to gather, analyze, and circulate appropriate terrorism threat information. When local information indicates gaps, commanders shall forward timely requests for information via appropriate intelligence collection and production channels.

E3.2.2.2. Develop Priority Intelligence Requirements (PIR) and Commander's Critical Information Requirements (CCIR) to focus collection and analysis efforts.

E3.2.2.3. Provide units in transit with tailored terrorist threat information.

E3.2.2.4. Integrate countersurveillance, surveillance detection, CI, and other specialized skills as a matter of routine in all AT programs.

E3.2.2.5. Identify an official as the focal point for the integration of operations and local or host-nation intelligence, CI, and CRIMINT information.

E3.2.2.6. Incorporate proactive techniques to detect and deter terrorists, particularly in support of assets or activities conducted in areas designated with SIGNIFICANT or HIGH threat levels. These activities shall include, but are not limited to: in-transit forces, HRP, special events, and high-value military cargo shipments.

E3.2.2.7. Ensure counterintelligence support for those DoD Components without organic counterintelligence capability within provisions of DoDD 5240.10 (Reference (n)).

E3.2.2.8. Ensure that commanders at all levels forward up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism involving DoD elements and personnel or assets for which they have responsibility, including the provision of such information to appropriate interagency officials.

E3.2.3. The Secretaries of the Military Departments shall ensure that military personnel are trained to maximize the use of information derived from law enforcement liaison, and from intelligence and CI processes and procedures. This includes intelligence procedures for handling PIR for in-transit units and implementation of procedures to conduct intelligence preparation of the battlespace and mission analysis.

E3.2.4. DoD intelligence, CI, and law enforcement elements shall disseminate information on U.S. persons to DoD Components as appropriate in support of AT program implementation within the provisions of DoD Directive 5200.27 (Reference (o)) and DoD 5240.1-R (Reference (p)).

E3.3. DoD STANDARD 3: AT Risk Management

E3.3.1. The Heads of the DoD Components shall establish an AT Risk Management process modeled upon the principles outlined in Reference (h) and applied in all aspects of AT program implementation and planning, including operational plans and decisions, development of risk mitigation measures, and the prioritization and allocation of resources. The essential components of AT Risk Management include: assessing the terrorist threat (threat assessment) determining the criticality of assets (criticality assessment); identifying the vulnerabilities of facilities, programs, and systems to terrorist attack; including the use of CBRNE or similar capabilities (vulnerability assessment), risk assessment, and outlining DoD Component capabilities to deter terrorist incidents, employ countermeasures, and mitigate and recover from the effects of a terrorist incident.

E3.3.2. The DoD Component AT Risk Management process and procedures shall be reviewed at least annually. An AT Program Review, an HHA, or a JSIVA visit satisfies the annual requirement.

E3.4. DoD STANDARD 4: Terrorism Threat Assessment. The Heads of the DoD Components shall:

E3.4.1. Establish a Terrorism Threat Assessment process consistent with the principles outlined in Reference (h) to identify the full range of known or estimated terrorist threat capabilities (including the use or threat of use of CBRNE and WMD) for those DoD Elements and Personnel that have AT responsibilities. These assessments shall be updated on an annual basis or more frequently as the terrorist threat environment dictates. Assessments shall be tailored to local conditions and address terrorist group's operational capability, intentions, and activity, and whether the operational environment is conducive to terrorist activity.

E3.4.2. Prepare specific Terrorism Threat Assessments to support operational planning and risk decisions for unique mission requirements or special events including, but not limited to, in-transit forces, training and exercises, operational deployments, and special events.

E3.4.3. Implement effective processes to integrate and fuse all sources of available threat information from local, State, Federal, host-nation law enforcement agencies; the appropriate local, State, Federal, and host-nation Intelligence Community (IC) activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a continuous analysis of threat information to support the Threat Warning process.

E.3.4.4. Terrorism Threat Assessments shall be integrated into the risk management process and be a major source of analysis and justification for recommendations to raise or lower FPCON levels, implementation of Random AT Measures (RAM), AT enhancements including Physical Security Program changes, program and budget requests, and used when conducting terrorism vulnerability assessments.

E3.5. DoD STANDARD 5: Criticality Assessment. The Heads of the DoD Components shall:

E3.5.1. Establish a Criticality Assessment process consistent with the principles outlined in Reference (h) and consistent with DoD STANDARD 3 to identify, classify, and prioritize mission-essential assets, resources, and personnel critical to DoD mission success. Criticality Assessments shall also be conducted for non-mission essential assets such as high-population facilities, mass gathering activities, and any other facility, equipment, service, or resource deemed important by the commander warranting protective measures to ensure continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration.

E3.5.2. Update Criticality Assessments at least annually to determine the degree of asset criticality based upon the following factors: relative importance, effect of loss, recoverability, mission functionality, substitutability, and reparability. Criticality Assessments, consistent with E.3.1.3, shall provide the basis for identifying those assets that require specific protective measures and priorities for resource allocation when developing and updating the AT Plan.

E3.6. DoD STANDARD 6: Terrorism Vulnerability Assessment

E3.6.1. The Heads of the DoD Components shall:

E3.6.1.1. Establish a Terrorism Vulnerability Assessment process consistent with the principles outlined in References (h) and the DoD Drinking Water Policy (Reference (q)) to provide a vulnerability-based analysis of mission-essential assets, resources, and personnel critical to mission success that are susceptible to terrorist attack.

E3.6.1.2. Within 90 days of a completed assessment, prioritize identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report to the first general officer, flag officer, or civilian equivalent director in the chain of command the results of the assessment.

E3.6.1.3. Ensure that the DoD vulnerability database (the Core Vulnerability Assessment Management Program (CVAMP)) is populated with all assessment results within 120 days from completion of the assessment.

E3.6.1.4. Conduct and update Terrorism Vulnerability Assessments at least annually or more frequently if the terrorist threat assessment or mission requirements dictate. Terrorism Vulnerability Assessments shall be conducted at a minimum for, but not limited to:

E3.6.1.4.1. Any facility populated daily by 300 or more DoD personnel.

E3.6.1.4.2. Any DoD facility bearing responsibility for emergency response or physical security plans and programs, or determined to host critical infrastructure.

E3.6.1.4.3. Any DoD facility or activity possessing authority to interact with local non-military or host-nation agencies or having agreements with other agencies or host-nation agencies to procure these services.

E3.6.1.4.4. Sea and air ports of embarkation and debarkation; movement routes (sea, air, ground, and rail); and assembly, staging, reception, and final beddown locations in support of any battalion, squadron, ship, or equivalent operational deployment; similar sized in-transit movement or training exercise; and any movement or shipment of military cargo (including Military Sealift Command voyage charters).

E3.6.1.4.5. Any personnel designated as HRP. These assessments are referred to as Personal Security Vulnerability Assessments (PSVA). PSVA will conform to Defense Criminal Investigative Office formats.

E3.6.1.4.6. Any event or activity determined to be a special event or other activity involving a gathering of 300 or more DoD personnel.

E3.6.1.4.7. Off-installation housing, schools, daycare centers, transportation systems, and routes used by DoD personnel and their dependent family members when the Terrorism

Threat Level is SIGNIFICANT or higher consistent with DoD STANDARD 3.

E3.6.1.5. Classify information derived from vulnerability assessments pursuant to the requirements outlined in the Defense Threat Reduction Agency JSIVA Security Classification Guide (Reference (r)).

E3.6.2. Geographic Combatant Commanders will:

E3.6.2.1. Establish the frequency for assessments, which should be conducted at least annually for those locations considered critical to strategic projection. The frequency of assessments and who conducts them is listed in Table E3.T1.

E3.6.2.2. Prescribe policies for no-notice or short-notice movements to locations where a Vulnerability Assessment has not been accomplished or is not current. Predeployment vulnerability assessments should assist commanders in updating AOR-specific training (see DoD STANDARD 29) and in obtaining necessary physical security materials and equipment to implement protective measures.

Table E3.T1

Type of Assessment	Conducted by	Frequency
PSVA	Defense Criminal Investigative Office (or others as designated)	Conduct per DoDI 2000.16 STANDARD 16; validate at least annually; conduct triennially
VA of critical Roads, bridges, sea and air ports, and staging/bed down areas	DoD Component	Per GCC guidance See DoDI 2000.16 STANDARD 6
VA of DoD Day Care, schools, & routes	DoD Component	At Threat Level: Significant
VA of Installations and facilities With 300 personnel, or Responsible for emergency response/critical infrastructure	DoD Component (local), Higher Headquarters, Service, Geographic Combatant Command, or JSIVA	At least annually Per DoDI 2000.16 STANDARD 6
Program Review	DoD Component (local) or as HHA Per E3.1.31.2	At least annually and in predeployment
External Higher Headquarters Assessment (HHA)/ Program Review	Higher Headquarters, Geographic Combatant Command, JSIVA Per E3.1.31.5	Triennially
CJCS led HHA	CJCS Per E3.1.31.6	Triennially

E3.7. DoD STANDARD 7: AT Plan

E3.7.1. The Heads of the DoD Components shall:

E3.7.1.1. Develop and maintain a comprehensive AT Plan for all DoD Elements and Personnel that have AT responsibility. Use of the Joint Antiterrorism (JAT) Guide, the only OSD and Joint Staff approved AT software planning tool, when used in its entirety, satisfies all minimum planning elements prescribed in this document. An AT Plan will not be considered complete unless signed and exercised.

