Army Regulation 525–13

Military Operations

Antiterrorism

Distribution Restriction Statement.
This regulation contains operational information for official Government use only; thus distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this regulation under the Freedom of Information Act or Foreign Military Sales Program must be made to HQDA (DAPM–MPO–AT), Office of the Provost Marshal General, 2800 Army Pentagon, Washington, DC 20310–2800.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Headquarters
Department of the Army
Washington, DC
3 December 2019

SUMMARY of CHANGE

AR 525–13
Antiterrorism

This expedited revision, dated 3 December 2019—

- Adds records management requirements (para 1–5).
- Updates responsibilities (paras 2–2*b*, 2–3, 2–5, 2–10*a*, 2–10*b*, 2–12*d*, 2–13, 2–14*a*, 2–22*b*(9), 2–24*a*, 2–24*e*, 2–25*a*, and 2–26*e*).
- Replaces Second Army/U.S. Army Network Enterprise Technology Command with Army Cyber (paras 2–22*b*(2) and 2–22*b*(3)).
- Adds responsibilities for the Commander, U.S. Army Intelligence and Security Command (para 2–23).
- Requires commanders to ensure appropriate antiterrorism training and awareness requirements for inclusion in all contracts requiring an antiterrorism/operation security cover sheet (para 3–6*e*).
- Requires contractors to coordinate with their Army service component command to obtain, and comply with, the combatant command's specific antiterrorism guidance for the area in which they are located (para 3–6*e*).
- Removes Standard 35: Core vulnerability assessment management program (formerly para 5–36 and table E–1 (last line)).
- Requires the designated Army service component commands and the Commander, U.S. Army Criminal Investigation Command to develop their annual threat to the Army assessment submissions in accordance with standard operating procedures (para 5–5*b*(2)(*h*)).
- Requires commanders to establish an antiterrorism criticality assessment process as part of their responsibilities for synchronizing and integrating Army priorities and initiatives across their command (para 5–6*a*).
- Updates the requirement to record vulnerability assessment data in the Department of Defense System of Record (paras 5–7*b*(3), 5–7*b*(4), 5–7*b*(6), H–4*f*(9), and H–4*f*(10)).
- Adds potential insider threats to the list of areas that antiterrorism plans will address (para 5–8*b*(3)(*e*)).
- Adds the requirement to review the antiterrorism plan at least annually (para 5–8*b*(4)).
- Adds the requirement to coordinate and synchronize antiterrorism plans with other protection plans (para 5–9*b*(1)(*c*)).
- Permits the Antiterrorism Working Group to be consolidated into an organization's Protection Working Group (para 5–11*b*(2)).
- Allows the execution of the antiterrorism executive-level committee as part of the command's protection executive committee (para 5–13*a*).
- Requires commanders to use an antiterrorism cover sheet to ensure that assistance agreements, cooperative agreements, grants, and technology investment agreements include the requisite antiterrorism related protections (para 5–19*b*(1)).

- Requires antiterrorism incident response measures be incorporated into command installation response and recovery plans (para 5–21*a*).
- Mandates that antiterrorism planning considerations for stand-alone facilities be included in the emergency action plan (para 5–22*b*(5)).
- Updates Standard 22, Force protection condition system (para 5–23).
- Requires all new-hire Army Civilian and (as appropriate), contractor personnel, in accordance with contract requirements, receive Antiterrorism Level I Awareness training by a certified Level II trained antiterrorism officer (para 5–26*b*(4)(*b*)).
- Mandates the use of the Digital Training Management System to record and track Antiterrorism Level I: Awareness training (para 5–26*b*(4)(*e*)).
- Updates Standard 33: Incorporation of antiterrorism into command information programs (para 5–34*b*(2)(*a*)).
- Updates force protection conditions and threat levels (app B).
- Updates web links (paras C–1*c*, C–2*c*, and C–4*d*(7)(*b*)1).
- Updates questions regarding Standard 6 (paras H–4*f*(1) and H–4*f*(2)).
- Removes questions regarding Standard 35 (formerly para H–4*ii*).
- Changes Assistant Chief of Staff for Installation Management to Deputy Chief of Staff, G–9 (throughout).