E3.7.1.2. Incorporate AT principles into all operational plans and risk decisions using the standards prescribed by this Instruction as a baseline to develop and implement AT policies in support of the DoD Components' unique roles and mission requirements. At a minimum, AT plans shall be developed at the installation, separate or leased facility/space, and ship levels, and also for operational deployments, training exercises, and special events.

E3.7.1.3. Tailor AT plans to the level of command or activity for which the AT principles were developed. At a minimum AT plans shall address:

E3.7.1.3.1. The minimum essential AT program elements (see STANDARD 1) and standards prescribed by this Instruction.

E3.7.1.3.2. Specific threat risk mitigation measures to establish a local baseline defensive posture. The local baseline defensive posture shall facilitate systematic movement to and from elevated security postures, including the application of Random Antiterrorism Measures (RAM).

E3.7.1.3.3. AT Physical Security Measures (see STANDARD 13).

E3.7.1.3.4. AT Measures for Off-installation Facilities, Housing, and Activities (see STANDARD 15).

E3.7.1.3.5. AT Measures for HRP (see STANDARD 16).

E3.7.1.3.6. AT Construction and Building Considerations (see STANDARD 17).

E3.7.1.3.7. AT Measures for Logistics and Other Contracting (see STANDARD 18).

E3.7.1.3.8. AT Measures for Critical Asset Security (see STANDARD 19).

E3.7.1.3.9. AT Measures for Intransit Movements.

E3.7.1.3.10. Terrorism Incident Response Measures (see STANDARD 20).

E3.7.1.3.11. Terrorism Consequence Management Measures, including CBRNE and WMD mitigation planning (see STANDARD 21).

E3.7.1.3.12. FPCON Implementation Measures, including site-specific AT measures (see STANDARD 22).

E3.7.1.3.13. CBRN Defense Joint Enabling Concepts of Sense, Shape, Shield, and Sustain per JROCM 180-3 (Reference (s)).

E3.7.2. The Geographic Combatant Commanders shall provide AT planning information (e.g., airfield, port, and movement route information and threat; vulnerability and criticality assessment data) to deploying DoD Component units to enable them to perform risk management and develop a tailored AT plan.

E3.7.2.1. Direct the execution of advance site reviews to facilitate the AT planning process in areas assessed as SIGNIFICANT or HIGH Threat Level or where a specific Terrorism Warning is in effect.

E3.7.2.2. At the discretion of the Geographic Combatant Commander, such security efforts may be waived for deployments or visits to controlled locations such as existing military installations or ships afloat. Augmentation of assessment personnel may be necessary to enable subordinate Component Commanders to discharge their responsibility to provide security, surveys, assessments, CI, and countersurveillance support, and to act as the liaison with the country team, host-nation security force, husbanding contractor, and port authority.

E3.7.2.3. In countries where available, FPD will assist by providing surveys, assessments, CI, and countersurveillance support, and act as the liaison with the country team, host-nation security forces, husbanding contractor, and port authority.

E3.8. DoD STANDARD 8: AT Program Coordination

E3.8.1. The Geographic Combatant Commanders shall coordinate AT and security matters with the appropriate Chiefs of Mission and host-nation authorities for countries within their AOR and with the Heads of the other DoD Components whose personnel are stationed in or transit the respective Geographic Combatant Commander's AOR.

E3.8.2. The Heads of the DoD Components (whose personnel will be stationed in, or transit, the AOR of a Geographic Combatant Commander) shall:

E3.8.2.1. Initiate coordination of AT matters with the appropriate Geographic Combatant Commander pursuant to the requirements established by Reference (b).

E3.8.2.2.. Coordinate AT matters with local, State, Federal, and host-nation authorities pursuant to existing law and DoD policy to support AT planning and program implementation.

E3.8.3. Subordinate elements of the DoD Components that are tenant units on installations or separate facilities shall coordinate their AT program and plan requirements with the host installation or separate facility commander or civilian equivalent director. Tenant units shall participate fully in installation and separate facility AT programs. At locations where there are multiple DoD Components, such as DoD-leased facilities or other facilities where DoD occupies space, the designated senior DoD Component shall be responsible for integrating and coordinating individual DoD Component security plans into a comprehensive installation or facility or area-wide AT program.

E3.9. DoD STANDARD 9: Antiterrorism Officer (ATO). The Heads of the DoD Components shall:

E3.9.1. Ensure subordinate elements designate, in writing, a Level II-certified (see DoD STANDARD 26 for criteria) commissioned officer, non-commissioned officer, or civilian staff officer as the ATO. ATOs shall be assigned at the battalion, ship, squadron, and separate facility and higher levels (stationary or deployed). A deploying unit having 300 or more personnel assigned or under the operational control of a designated commander will have a Level II-certified ATO.

E3.9.2. At the Combatant Command, Military Department, and Defense Agency or Field Activity Headquarters level, designate, train, and resource a full-time staff to support ATOs in administering their respective AT programs.

E3.9.3. Consider maintaining full-time AT staffs, including individuals with CBRNE expertise, at the Component Command, installation, separate facility, and other subordinate headquarters levels as appropriate.

E3.10. DoD STANDARD 10: Antiterrorism Working Group (ATWG). The Heads of the DoD Components shall establish an ATWG at the installation and separate facility level and higher (stationary or deployed) that meets at least semi-annually or more frequently, depending upon the level of threat activity, to oversee the implementation of the AT program, to develop and refine AT plans, and to address emergent or emergency AT program issues. ATWG membership shall include the ATO, the Commander (or a designated representative), representatives of the principal staff, including CBRNE expertise, tenant unit representatives, and other representatives as required to support AT planning and program implementation.

E3.11. DoD STANDARD 11: Threat Working Group (TWG). The Heads of the DoD Components shall establish a TWG at the installation and separate facility level and higher (stationary or deployed) that meets at least quarterly or more frequently, depending upon the level of threat activity, to develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries. TWG membership shall include the ATO; the Commander (or a designated representative); members of the staff; tenant unit representatives; and appropriate representation from direct-hire, contractor, local, State, Federal, and host-nation law enforcement agencies and the IC.

E3.12. DoD STANDARD 12: AT Executive Committee (ATEC). The Heads of the DoD Components shall establish an AT executive-level committee or similarly structured corporate body at the installation and separate facility level and higher (stationary or deployed) that meets at least semi-annually to develop and refine AT program guidance, policy, and standards; to act upon recommendations of the ATWG and TWG; and to determine resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities.

E3.13. DoD STANDARD 13: AT Physical Security Measures. The Heads of the DoD Components shall:

E3.13.1. Apply the principles of Reference (f) and fully integrate them into AT Plans to ensure employment of a holistic security system to counter terrorist capabilities. Well-designed AT physical security measures are multi-layered and include the integration and synchronization of the following essential elements: detection (human, animal, or sensors to alert security personnel of possible threats and unauthorized entry attempts at or shortly after occurrence); assessment (electronic audio-visual means, security patrols, or fixed posts to localize and determine the size and intentions of unauthorized intrusion or activity); delay/denial (active and passive security measures including barriers to impede intruders' efforts); communication (command and control procedures) and response (trained and properly equipped security forces). The development of comprehensive AT physical security measures requires the integration of facilities, physical security equipment, trained personnel, and procedures oriented at a minimum in support of perimeter and area security, access and egress control, protection against CBRNE attacks (including those using the postal system), HRP protection, barrier plans, and facility standoff distances.

E3.13.2. Develop AOR or other mission-specific physical security policies to guide subordinate development of local physical security systems and the purchase of physical security equipment.

E3.13.3. Coordinate and integrate tenant command and unit security plans and measures into the AT Plan.

E3.14. DoD STANDARD 14: Random Antiterrorism Measures (RAM). The Heads of the DoD Components shall:

E3.14.1. Develop and implement RAM as an integral component of the overall AT program guided by the principles outlined in Reference (i). To maximize the effectiveness and deterrence value, RAM should be implemented without a set pattern, either in terms of the measures selected, time, place, or other variables. RAM, at a minimum, shall consist of the random implementation of higher FPCON measures in consideration of the local terrorist capabilities. Random use of other physical security measures should be used to supplement FPCON measures.

E3.14.2. Employ RAM, in conjunction with site-specific FPCON measures (see DoD STANDARD 22), in a manner that portrays a robust security posture from which terrorists cannot easily discern security AT and security patterns or routines.

E3.14.3. Include tenant units and commands in RAM planning and execution.

E3.14.4. Develop command-unique and site-specific FPCON measures for added deterrence effect (see DoD STANDARD 22).

E3.15. DoD STANDARD 15: AT Measures for Off-Installation Facilities, Housing, and Activities. The Heads of the DoD Components shall:

E3.15.1. Develop in their overall AT programs specific AT measures for off-installation facilities, housing, transportation services, daycare centers, and other activities used by or involving a mass-gathering of DoD personnel and their dependent family members. These risk mitigation measures shall include, but are not limited to: emergency notification and recall procedures; guidance for selection of off-installation housing, temporary billeting, and other facility use (including compliance with Unified Facilities Criteria 04-010-01 (Reference (t)) for leased, newly constructed, and expeditionary buildings); physical security measures; CBRNE defensive measures; and shelter-in-place, relocation, and evacuation procedures.

E3.15.2. Develop Mutual Aid Agreements or other similarly structured protocols with the appropriate local, State, Federal, and host-nation authorities to coordinate security measures and assistance requirements to ensure the protection of DoD personnel and their family members at off-installation facilities and activities.