Headquarters
Department of the Army
Washington, DC
3 December 2019

*Army Regulation 525–13

Effective 3 January 2020

Military Operations

Antiterrorism

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is an expedited revision. The portions affected by this expedited revision are listed in the summary of change.

Summary. This regulation prescribes policy and procedures and assigns responsibilities for the Army Antiterrorism Program. This program implements DODI 2000.12 and DODI O–2000.16, Volume 1 and Volume 2 and provides guidance and mandatory standards for protecting Department of the Army personnel, information, and critical resources from acts of terrorism.

Applicability. This regulation applies to the Regular Army, Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. Also, it is applicable to civil works projects. During mobilization, the proponent may modify chapters and policies contained in this regulation.

Proponent and exception authority. The proponent of this regulation is the Provost Marshal General. The proponent has the authority to approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see appendix H).

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Provost Marshal General (DAPM–MPO–AT), 2800 Army Pentagon, Washington, DC 20310–2800.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Office of the Provost Marshal General (DAPM–MPO–AT), 2800 Army Pentagon, Washington, DC 20310–2800 or email usarmy.pentagon.hqda.list.aoc-at-division@mail.mil.

Committee management. AR 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the Office of the Administrative Assistant to the Secretary of the Army, Department of the Army Committee Management Office (AARP–ZA), 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5527 (email to usarmy.pentagon.hqda-oaar-rpa.mbx.committee-management@mail.mil). Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, as found in the AR 15–1, then the proponent will follow all AR 15–1 requirements for establishing and continuing the group as a committee.

Distribution. This publication is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve. Requests from outside the U.S. Government for release of this regulation under the Freedom of Information Act or Foreign Military Sales Program must be made to the Provost Marshal General (DAPM–MPO–AT), 2800 Army Pentagon, Washington, DC 20310–2800 or email to usarmy.pentagon.hqda.list.aoc-at-branch@mail.mil.

Distribution Restriction Statement.
This regulation contains operational information for official Government use only; thus distribution is limited to U.S. Government agencies. Requests from outside the U.S. Government for release of this regulation under the Freedom of Information Act or Foreign Military Sales Program must be made to HQDA (DAPM–MPO–AT), Office of the Provost Marshal General, 2800 Army Pentagon, Washington, DC 20310–2800.

Destruction Notice.
Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Contents (Listed by paragraph and page number)

*This regulation supersedes AR 525–13, dated 17 February 2017.

Contents—Continued

Contents—Continued

Appendixes

Contents—Continued

Table List

Glossary

Chapter 1
Introduction and Policies

1–1. Purpose
This regulation establishes the Army Antiterrorism (AT) Program to protect personnel (Soldiers, members of other Services, Department of the Army (DA) Civilian employees, Department of Defense (DOD) contractors and Family members of DOD employees), information, property, and facilities (including civil work and like projects) in all locations and situations against terrorism. It provides—

a. Department of the Army AT tasks.
b. Department of the Army AT standards.
c. Implementing guidance for the execution of the AT standards.
d. Policies, procedures, and responsibilities for execution of the AT Program.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See glossary.

1–4. Responsibilities
Responsibilities are listed in chapter 2.

1–5. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule-Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

1–6. Statutory authority
Statutory authority for this regulation is derived from Section 3013, Title 10, United States Code (10 USC 3013).