E3.16. DoD STANDARD 16: AT Measures for High-Risk Personnel (HRP). The Heads of the DoD Components shall:

E3.16.1. Develop AT measures pursuant to the principles outlined in Reference (h) for personnel designated as HRP, for those personnel occupying HRB, and for other personnel designated as distinguished visitors.

E3.16.2. Annually, identify to the responsible Military Department those personnel designated as HRP, and those personnel assigned to HRB.

E3.16.3. Identify to the responsible Military Department those personnel, including designated HRP family members, requiring formal HRP training before assignment. This will enable the Military Departments to schedule the required training.

E3.16.4. Ensure HRP and family members, as appropriate, complete appropriate high-risk training (personal protection, evasive driving, AT awareness, and hostage survival); are properly cleared for assignment to HRBs, facilities, or countries requiring such protection; and have been thoroughly indoctrinated on the duties and responsibilities of protective service personnel.

E3.16.5. Ensure that HRP designees and their family members are familiar with treaty, statutory, policy, regulatory, and local constraints on the application of supplemental security measures for certain high-ranking DoD officials who are provided additional protection due to their position.

E3.16.6. Complete PSVA for each person designated as HRP. PSVA will be initiated within 90 days of an individual's assignment to an HRB or designation of an individual as HRP. PSVA will be revalidated annually and updated if the Terrorism Threat Level changes but no less than every 3 years.

E3.16.7. Review HRP security measures within 60 days of changes to the Terrorism Threat Level for the affected country and HRP.

E3.16.8. Comply with the provisions of the DoD Non-Tactical Armored Vehicle Policy (DoD C-4500.51, Reference (u)) for the acquisition and use of non-tactical armored vehicles.

E3.17. DoD STANDARD 17: AT Construction and Building Considerations. The Heads of the DoD Components shall:

E3.17.1. Fully comply with the standards prescribed in Reference (f) and the Unified Facilities Criteria (References (v) and (w)) regarding the adoption of and adherence to common criteria and minimum construction standards to mitigate vulnerabilities.

E3.17.2. Develop a prioritized list of AT measures for use by site selection teams. These criteria shall be used to determine if facilities either currently occupied or under consideration for occupancy by DoD personnel provide adequate protection of occupants against the effects of a terrorist attack. Circumstances may require the movement of DoD personnel or assets to facilities the U.S. Government had not previously used or surveyed. AT standards shall be a key consideration in evaluating the suitability of these facilities for such use.

E3.18. DoD STANDARD 18: AT Measures for Logistics and Other Contracting. The Heads of the DoD Components shall:

E3.18.1. Incorporate AT measures into the logistics and contracting processes (requirements development, vendor selection, award, execution, and evaluation) when the provisions of the contract or services provided affect the security of DoD elements, personnel, or mission-essential cargo, equipment, assets, or services. Consider AT performance as an evaluation factor for award (past performance and proposed performance under the instant contract), and as a performance metric under the resultant contract.

E3.18.2. Implement a verification process, whether through background checks or other similar processes, that enables the U.S. Government to attest to the trustworthiness of DoD contractors and sub-contractors (U.S. citizens, host-nation, and third country personnel) to the greatest extent possible, including those personnel having direct or indirect involvement in the delivery or provision of services. Priority will go to service provisioning related to mail, supplies, food, water, or other materiel and equipment intended for use by DoD personnel. This vetting of trustworthiness shall include husbanding agents and crews on contracted ships, planes, trains, and overland vehicles.

E3.18.3. Develop and implement site-specific risk mitigation measures to maintain positive control of DoD contractor and sub-contractor access to and within installations, sensitive facilities, and classified areas.

E3.18.4. Develop and implement site-specific risk mitigation measures to screen contractor or sub-contractor transportation conveyances for CBRNE hazards before entry into or adjacent to areas with DoD personnel and mission-essential assets.

E3.18.5. Ensure that contracts comply with the AT provisions of the Defense Federal Acquisition Regulation Supplement (Reference (x)).

E3.18.6. Ensure that contracts incorporate AT Level I training requirements

E3.19. DoD STANDARD 19: AT Measures for Critical Asset Security. The Heads of the DoD Components shall:

E3.19.1. Develop and implement risk mitigation measures to reduce the vulnerabilities of DoD critical assets to terrorist attack, with emphasis on risk management, and integrate these measures into overall AT program efforts. Critical assets include those assets designated as Unified Facilities Criteria (per Reference (w)) and distributive information and computer-based systems and networks.

E3.19.2. Include coordination with the appropriate local, State, Federal, or host-nation authorities responsible for the security of non-DoD assets deemed essential to the functioning of DoD critical assets and overall capability of the Department of Defense to execute the National Military Strategy.

E3.20. DoD STANDARD 20: Terrorism Incident Response Measures

E3.20.1. The Heads of the DoD Components shall develop terrorism incident response measures consistent with the principles outlined in Reference (h) and include these measures in the overall AT plan. These measures shall include procedures for determining the nature and scope of incident response (including incidents with a CBRNE component); procedures for coordinating security, fire, medical, hazardous materiel, and other emergency responder capabilities; and steps to recover from the incident while continuing essential operations.

E3.20.2. The Geographic Combatant Commanders shall prepare terrorist incident response measures for their AOR. It is critical that Geographic Combatant Commanders deploy in a timely manner a Terrorist Incident Response team capable of providing advice to local, State, Federal, or host-nation authorities; supporting emergency lifesaving and rescue functions; providing protection of DoD personnel and property; reducing further effects and damage; and when appropriate, conducting or supporting criminal investigations. This preparation shall include FPD involvement in contingency planning for in-transit units.

E3.21. DoD STANDARD 21: Terrorism Consequence Management Measures. The Heads of the DoD Components shall:

E3.21.1. Include terrorism consequence management, CBRNE and public health emergency preparedness, and emergency response measures as an adjunct to the overall AT Plan. These measures shall focus on mitigating vulnerabilities of personnel, families, facilities, and materiel to terrorist use of WMD and CBRNE weapons, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures shall include integration and full compliance with DoD Emergency Responder guidelines (Reference (d)); mass notification

system standards (Unified Facilities Criteria 4-021-01 (Reference (x))); establishment of medical surveillance systems (DoD Directive 6490.2 (Reference (y))); and deployment of CBRNE sensors and detectors; providing collective protection; and providing individual protective equipment in the following priority:

E3.21.1.1. Emergency Responders and First Responders. Personnel who work closest to known or suspected CBRNE hazards (e.g., emergency responders) should be given the best protection (e.g., “Level A”). Responders should use maximum possible protection until determined otherwise by competent authority.

E.3.21.1.2. Critical Personnel. Personnel deemed essential to the performance of critical military missions (whether military, civilian, contractor, host-nation personnel, or third country nationals) should be provided an appropriate level of protection to support continuity of those critical military missions. Since critical missions should be continued without interruption, collective or individual protection may be necessary to sustain them.

E.3.21.1.3. Essential Personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, host-nation personnel, or third country nationals) should be provided an appropriate level of protection to support near continuity for those essential military operations. Since essential operations may be interrupted for relatively short periods (e.g., hours to days), escape protection may be necessary to sustain essential operations (i.e., escape, survive, and restore essential operations).

E.3.21.1.4. Other Personnel. For all other persons not in the above categories, the objective will be to provide the procedures or protection necessary to safely survive an incident. Evacuation procedures, for example, may fulfill this requirement.

E.3.21.1.5. Included as part of the above categories are those who work or live on DoD installations worldwide, family members authorized overseas, and DoD contractors if designated in contract agreements and designated as essential to perform critical DoD missions.

E3.21.2. Develop and implement site-specific CBRNE preparedness and emergency response measures that are synchronized with a corresponding FPCON measure.

E3.21.3. Establish Mutual Aid Agreements or other similarly constructed protocols with the appropriate local, State, Federal, or host-nation authorities to support AT plan execution and augment incident response and post-incident consequence management activities.

E3.21.4. Ensure the installation can warn its resident population in affected areas of CBRNE hazard identification immediately, but no longer than 10 minutes after detection. The warning must include instructions to remain in place or evacuate.

E.3.21.5. Develop and implement site-specific public health emergency response measures that are synchronized with FPCON levels in accordance with References (r) and (z).

E3.22. DoD STANDARD 22: FPCON Measures

E3.22.1 The Geographic Combatant Commanders have ultimate AT authority and responsibility for all DD Elements and Personnel (including family members), except for those under the security responsibility of a COM, within the Combatant Commander's AOR (Reference (b)). The Geographic Combatant Commanders shall be responsible for establishing the baseline FPCON for the AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented.

E3.22.2. The Heads of the DoD Components shall:

E3.22.2.1. Establish policies and procedures for setting FPCON levels; FPCON transition; dissemination and implementation of FPCON measures; notification of higher headquarters and affected DoD Component headquarters; development of site-specific FPCON measures; and a waiver (exceptions) process for FPCON implementation (approved waivers shall be in writing, consistent with the guidelines outlined in Reference (h)).

E3.22.2.2. Establish a review mechanism to lower the FPCON level as soon as the threat environment permits. This is essential because implementation of FPCON measures at elevated FPCON levels for an extended duration can be counter-productive to effective security and overall mission accomplishment. In some circumstances, based upon local conditions and the threat environment, commanders should consider implementing a lower-level FPCON and supplement with other local security measures and RAM as an effective alternative to executing the higher-level FPCON measures.

E3.22.2.3. Develop and implement site-specific FPCON measures for stationary and in-transit forces to supplement the FPCON measures and actions enumerated for each FPCON level in Enclosure 4 to this Instruction. The development of site-specific FPCON measures must permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement (Chairman of the Joint Chiefs of Staff Instruction 3121.01B (Reference (z)) and Rules of Force (DoD Directive 5210.56 (Reference (aa))). Organic intelligence, CI, and law enforcement resources, institutional knowledge of the area of AT responsibility, and comprehensive understanding of organic capabilities, supported by national and AOR assets, shall be leveraged in directing tailored FPCON measures to be implemented at specific sites for both stationary and in-transit forces.

E3.22.3. The DoD Component Subordinate Commanders shall:

E3.22.3.1. Determine an appropriate FPCON level for those personnel and assets for which they have AT responsibility. DoD Component subordinate commanders may raise a higher-level commander's FPCON level, but they shall not lower a higher-level commander's FPCON level without the higher-level commander's written concurrence.

E3.22.3.2. Establish Site-specific AT measures and physical security actions, linked to an FPCON, which shall be classified “CONFIDENTIAL.” When separated from the AT Plan, specific AT measures linked to a FPCON and site-specific FPCON levels may be downgraded to “FOR OFFICIAL USE ONLY” if appropriate.

E3.23. DoD STANDARD 23: AT Training and Exercises

E3.23.1. The Heads of the DoD Components shall:

E3.23.1.1. Ensure that AT training and exercises are integrated with overall physical security and are afforded the same emphasis as combat task training and executed with the intent to identify shortfalls affecting the protection of personnel and assets against terrorist attack and subsequent terrorism consequence management efforts.

E3.23.1.2. Ensure that AT training, particularly pre-deployment training, is supported by measurable standards, including credible deterrence and response standards; deterrence-specific tactics, techniques, and procedures (TTP); and lessons learned. AT training shall also be incorporated into unit-level training plans and predeployment exercises. Ensure that joint operations and exercises incorporate AT training and planning for forces involved. Predeployment training shall also include terrorist scenarios and hostile intent decision making.

E3.23.1.3. Conduct comprehensive field and staff training, including deploying units (battalion, ship, squadron, equivalent-sized units, and above) to exercise AT plans at least annually. Ensure that annual AT exercises encompass all aspects of AT and physical security plans. Additionally, the current baseline FPCON through FPCON Charlie measures shall be exercised at installations and separate facilities.

E3.23.2. Commanders shall:

E3.23.2.1. Maintain AT exercise documentation for no less than 2 years to ensure incorporation of lessons learned.

E3.23.2.2. Encourage subordinates to exercise their AT plans more frequently.

E3.23.2.3. Ensure AT lessons learned are submitted in accordance with the Joint Lessons Learned Program (Chairman of the Joint Chiefs of Staff Instruction 3150.25A, Reference (ab)).

E3.23.2.4. Implement AT measures through FPCON Delta at parts of the installation.

E3.23.3. The AT Officer shall develop an annual training and exercise program to provide the necessary individual and collective training to prepare for the annual exercise.

E3.24. DoD STANDARD 24: Formal AT Training. The DoD's formal AT Training Program shall consist of Level I through Level IV Training, AOR-specific Training, and HRP AT Training (see DoD STANDARD 16 for HRP training requirements).

E3.24.1. The Heads of the DoD Components shall ensure all assigned personnel complete appropriate formal training and education. Individual records shall be updated to reflect completion of the AT training prescribed by this Instruction and DoD Component policy.

E3.24.2. Commanders, at all levels, who receive individuals not properly trained shall provide the required AT training as soon as possible following the arrival of such individuals. Concurrently, they shall report the deficiency through their DoD Component chain of command to the losing DoD Component, which shall institute appropriate corrective action to prevent recurrence of the discrepancy. Tables E3.T1. through E3.T4 outline the minimum requirements for Level I through Level IV training.

E3.25. DoD STANDARD 25: Level I AT Awareness Training. (Table E3.T1. outlines the minimum requirements for Level I training).

E3.25.1. The Heads of the DoD Components shall:

E3.25.1.1. Ensure that every military service member, DoD employee, and local national or third country citizen in a direct-hire status by the Department of Defense, regardless of grade or position, completes Level I AT Awareness Training requirements prescribed by this Instruction and is knowledgeable on AT TTP.

E3.25.1.2. Provide AT information to DoD contractors as required by Reference (x), section 252.225-7043. Offer AT Awareness Training to DoD contractor employees under the terms and conditions as specified in the contract.

E3.25.1.3. Ensure that dependent family members ages 14 years and older (or younger at the discretion of the DoD sponsor) traveling outside the Continental United States (OCONUS) on official business (e.g., on an accompanied permanent change of station move) complete Level I AT Awareness Training as part of their pre-departure requirements.

E3.25.1.4. Provide Level I AT Awareness Training in initial entry basic training or in general military subject training for all initial entry Military Department and Defense Agency or Field Activity civilian personnel. DoD personnel accessions must receive this initial training under the instruction of a qualified Level I AT Awareness Instructor.

E3.25.1.5. Provide post-accession Level I AT Awareness Training annually to all DoD personnel. Annual post-accession Level I AT Awareness Training may be accomplished by one of two means:

E3.25.1.5.1. Under the instruction of a qualified Level I AT Awareness Instructor.

E3.25.1.5.2. Completion of a DoD-sponsored and certified computer or web-based distance learning instruction for Level I AT Awareness. Personnel assigned or attached to an embassy on TDY under Chief of Mission authority must receive Level I AT Training from a qualified instructor (Level II AT Training qualified). The completion of a DoD-sponsored and certified computer-based distance learning instruction for Level I AT awareness will not satisfy Department of State Chief of Mission requirements.

E3.25.1.6. Designate in writing all individuals qualified to administer Level I AT Awareness Training. Individuals may qualify to administer Level I AT Awareness Training via two methods:

E3.25.1.6.1. Completion of a formal Military Department-approved Level II ATO Training Course of Instruction, whether a course in residence or through a mobile training team.

E3.25.1.6.2. For DoD Agencies and field activities only, certification may be achieved by completion of a DoD-sponsored and certified computer or web-based distance learning instruction course for Level II ATO Training. Other DoD components may use DoD-sponsored and certified computer or web-based distance learning instruction only to augment their formal Course of Instruction.

E3.25.2. Commanders shall:

E3.25.2.1. Certify and appoint qualified Subject Matter Experts (e.g., military police, security forces, special agents, CBRNE, intelligence personnel) who have received formal training in AT TTP and individual security and protection, and are knowledgeable in the current AT publications and methods for obtaining AOR-specific updates. Commanders must clearly describe the qualifications of the individual in the appointment letter to justify this method and explain why the other options are not feasible.

E3.25.2.2. Encourage dependent family members to complete Level I AT Awareness Training before any travel OCONUS (e.g., leave) or to any locale where the Terrorism Threat Level is MODERATE or higher.

E3.25.3. Individuals completing this training shall:

E3.25.3.1. Have the requisite knowledge to remain vigilant for possible terrorist actions.

E3.25.3.2. Be capable of employing AT TTP as outlined in Reference (h).

Table E3.T2. Minimum Level I AT Awareness Training Requirements

Level I AT Awareness Minimum Training Requirements
<p>1. View a Military Department, Defense Agency, or Field Activity-selected personal AT awareness video. Those personnel who complete a DoD-sponsored and certified computer or web-based distance learning Level I training course are not required to view an awareness video.</p> <p>2. Level I AT Awareness Instruction shall include at least the following:</p> <ul style="list-style-type: none"> • Introduction to Terrorism • Terrorist Tactics and Operations • Individual Protective Measures • Personal Protective Measures for CBRNE attacks to Include Sheltering in Place or Evacuation, Indicators of CBRNE attack, Impromptu Methods of Decontamination, etc. • Terrorist Surveillance Techniques • Improvised Explosive Device (IED) Attacks • Kidnapping and Hostage Survival • Explanation of Terrorism Threat Levels and FPCON System Levels and Measures <p>3. Note: All DoD Personnel should be provided and retain personal copies of Chairman of the Joint Chiefs of Staff Guide 5260, "Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism," (Reference (ac)) and Chairman of the Joint Chiefs of Staff Pocket Card 5260 "Antiterrorism Individual Protective Measures" (Reference (ad)). Local reproduction of both CJCS issuances is authorized.</p>

E3.26. DoD STANDARD 26: Level II Antiterrorism Officer (ATO) Training. The Heads of the DoD Components shall:

E3.26.1. Ensure that each installation, separate facility, and stationary or deployed unit, throughout the chain of command (battalion, squadron, equivalent-sized units, and above) is assigned at least one Level II certified ATO who is appointed in writing. A deploying unit having 300 or more personnel assigned or under the operational control of a designated commander will have a Level II-certified ATO. Deploying units consisting of less than 300 personnel may designate a Level-II ATO due to Military Department, COCOM, or threat assessment constraints.

E3.26.2. Qualify individuals as an ATO by completion of a formal Military Department-approved Level II ATO Training Course of Instruction, whether a course in residence or through a mobile training team. Level II ATO Training shall prepare ATOs to manage AT Programs, advise the Commander on all AT issues, and qualify individuals to administer Level I AT Awareness Training. Table E3.T2. outlines Level II ATO training requirements separated by installation and deployable unit ATOs.