Chapter 2
Responsibilities

2–1. Assistant Secretary of the Army (Acquisition, Logistics and Technology)
The ASA (ALT) will—

a. Establish policies that require Army contracting officers, in coordination with Army commanders, to develop procedures that ensure AT measures are incorporated into contracting actions (requirements development, source selection/award, and contract execution) when the provisions of the contract or services provided affect the security of DOD elements, personnel, or mission-essential cargo, equipment, assets or services.

b. Ensure policy for statements of work include the AT and operations security (OPSEC) cover sheet, incorporating necessary AT measures into the contracting process as specified in paragraph 5–19 (Standard 18).

2–2. Assistant Secretary of the Army (Installation, Energy and Environment)
The ASA (IE&E) will—

a. As necessary, provide supervision and waiver authority for AT related military construction requirements contained in Unified Facilities Criteria (UFC) 4–010–01 and UFC 4–010–02.

b. In conjunction with Deputy Chief of Staff, G–9 (DCS, G–9), program for AT mission support as part of the program objective memorandum.

2–3. Assistant Secretary of the Army (Manpower and Reserve Affairs)

The ASA (M&RA), will provide oversight of AT policy through the Army Protection Program (APP). Ensure policy on non-appropriated funds statements of work include the AT and OPSEC cover sheet to ensure that necessary AT-related measures are included in subsequent contracts.

2–4. Chief Information Officer/G–6

The CIO/G–6 will, in coordination with the U.S. Army Cyber Command (ARCYBER), monitor communication, coordination, and information sharing in the execution of missions and functions in support of the Army's AT Program.

2–5. The Inspector General

TIG consider adding AT as an item of interest on all Headquarters, Department of the Army (HQDA) level inspections.

2–6. Chief, Public Affairs

The CPA will provide guidance to Army commands (ACOMs), Army service component command (ASCCs), and direct reporting units (DRUs) for the development and execution of command information and public information programs in support of AT efforts.

2–7. Chief of Staff, Army

The General Officer Management Office (GOMO) will establish procedures to ensure Army General Officers who are designated as high-risk personnel (HRP), in accordance with paragraph 5–17 (Standard 16), are programmed to attend the required individual AT Awareness training prior to reporting to such positions.

2–8. Deputy Chief of Staff, G–1

The DCS, G–1 will—

a. Ensure AT policies and procedures are incorporated in personnel management functions and official and unofficial personal travel guidance, to include Army policies governing permanent change of station (PCS), temporary duty (TDY) outside continental United States (OCONUS), leave OCONUS, and documentation of required AT training.

b. Establish procedures to ensure Army personnel (O–6 and below) who will be designated as HRP in accordance with paragraph 5–17 (Standard 16) are programmed to attend the required individual AT Awareness training prior to reporting to such positions.

c. Establish procedures to ensure assignment orders delineate special instructions for training in accordance with this regulation and DODI O–2000.16 prior to assignment to the gaining command.

2–9. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Act as the principal staff proponent and develop policy, procedures, and programming for Army counterintelligence (CI) and human intelligence collection, reporting, production, and dissemination of information regarding the international terrorist threat to the Army.

b. In coordination with the DCS, G–3/5/7 provide intelligence personnel to support operation of the Army Threat Integration Center (ARTIC).

c. Provide Army intelligence resource requirements related to terrorism to the National Intelligence Program and the Military Intelligence (MI) Program.

d. Provide policy, programming, and resources for the detailing of Army CI personnel to the Federal Bureau of Investigation (FBI) National Joint Terrorism Task Force and regional Joint Terrorism Task Forces in the continental United States (CONUS) to leverage opportunities to identify international terrorist information which may pose a threat to Army and DOD.

e. Provide policy implementation, programming, and resources for assignment of CI personnel to DOD force protection (FP) detachments OCONUS for the purpose of detecting and warning of terrorism and FP related threats to DOD organizations and personnel in transit at or through overseas locations.

f. Represent the Army in matters related to intelligence support to AT in the national and defense intelligence communities.

g. Provide policy implementation, programming, and resources for the training of Army personnel on Threat Awareness and Reporting Program (TARP) and the receipt of reports generated under the provisions of AR 381–12.

h. Coordinate with the Army G–34 on antiterrorism aspects of insider threat program management.

i. Co-chair the Insider Threat Working Group (TWG).