E3.26.2.1. For DoD Agencies and Field Activities only, certification may be achieved by completion of a DoD-sponsored and certified computer or web-based distance learning instruction course for Level II ATO Training. Other DoD components may use DoD-sponsored and certified computer or web-based distance learning instruction only to augment their formal Course of Instruction.

E3.26.2.2. Ensure completion of a formal Military Department-approved Level II ATO refresher Training Course of Instruction at least every 3 years.

Table E3.T3. Minimum Level II ATO Training Requirements⁷

Level II AT Officer (ATO) Minimum Training Requirements
<p>1. (I/U) Complete a formal Military Department-approved Level II ATO Training Course of Instruction, whether a course in residence or through a mobile training team (CONUS or OCONUS). For DoD agencies or field activities, a DoD-sponsored and certified computer or web-based distance learning instruction course for Level II ATO Training is acceptable.</p> <p>2. (I/U) Level II ATO Training shall consist of the following minimum topics:</p> <ul style="list-style-type: none"> • (I/U) Understanding AT Roles and Responsibilities <ul style="list-style-type: none"> – (I) Understand Department of Defense, Military Department, and applicable Agency/Field Activity Policy – (I/U) Understand Current Standards – (I/U) Access Reference Sources to include the AT Enterprise Portal (ATEP) on the SIPRNET at https://www.atep.smil.mil or NIPRNET at https://atep.dtic.mil/portal/site/atep – (I/U) Understand online Core Vulnerability Assessment Management Programs (CVAMP) – (I) Understand necessary coordination with host-nation, Combatant Commands, Department of State, U.S. Embassies, and other government agencies • (I/U) Understanding Minimum Required AT Program Elements <ul style="list-style-type: none"> – (I/U) Risk Management – (I/U) AT Planning – (I/U) Training and Exercises – (I/U) Resource Application

⁷ Requirements are identified by Installation ATO (I), Unit ATO (U) or both (I/U). For DoD components separating installation from unit ATO training, unit level ATO training should emphasize managing AT programs in contingency operations.

Level II AT Officer (ATO) Minimum Training Requirements	
–	(I/U) Comprehensive Program Reviews
•	(I/U) How to Organize AT Groups
–	(I) Command and Staff Relationships on an Installation
–	(U) Command and Staff Relationships in Contingency and Joint Operations
–	(I) ATWG
–	(I) TWG
–	(I) ATEC
–	(U) Establishing the ATWG, TWG, and ATEC in a Contingency Environment
–	(U) Understanding Operations Center Functions
•	(I/U) Risk Management Considerations
–	(I/U) Threat Assessments
○	(I/U) Identify Terrorism
○	(I) Terrorist Tactics and Operations
○	(U) Terrorist Tactics and Operations in a Contingency Environment
○	(I) Domestic and International Terrorist Threat
○	(I) Intelligence and CI Integration
○	(I/U) Practical Exercise—Conducting a Threat Assessment
–	Criticality Assessments
○	(I) Assessment Methodology for an Installation
○	(I/U) Practical Exercise—Conducting a Criticality Assessment
–	(I/U) Vulnerability Assessments
○	(I) Assessment Methodology for an Installation
○	(U) Assessment Methodology in a Tactical Environment
○	(I/U) Practical Exercise - Conducting a Vulnerability Assessment
–	(I/U) Risk Assessments
○	(I/U) Assessment Methodology
○	(I/U) Practical Exercise—Conducting a Risk Assessment
•	(I/U) Create and Execute AT Programs (consider using the Joint Antiterrorism (JAT) Guide program)
–	(I/U) Use of Terrorism Threat Levels and FPCON
–	(I/U) Site Specific Protective Measures
–	(U) Establishing Access Control Points/Entry Control Points in Contingency Operations
–	(U) Barrier Planning in Contingency Operations
–	(U) Establishing Electronic Detection and Security Capability in Contingency Operations
–	(I/U) Mitigating Vulnerabilities
–	(I/U) Use of RAM
•	(I/U) Prepare AT Plans (consider using the JAT Guide)
–	(I/U) Templates and Planning Tools
–	(I/U) Minimum Essential AT Plan Elements
–	(I/U) How to Develop and Write Plans

Level II AT Officer (ATO) Minimum Training Requirements	
<ul style="list-style-type: none"> – (U) How to Integrate AT Plans with Base Defense/Tactical Operations – (I) CBRNE and WMD Considerations – (I) Vehicle Bomb Search Planning – (I/U) Vehicle Inspection Checklist – (U) Deployment/In-transit Considerations • (I/U) Determine AT Resource Management – (I/U) Vulnerability Identification and Management, Resource Application, and Prioritization using CVAMP – (I/U) CbT RIF – (I/U) Identify Physical Security and Construction Requirements – (I/U) Identify Communications Systems Requirements • (I/U) Conduct AT Training – (U) Conduct and Oversee Level I AT Awareness Training – (I) Develop AT Exercise Plans – (I/U) Obtain AOR-specific Updates for deployments and travel areas • (I) Case Studies – Installation Based • (U) Case Studies – Contingency Operations • (I) Legal Considerations • (I) Interagency and Host-Nation Responsibilities and Jurisdictions • (I) Special law enforcement Considerations • (I/U) Access to DoD AT Lessons Learned Databases • (I) Familiarization with HRB/HRP Requirements • (I) AT Considerations in Contracting <p>3. (I/U) Review of the following DoD and Joint Staff publications.</p> <ul style="list-style-type: none"> • (I) DoD Directive 2000.12 • (I/U) DoD Instruction 2000.16 • (I/U) DoD Instruction 2000.18 • (I/U) DoD O-2000.12-H • (I/U) CJCS Guide 5260 • (I/U) Unified Facilities Criteria (UFC) 4-010-01, 4-010-02, and 4-021-01 • (I/U) DoD 4500.54-G • (I/U) Other applicable Military Department, Defense Agency, or Field Activity publications <p>4. (I/U) Component-directed modules on other aspects of AT such as physical security requirements, critical infrastructure protection, technology updates, and CBRNE installation preparedness.</p>	

E3.27. DoD STANDARD 27: Level III Pre-Command AT Training. The Heads of the DoD Components shall ensure that O5 and O6 commanders (or civilian equivalent director position) complete Level III Pre-Command AT Training before assuming command.

Table E3.T4. Minimum Level III AT Training Requirements⁸

Level III Pre-Command AT Minimum Training Requirements
<p>1. Level III Pre-Command AT Training shall be conducted during pre-command or pre-assignment training/orientation.</p> <p>2. Level III Pre-Command AT Training shall include the following minimum topics:</p> <ul style="list-style-type: none"> • Understanding AT Responsibilities and Minimum AT Program Elements <ul style="list-style-type: none"> – Understanding Policy – Staff AT Roles – Duties and Responsibilities of the ATO – Risk Management and Risk Assessments – AT Planning – AT Training and Exercises – AT Resource Application – Comprehensive AT Program Review • Ensuring Preparation of AT Plans <ul style="list-style-type: none"> – Baseline FPCON Posture – Mitigating CBRNE/WMD Attack/Risks – MOUs, MOAs, and MAAs – JAT Guide Capabilities • Ensuring Conduct of AT Planning <ul style="list-style-type: none"> – AT Plans and Training – Level I Training – Level II Training • Organizing AT Groups <ul style="list-style-type: none"> – ATWG – TWG – ATEC • Understanding the Local Threat Picture <ul style="list-style-type: none"> – Potential Sources of Law Enforcement-Derived Force Protection information – Fusion of Intelligence, Counterintelligence, and law enforcement Information – Terrorism Threat Levels • Building a Sustainable AT Program <ul style="list-style-type: none"> – CVAMP Capabilities • Executing Resource Responsibilities <ul style="list-style-type: none"> – AT Resourcing Program

⁸ Level III Pre-Command AT Training provides prospective O5 and O6-level commanders with the requisite knowledge to direct and supervise AT programs.

Level III Pre-Command AT Minimum Training Requirements
<ul style="list-style-type: none"> - Role of CVAMP in Resource Process - Construction Standards • Understanding Use of Force and Rules of Engagement <ul style="list-style-type: none"> - Terrorist Scenarios and Hostile Intent Decision Making <p>3. Review of References (b) and (i), this Instruction, and other applicable DoD Joint, Military Department, Defense Agency, or Field Activity publications.</p> <p>4. Note: All Level III recipients should be issued and retain a personal copy of Joint Pub 3-07.2.</p>

E3.28. DoD STANDARD 28: Level IV AT Executive Seminar. The Heads of the DoD Components shall ensure that the appropriate military officers in the grades of O6 through O8 and civilian equivalent/senior executive service civilian employees attend the Level IV AT Executive Seminar. Table E3.T5. outlines the minimum requirements for the training.

E3.28.1. Administered by the Joint Staff (J3, DD AT/HD, J34), this seminar provides DoD senior military and civilian executive leadership with the requisite knowledge to enable development of AT Program policies and facilitate oversight of all aspects of AT Programs at the operational and strategic levels.

E3.28.1. Directors of Defense Agencies and Defense Field Activities should also attend this training.

Table E3.T5. Minimum Level IV AT Training Requirements

Level IV AT Executive Seminar Minimum Training Requirements
Executive-level seminar hosted by J-3 Deputy Director for AT/Homeland Defense, J34. Provides AT updates, briefings, panel discussion topics, and tabletop AT and Terrorist Consequence Management war games.

E3.29. DoD STANDARD 29: AOR-Specific Training for DoD Personnel and In-transit Forces. The Geographic Combatant Commanders shall:

E3.29.1. Develop AT Awareness Training and Education programs to orient all DoD personnel (including family members ages 14 years and older) assigned permanently or temporarily, transiting through, or performing exercises or training in the AOR with AOR-specific information on AT protection. This AOR-specific information is in addition to annual

Level I AT Awareness Training and may be provided through multiple means including Combatant Command publications, messages, Internet homepages, and the DoD Foreign Clearance Guide (DoD 4500.54-G (Reference (ae))).

E3.29.2. Ensure that DoD personnel (including family members ages 14 years and older) departing to another Geographic Combatant Commander's AOR complete the gaining Combatant Commander's AOR-specific AT education requirements within three months of a permanent change of station.

E3.29.3. Provide in-transit forces, units, and individuals with detailed threat information covering transit routes and sites that will be visited by the deploying unit or individuals. Such information shall include focused information on potential terrorist threats (e.g., tailored production and analysis) and guidance on the development of AT protection risk mitigation measures to aid in the development of tailored AT planning. Similar tailored information shall also be provided to intra-theater transiting units and individuals.

E3.29.4. Periodically update Reference (ac) regarding the country and AOR-specific AT training and education requirements for travel within the AOR.

E3.30. DoD STANDARD 30: AT Resource Application

E3.30.1. The Heads of the DoD Components shall:

E3.30.1.1 Assess the risk against the standard and apply mitigation measures. Where the resulting risk is still deemed too great, elevate the vulnerability using the PPBE process and implement the DoD-approved methodology for documenting and prioritizing AT resource requests.

E3.30.1.2. When faced with emergency or emergent AT risks that could not reasonably have been anticipated or programmed, submit to the Chairman of the Joint Chiefs of Staff through the appropriate Combatant Commander CbT-RIF requests pursuant to the requirements specified in CJCSI 5261.01D (Reference (af)).

E3.30.1.3. Submit validated prioritized AT resource requests with compelling justification, including those submitted or considered for CbT-RIF, to the Chairman of the Joint Chiefs of Staff on an annual basis pursuant to current DoD Program Objective Memorandum guidance and timelines using the CVAMP.

E3.30.2. The Combatant Commanders shall forward CbT-RIF requests to the Department of Defense via the Chairman of the Joint Chiefs of Staff using CVAMP.

E3.31. DoD STANDARD 31: Comprehensive AT Program Review. The Heads of the DoD Components shall:

E3.31.1. Conduct comprehensive AT Program Reviews to evaluate the effectiveness and adequacy of AT Program implementation. The evaluation shall include an assessment of the degree to which DoD Component AT Programs comply with the standards prescribed in this Instruction. AT Program Reviews shall evaluate all mandatory AT program elements (see DoD STANDARD 1) and assess the viability of AT Plans (see DoD STANDARD 7) in view of local operational environment constraints and conditions.

E3.31.2. Ensure that comprehensive AT Program Reviews are conducted at least annually by all commanders required to establish AT programs.

E3.31.3. Ensure that a comprehensive AT Program Review is conducted in conjunction with predeployment vulnerability assessments (see DoD STANDARD 6).

E3.31.3.1. The purpose of a Predeployment AT Program Review is to ensure that deploying units have viable AT programs and executable AT Plans for transit to, from, and during operations or training exercises in the deployed AOR.

E3.31.3.2. The deploying DoD Component's elements shall comply with the geographic Combatant Commander's AT guidance.

E3.31.4. Ensure that a comprehensive AT Program Review is conducted whenever there are significant changes in threat, vulnerabilities, or asset criticality.

E3.31.5. Ensure subordinate commands undergo an external AT Program Review at least once every three years. The ultimate outcome of triennial AT Program Reviews is the identification of AT program deficiencies and vulnerabilities that may be exploited by terrorists. The AT Program Review teams should provide realistic solutions aimed at improving AT program implementation and risk mitigation strategies.

E3.31.5.1. Triennial AT Program Reviews may be conducted as an HHA or JSIVA. The DoD Components may use an HHA or JSIVA in lieu of an annual AT Program Review.

E3.31.5.2. In addition to providing an assessment of compliance with the standards prescribed in this Instruction, an HHA or JSIVA shall assess and evaluate the viability of a headquarters' AT policies, subordinate AT program implementation, the methodology for addressing resource shortfalls, inter-organization coordination, and synchronization of the AT program elements.

E3.31.6. Ensure that Combatant Commands, Services, and Defense Agencies undergo a Chairman of the Joint Chiefs of Staff -led Headquarters AT Program Review at least once every three years. These triennial reviews shall assess a commander's ability to administer AT Program responsibilities including support to subordinate commands and assess and evaluate the viability of AT policies, subordinate AT program implementation, the methodology for

addressing resource shortfalls, inter- and intra-organization coordination, and synchronization of the AT program elements.

E3.31.7. Ensure tenant commands and units are included in all comprehensive AT Program Reviews.

E3.32. DoD STANDARD 32: AT Program Review Teams. The Heads of the DoD Components shall:

E3.32.1. Develop AT Program Review Assessment Team guidelines for the conduct of AT Program Reviews. These guidelines shall be modeled upon the Defense Threat Reduction Agency Antiterrorism Vulnerability Assessment Team Guidelines (Reference (ag)) and include, at a minimum, compliance with the standards prescribed in this Instruction, accepted TTP, and best AT practices.

E3.32.2. Resource a sufficient number of AT Program Review Teams to execute the program review assessment requirements of the DoD Component concerned, and ensure AT Program Review teams comprise individuals with sufficient functional expertise (modeled upon the criteria established in Reference (ag)) to assess satisfactorily and evaluate the effectiveness and adequacy of AT Program implementation at the level (headquarters, unit, command, installation, activity, etc.) for which the AT Program Review is being conducted.

E4. ENCLOSURE 4

DoD FPCON

E4.1. INTRODUCTION

The DoD FPCON progressively increases protective measures implemented by the DoD Components in anticipation of or in response to the threat of terrorist attack. The FPCON is the principal means through which commanders apply an operational decision on how to best guard against the terrorist threat. These FPCON measures assist commanders in reducing the risks of terrorist attacks and other security threats to DoD personnel, units, and activities.

E4.2. FPCON

The DoD FPCON consists of five progressive levels of increasing AT protective measures. The implementing measures for each level are detailed in sections E4.4. and E4.5. The circumstances that apply and the purposes of each protective posture are as follows:

E4.2.1. FPCON NORMAL: Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DoD installations and facilities.

E4.2.2. FPCON ALPHA: Applies when there is an increased general threat of possible terrorist activity against personnel or facilities, and the nature and extent of the threat are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

E4.2.3. FPCON BRAVO: Applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.

E4.2.4. FPCON CHARLIE: Applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Prolonged implementation of CHARLIE measures may create hardship and affect the activities of the unit and its personnel.

E4.2.5. FPCON DELTA: Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

E4.3. FPCON PROCEDURES

E4.3.1. Site-specific AT measures, linked to an FPCON and physical security actions, shall be classified “CONFIDENTIAL.” When separated from the AT or Physical Security Plan, specific AT measures linked to an FPCON and site-specific FPCON levels may be downgraded to “FOR OFFICIAL USE ONLY” if appropriate.

E4.3.2. Upon declaration of an FPCON level, all listed security measures for that FPCON level are to be implemented immediately unless waived in writing by competent authority (see Reference (d) for guidelines). In non-DoD controlled facilities housing DoD occupants, DoD organization shall implement applicable FPCON security measures in space directly controlled by DoD to the extent possible. The supplementing RAM and command-unique or site-specific measures should also be implemented to complicate a terrorist group’s operational planning and targeting.

E4.3.3. Airfield-specific measures are for installations and facilities with a permanently functioning airfield. Installations and facilities with an emergency helicopter pad should review and implement any applicable airfield-specific measures when they anticipate air operations.

E4.3.4. Because of specific security requirements, shipboard measures are listed separately, beginning at section E4.5. The measures applying solely to U.S. Navy combatant ships are further identified throughout this section. The shipboard measures are tailored to assist commanding officers and ship masters in reducing the effect of terrorist and other security threats to DoD combatant and non-combatant vessels, including U.S. Army and Military Sealift Command ships worldwide.

E4.4. BASELINE FPCON LEVELS AND MEASURES

E4.4.1. FPCON NORMAL Measures

E4.4.1.1. Measure NORMAL 1: Secure and randomly inspect buildings, rooms, and storage areas not in regular use.

E4.4.1.2. Measure NORMAL 2: Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

E4.4.1.3. Measure NORMAL 3: Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

E4.4.1.4. Measure NORMAL 4: Identify defense critical assets (per E2.1.8.) and high-occupancy buildings (per E3.1.6.3.1.).

E4.4.2. FPCON ALPHA Measures

E4.4.2.1. Measure ALPHA 1: Continue, or introduce, all measures of the previous FPCON level.

E4.4.2.2. Measure ALPHA 2: At regular intervals, inform personnel and family members of the general situation. Ensure personnel arriving for duty are briefed on the threat. Also, remind them to be alert for and to report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

E4.4.2.3. Measure ALPHA 3: The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Plans should be in place to execute access control procedures. Key personnel required to implement security plans should be on-call and readily available.

E4.4.2.4. Measure ALPHA 4: Increase security spot checks of vehicles and persons entering installations or facilities under the jurisdiction of the United States.

E4.4.2.5. Measure ALPHA 5: Initiate food and water risk management procedures, brief personnel on food and water security procedures, and report any unusual activities.