2–10. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 is responsible for the security of the Army and provides overall policy guidance, staff supervision, and coordination and has overall general staff responsibility for the APP that includes AT. The DCS, G–3/5/7 will—

a. Assist and support the ASA (M&RA) in developing and executing protection-related Army strategies, policies, and plans; executing and ensuring the execution of policies, plans, and programs by HQDA principal officials and organizations; and reviewing and assessing the execution of policies, plans, and programs through the APP which includes AT.

b. Coordinate and conduct APP assessments of the ACOMs, ASCCs, and DRUs triennially in coordination with HQDA subject matter experts from the APP functional elements, including AT per AR 525–2.

2–11. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Develop policy and procedures that direct the incorporation of AT measures into the logistics and contracting actions (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. These policies and procedures will include the requirements specified in paragraph 5–19 (Standard 18).

b. Provide oversight and assessment of the logistical and contracting process to ensure the incorporation of AT measures specified in this regulation.

c. Provide technical personnel support to the DCS, G–3/5/7 designated assessment teams, as required.

2–12. Deputy Chief of Staff, G–9

The DCS, G–9 will—

a. Mandate compliance with the Unified Facilities Code (UFC) 4–010–01 and UFC 4–010–02 relative to the construction of new facilities and major renovation projects (when any of the applicable requirements are triggered) in support of the Army's AT Program.

b. Act as the HQDA office of primary responsibility concerning the processing and coordination of all Army waivers and exceptions to the requirements contained in UFC 4–010–01 and UFC 4–010–02.

c. Provide administrative and technical advice and assistance and make recommendations concerning AT real property matters as requested by ACOMs, ASCCs, and DRUs to the Secretary of the Army; the Chief of Staff, Army; and HQDA staff agencies.

d. In conjunction with ASA (IE&E) program for AT mission support as part of the program objective memorandum.

2–13. The Surgeon General

TSG will—

a. Consider the use of weapons of mass destruction (WMD) when establishing policy and procedures for casualty treatment and preventive medicine procedures.

b. Consider medical threat data when establishing policy for preventive medicine procedures. Synchronize preventive medicine threat procedures with command's emergency management planning.

c. Conduct risk assessments on medical functions and facilities.

d. Provide formal Army policy on the installation food vulnerability assessment (IFVA) program.

e. Provide technical support and guidance for IFVA assessments and food and water defense at the installation level as well as in geographical areas of responsibility for subsistence.

f. Support installation AT working groups with technical assistance on animal medicine issues and requirements and procedures for implementing IFVA and reporting results.

g. Coordinate with the Provost Marshal General (PMG) to ensure IFVA risk management processes are incorporated into the terrorism vulnerability assessments and AT working group requirements contained in paragraph 5–11.

2–14. The Provost Marshal General

The PMG in direct support to the DCS, G–3/5/7 in the management and execution of the Army AT mission will—

a. Provide an AT division that—

(1) Serves as the functional proponent for AT and establish Army AT policy and objectives; coordinates and evaluates policies and procedures consistent with DOD directives and AR 525–2; and provides resources.

(2) In support of the DCS, G–3/5/7, develops updates to the Army AT Strategic Plan with assigned objectives to sustain improvement of the Army AT Program.

(3) Establishes an AT Strategic Plan with assigned objectives to maintain improvement of the Army AT Program. The Army AT Strategic Plan will be updated on an annual basis.

(4) Integrates and synchronizes all AT elements and enablers with the assistance of proponent HQDA staff sections, ACOMs, ASCCs, DRUs, and other intelligence, security and law enforcement agencies, as appropriate.

(5) Evaluates the Army posture and the effectiveness of Army AT Programs annually, and provides guidance and assistances, as required.