E4.4.2.6. Measure ALPHA 6: Test mass notification system.

E4.4.2.7. Measure ALPHA 7: Review all plans, identify resource requirements, and be prepared to implement measures of the next higher FPCON level.

E4.4.2.8. Measure ALPHA 8: Review and, if necessary, implement security measures for high-risk personnel.

E4.4.2.9. Measure ALPHA 9: As appropriate, consult local authorities on the threat and mutual AT measures.

E4.4.2.10. Measure ALPHA 10: Review intelligence, CI, and operations dissemination procedures.

E4.4.2.11. Measure ALPHA 11: Review barrier plans.

E4.4.2.12. Measure ALPHA 12: Review all higher FPCON measures.

E4.4.3. FPCON BRAVO Measures

E4.4.3.1. Measure BRAVO 1: Fully implement all measures of lower FPCON levels.

E4.4.3.2. Measure BRAVO 2: Enforce control of entry onto facilities containing U.S. infrastructure critical to mission accomplishment, lucrative targets, or high-profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large IED (e.g., cargo vans, delivery vehicles) sufficient to cause catastrophic damage to property or loss of life.

E4.4.3.3. Measure BRAVO 3: Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings. Consider applying to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure; IED/Vehicle Borne IED threat; References (s) and (u), and available security measures. Consider centralized parking and implementation of barrier plans.

E4.4.3.4. Measure BRAVO 4: Secure and periodically inspect all buildings, rooms, and storage areas not in regular use.

E4.4.3.5. Measure BRAVO 5: At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

E4.4.3.6. Measure BRAVO 6: Implement mail-screening procedures to identify suspicious letters and parcels.

E4.4.3.7. Measure BRAVO 7: Randomly inspect commercial deliveries. Advise family members to check home deliveries.

E4.4.3.8. Measure BRAVO 8: Randomly inspect food and water for evidence of tampering or contamination before use by DoD personnel. Inspections should include delivery vehicles, storage areas, and storage containers.

E4.4.3.9. Measure BRAVO 9: Increase security measures and guard presence or initiate increased patrols and surveillance of DoD housing areas, schools, messes, on-base clubs, military treatment facilities, and similar high-occupancy targets to improve deterrence and defense, and to build confidence among staff and family members.

E4.4.3.10. Measure BRAVO 10: Implement plans to enhance off-installation security for DoD facilities. In areas with Threat Levels of Moderate, Significant, or High, coverage includes facilities (e.g., DoD schools and daycare centers) and transportation services and routes (e.g., bus routes) used by DoD employees and family members.

E4.4.3.11. Measure BRAVO 11: Inform local security committees of actions being taken.

E4.4.3.12. Measure BRAVO 12: Verify identity of visitors to the installation and randomly inspect their suitcases, parcels, and other containers.

E4.4.3.13. Measure BRAVO 13: Conduct random patrols to check vehicles, people, and buildings.

E4.4.3.14. Measure BRAVO 14: As necessary, implement additional security measures for HRP.

E4.4.3.15. Measure BRAVO 15: Place personnel required for implementing AT plans on call; commanders should exercise discretion in approving absences.

E4.4.3.16. Measure BRAVO 16: Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

E4.4.3.17. Measure BRAVO 17: As deemed appropriate, verify identity of personnel entering buildings.

E4.4.3.18. Measure BRAVO 18: Review status and adjust as appropriate operations security, communications security, and information security procedures.

E4.4.3.19. Measure BRAVO 19: (Airfield-specific) As appropriate, erect barriers and establish manned checkpoints at entrances to airfields. Ensure the identity of all individuals entering the airfield (flight line and support facilities) with no exceptions. Randomly inspect vehicles, briefcases, and packages entering the airfield.

E4.4.3.20. Measure BRAVO 20: (Airfield-specific) Coordinate plans to safeguard aircraft departure and approach flight paths with local authorities. Be prepared to activate contingency plans and issue detailed air traffic control procedures. As appropriate, take actions to mitigate the threat of surface-to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

E4.4.3.21. Measure BRAVO 21: Review all higher FPCON measures.

E4.4.4. FPCON CHARLIE Measures

E4.4.4.1. Measure CHARLIE 1: Fully implement all measures of lower FPCON levels.

E4.4.4.2. Measure CHARLIE 2: Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and any applicable Status of Forces Agreements (SOFA). Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

E4.4.4.3. Measure CHARLIE 3: Be prepared to react to requests for assistance from both local authorities and other installations in the region.

E4.4.4.4. Measure CHARLIE 4: Limit access points in order to enforce entry control. Randomly search vehicles.

E4.4.4.5. Measure CHARLIE 5: Ensure or verify the identity of all individuals entering food and water storage and distribution centers, use sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.

E4.4.4.6. Measure CHARLIE 6: Initiate contingency monitoring for chemical, biological, and radiological contamination as required. Suspend contractors and off-facility users from tapping into the facility water system. An alternate locally developed measure should be implemented when contractors are responsible for DoD water supplies or when water is provided by local (non-DoD) sources or agencies.

E4.4.4.7. Measure CHARLIE 7: Increase standoff from sensitive buildings based on the threat. Implement barrier plan to hinder vehicle-borne attack.

E4.4.4.8. Measure CHARLIE 8: Increase patrolling of the installation/facility/unit including waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions and persons outside the perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat. Coordinate with Transportation Security Administration, Marine Patrol, U.S. Coast Guard, and local law enforcement as required to cover off-facility approach and departure flight corridors.

E4.4.4.9. Measure CHARLIE 9: Protect all designated infrastructure critical to mission accomplishment. Give special attention to and coordinate with local authorities regarding infrastructure outside the military establishment.

E4.4.4.10. Measure CHARLIE 10: To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

E4.4.4.11. Measure CHARLIE 11: Randomly inspect suitcases, briefcases, packages being brought onto the installation through access control points and consider randomly searching them upon leaving the installation.

E4.4.4.12. Measure CHARLIE 12: Review personnel policy procedures to determine appropriate courses of action for dependent family members.

E4.4.4.13. Measure CHARLIE 13: Review access procedures for all non-U.S. personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flight line and support facilities.

E4.4.4.14. Measure CHARLIE 14: Consider escorting children to and from DoD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, etc.).

E4.4.4.15. Measure CHARLIE 15: (Airfield-specific) Reduce flying to only essential operational flights. Implement appropriate flying countermeasures as directed by the Flight Wing Commander (military aircraft) or Transportation Security Administration (civilian aircraft). Consider relief landing ground actions to take for aircraft diversions into and out of an attacked airfield. Consider augmenting fire-fighting details.

E4.4.4.16. Measure CHARLIE 16: Review all FPCON DELTA measures.

E4.4.5. FPCON DELTA Measures

E4.4.5.1. Measure DELTA 1: Fully implement all measures of lower FPCON levels.

E4.4.5.2. Measure DELTA 2: Augment guards as necessary.

E4.4.5.3. Measure DELTA 3: Identify all vehicles within operational or mission support areas.

E4.4.5.4. Measure DELTA 4: Search all vehicles and their contents before allowing entrance to the installation. Selected pre-screened and constantly secured vehicles used to transport escorted very important personnel may be exempted.

E4.4.5.5. Measure DELTA 5: Control facility access and implement positive identification of all personnel with no exceptions.

E4.4.5.6. Measure DELTA 6: Search all personally carried items (e.g., suitcases, briefcases, packages, backpacks) brought into the installation or facility.

E4.4.5.7. Measure DELTA 7: Close DoD schools.

E4.4.5.8. Measure DELTA 8: Make frequent checks of the exterior of buildings and of parking areas.

E4.4.5.9. Measure DELTA 9: Restrict all non-essential movement.

E4.4.5.10. Measure DELTA 10: (Airfield specific) Cease all flying except for specifically authorized operational sorties. Be prepared to deploy light aircraft and/or helicopters for surveillance tasks or to move internal security forces. Implement, if necessary, appropriate flying countermeasures.

E4.4.5.11. Measure DELTA 11: (Airfield specific) As appropriate, airfields should prepare to accept aircraft diverted from other stations.

E4.4.5.12. Measure DELTA 12: If permitted, close public and military roads and facilities. If applicable, close military roads allowing access to the airfield.

E4.4.5.13. Measure DELTA 13: Begin continuous monitoring for chemical, biological, and radiological contamination.

E4.5. SHIPBOARD FPCON LEVELS AND MEASURES

E4.5.1. FPCON NORMAL Measures

E4.5.1.1. Measure NORMAL 1: Brief crew on the port-specific threat, the AT and security plans, and security precautions to be taken while ashore. Ensure all hands are knowledgeable of FPCON requirements and that they understand their role in implementation of these measures.

E4.5.1.2. Measure NORMAL 2: Remind all personnel to be suspicious and inquisitive of strangers, be alert for abandoned parcels or suitcases and for unattended vehicles in the vicinity. Report unusual activities to the Officer of the Deck, Master or Mate on watch, as applicable.

E4.5.1.3. Measure NORMAL 3: Secure and periodically inspect spaces not in use.

E4.5.1.4. Measure NORMAL 4: Review security plans and keep them available.

E4.5.1.5. Measure NORMAL 5: Review pier and shipboard access control procedures including land and water barriers.

E4.5.1.6. Measure NORMAL 6: Ensure sentries, Mate on Watch, roving patrols, the quarterdeck watch, and gangway watch have the ability to communicate with one another.

E4.5.1.7. Measure NORMAL 7: Coordinate pier and fleet landing security requirements with collocated forces, and/or husbanding agent. Identify anticipated needs for mutual support and define methods of implementation and communication.

E4.5.2. FPCON ALPHA Measures

E4.5.2.1. Measure ALPHA 1: Muster, arm, and brief security personnel on the threat and rules of engagement. Keep key personnel who may be needed to implement security measures on call.

E4.5.2.2. Measure ALPHA 2: U.S. Navy combatant ships when in a non-U.S. Navy controlled port, deploy barriers to keep vehicles away from the ship if possible (100 feet in U.S. ports and 400 feet outside the United States as the minimum standoff distances). DoD non-combatant ships in a non-U.S. Government controlled port, request husbanding agents to arrange and deploy barriers to keep vehicles away from the ship (100 feet in U.S. ports and 400 feet outside the United States as the minimum standoff distances).

E4.5.2.3. Measure ALPHA 3: (U.S. Navy combatant ship-specific) Randomly inspect vehicles entering pier.

E4.5.2.4. Measure ALPHA 4: Randomly inspect hand-carried items and packages before they are brought aboard.

E4.5.2.5. Measure ALPHA 5: Regulate shipboard lighting as appropriate to the threat environment.

E4.5.2.6. Measure ALPHA 6: When in a non-U.S. Government controlled port, rig hawse pipe covers and rat guards on lines, cables, and hoses. Consider using an anchor collar.

E4.5.2.7. Measure ALPHA 7: When in a non-U.S. Government controlled port, raise accommodation ladders and stern gates when not in use.

E4.5.2.8. Measure ALPHA 8: Increase frequency of security drills.

E4.5.2.9. Measure ALPHA 9: Establish internal and external communications, including connectivity checks with the local operational commander, agencies, and authorities that are expected to provide support, if required.

E4.5.2.10. Measure ALPHA 10: Establish procedures for screening food, mail, water, and other supplies and equipment entering the ship.

E4.5.3. FPCON BRAVO Measures

E4.5.3.1. Measure BRAVO 1: Continue or introduce all measures of lower FPCON level.

E4.5.3.2. Measure BRAVO 2: Set Material Condition YOKE (secure all watertight door and hatches), main deck and below.

E4.5.3.3. Measure BRAVO 3: Consistent with local rules, regulations, and/or any applicable SOFA, U.S. Navy combatant ships post armed pier sentries as necessary and non-combatant ships post pier sentries (armed at the Master's discretion) as necessary.

E4.5.3.4. Measure BRAVO 4: Restrict vehicle access to the pier. Discontinue parking on the pier. Consistent with local rules, regulations, and/or any applicable SOFA, establish unloading zones and move all containers as far away from the ship as possible (100 feet in the United States, 400 feet outside the United States as the minimum stand-off distance).

E4.5.3.5. Measure BRAVO 5: Consistent with the local rules, regulations, and/or any applicable SOFA, U.S. Navy combatant ships post additional armed watches as necessary and non-combatant ships post additional watches (armed at the Master's discretion) as necessary. Local threat, environment, and fields of fire should be considered when selecting weapons.

E4.5.3.6. Measure BRAVO 6: Post signs in local language to establish visiting and loitering restrictions.

E4.5.3.7. Measure BRAVO 7: When in a non-U.S. Government controlled port, identify and randomly inspect authorized watercraft, such as workboats, ferries, and commercially rented liberty launches, daily.

E4.5.3.8. Measure BRAVO 8: When in a non-U.S. Government controlled port, direct liberty boats to make a security tour around the ship upon departing from and arriving at the ship, with particular focus on the waterline and under pilings when berthed at a pier.

E4.5.3.9. Measure BRAVO 9: Before allowing visitors aboard, inspect all their hand-carried items and packages. Where available, use baggage scanners and walk-through or hand-held metal detectors to screen visitors and their packages prior to boarding the ship.

E4.5.3.10. Measure BRAVO 10: Implement measures to keep unauthorized craft away from the ship. Authorized craft should be carefully controlled. Coordinate with host-nation's husbanding agent or local port authority, as necessary, and request their assistance in controlling unauthorized craft.

E4.5.3.11. Measure BRAVO 11: Raise accommodation ladders, etc., when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.

E4.5.3.12. Measure BRAVO 12: Review liberty policy in light of the threat and revise it as necessary to maintain safety and security of ship and crew.

E4.5.3.13. Measure BRAVO 13: U.S. Navy combatant ships conduct division quarters at foul weather parade. All DoD ships avoid conducting activities that involve gathering a large number of crewmembers at the weatherdecks. Where possible, relocate such activities inside the skin of the ship.

E4.5.3.14. Measure BRAVO 14: Ensure an up-to-date list of bilingual personnel for the area of operations is readily available. Maintain warning tape, in both the local language and English, in the bridge, pilot house, or quarterdeck, for use on the ship's announcing system to warn small craft to remain clear.

E4.5.3.15. Measure BRAVO 15: If they are not already armed, arm the quarterdeck, gangway or mate on watch.

E4.5.3.16. Measure BRAVO 16: If they are not already armed, consider arming the sounding and security patrol.

E4.5.3.17. Measure BRAVO 17: Review procedures for expedient issue of firearms and ammunition to the shipboard security reaction force (SRF) and other members of the crew, as deemed necessary by the commanding officer/master.

E4.5.3.18. Measure BRAVO 18: Instruct watches to conduct frequent, random searches of the pier, including pilings and access points.

E4.5.3.19. Measure BRAVO 19: Conduct visual inspections of the ship's hull and ship's boats at intermittent intervals and immediately before it is put to sea using both landside personnel and waterside patrols.

E4.5.3.20. Measure BRAVO 20: Hoist ship's boats aboard when not in use.

E4.5.3.21. Measure BRAVO 21: Terminate all public visits. In U.S. Government controlled ports, host visits (family, friends, small groups sponsored by the ship) may continue at the commanding officer's/master's discretion.

E4.5.3.22. Measure BRAVO 22: After working hours, reduce entry points to the ship's interior by securing infrequently used entrances. Safety requirements must be considered.

E4.5.3.23. Measure BRAVO 23: In non-U.S. Government-controlled ports, use only one brow/gangway to access the ship (remove any excess brows/gangways). Aircraft carriers and other large decks may use two as required, when included in an approved AT Plan specific to that port visit.

E4.5.3.24. Measure BRAVO 24: In non-U.S. Government-controlled ports, maintain the capability to get underway on short notice or as specified by standard operating procedures.

E4.5.3.25. Measure BRAVO 25: In non-U.S. Government-controlled ports, consider the layout of fire hoses. Brief designated crew personnel on procedures for repelling boarders, small boats and ultra-light aircraft.

E4.5.3.26. Measure BRAVO 26: Where applicable, obstruct possible helicopter landing areas.

E4.5.3.27. Measure BRAVO 27: Where possible, monitor local communications (ship-to-ship, TV, radio, police scanners).

E4.5.3.28. Measure BRAVO 28: As appropriate, inform local authorities of actions being taken as FPCON increases.

E4.5.3.29. Measure BRAVO 29: (U.S. Navy combatant ship-specific) If the threat situation warrants, deploy picket boats to conduct patrols in the immediate vicinity of the ship. Brief boat crews and arm them with appropriate weapons considering the threat, the local environment, and fields of fire.

E4.5.4. FPCON CHARLIE Measures

E4.5.4.1. Measure CHARLIE 1: Continue or introduce all measures of lower FPCON levels.

E4.5.4.2. Measure CHARLIE 2: Consider setting Material Condition Zebra (secure all access doors and hatches), main deck and below.

E4.5.4.3. Measure CHARLIE 3: Cancel liberty. Execute emergency recall.

E4.5.4.4. Measure CHARLIE 4: Prepare to get underway on short notice. If conditions warrant, request permission to sortie/get underway.

E4.5.4.5. Measure CHARLIE 5: Block unnecessary vehicle access to the pier.

E4.5.4.6. Measure CHARLIE 6: Coordinate with host-nation husbanding agent and/or local port authorities to establish a small boat exclusion zone around ship.

E4.5.4.7. Measure CHARLIE 7: (U.S. Navy combatant ship-specific) Deploy the SRF to protect command structure and augment posted watches. Station the SSDF to provide 360-degree coverage of the ship.

E4.5.4.8. Measure CHARLIE 8: Energize radar and/or sonar, rotate screws, and cycle rudder(s) at frequent and irregular intervals, as needed to assist in deterring, detecting, or thwarting attacks.

E4.5.4.9. Measure CHARLIE 9: Consider staffing repair locker(s). Be prepared to staff one repair locker on short notice. Ensure adequate lines of communications are established with damage control central.

E4.5.4.10. Measure CHARLIE 10: (U.S. Navy combatant ship-specific) If available and feasible, consider use of airborne assets as an observation/FP platform.

E4.5.4.11. Measure CHARLIE 11: If a threat of swimmer attack exists, activate an anti-swimmer watch.

E4.5.4.12. Measure CHARLIE 12: In non-U.S. Government-controlled ports and if unable to get underway, consider requesting armed security augmentation from area Combatant Commander.

E4.5.5. FPCON DELTA Measures

E4.5.5.1. Measure DELTA 1: Fully implement all measures of lower FPCON levels.

E4.5.5.2. Measure DELTA 2: Permit only necessary personnel topside.

E4.5.5.3. Measure DELTA 3: If possible, cancel port visit and get underway.

E4.5.5.4. Measure DELTA 4: Employ all necessary weapons to defend against attack.