(6) Validates and prioritizes all requirements for staffing and administering Army AT Program functions. Tracks resource execution.

(7) Develops policy for the development of AT doctrine and training.

(8) Reviews AT doctrine and training to ensure conformity with national, DOD, and Army AT policy and guidance.

(9) Reviews requests for specialized AT training (for example, HRP, evasive driving) to ensure allocation of school quotas supports AT operational requirements.

(10) Monitors and reports worldwide force protection conditions (FPCONs).

(11) Reviews requests for UFC waivers and exceptions in accordance with appendix F.

(12) Oversees Army AT training and doctrine and conducts periodic evaluations to ensure appropriate evolution, matching current and anticipated trends.

(13) Provides coordination on all waivers and exceptions to requirements contained in paragraphs 2–9*a* and 2–9*b*.

b. Operate an ARTIC in close coordination with the Office of the DCS, G–2. The ARTIC will—

(1) Issue early warning of criminal and terrorist threats to Army ACOMs, ASCCs, DRUs, and other senior Army leaders and organizations.

(2) Coordinate the analysis and reporting of terrorist-related intelligence with appropriate intelligence and law enforcement agencies in order to provide warning and maintain visibility of threats to ACOMs, ASCCs, and DRUs, the senior Army leadership, and threatened installations, activities, facilities, and personnel.

(3) Fuse criminal and terrorist threat information to form a single threat picture.

(4) Assess the terrorist and criminal threats to Army forces and publish an annual comprehensive DA threat statement and daily DA FP memorandum, to disseminate potential and future threats, thereby enhancing threat awareness at all levels.

(5) Publish DA AT travel advisories, as required, to inform commanders of DOD-designated HIGH or SIGNIFICANT threat level countries, high crime rate cities, and Department of State (DOS) travel advisories.

c. Ensure the Commander, U.S. Army Criminal Investigation Command (USACIDC)—

(1) Collects, analyzes, and disseminates to affected commands criminal intelligence pertaining to threat activities, within the provisions of applicable statutes and regulations.

(2) Maintains a capability to analyze and disseminate collected, time-sensitive information concerning the criminal threat against Army interests.

(3) Provides appropriate threat-related criminal intelligence to HQDA (ARTIC), U.S. Army Intelligence and Security Command (INSCOM), and the Army Counterintelligence Center (ACIC).

(4) Investigates threat incidents of Army interest. Monitors the conduct of such investigations when conducted by civilian, host nations (HNs), military, or other police agencies. Provides applicable results of terrorist-related investigations to HQDA (ARTIC), ACIC, and the Center for Army Lessons Learned (CALL).

(5) Provides trained hostage negotiators to support Army AT operations worldwide.

(6) Plans and coordinates the protection of high-risk personnel for DOD, DA, and foreign officials as directed by HQDA.

(7) Serves as the Army's primary liaison representative to Federal, State, and local law enforcement agencies and host country agencies to exchange criminal intelligence.

(8) Establishes procedures to ensure appropriate liaison at all levels between USACIDC, INSCOM, and provost marshal/security officer (PM/SO) elements operating in support of the AT Program.

(9) Immediately notifies the affected installation PM/SO, the installation’s higher headquarters, and HQDA (in accordance with app C) upon receipt of time-sensitive threat information.

(10) Performs criminal activity threat assessments and personal security vulnerability assessments for Army personnel, installations, systems, operations, and other interests as directed by HQDA and/or based on Army commanders' operational requirements.

(11) Provides technical personnel support to DCS, G–3/5/7 designated assessment teams, as required.

(12) Investigates all incidents of suspected domestic terrorism as criminal acts, to include the safeguarding of evidence, collection of statements, preparation of investigative reports, and presentation to appropriate judicial officials. Investigations will be conducted jointly with Federal, State, local, and foreign law enforcement agencies, as appropriate.

(13) Provides appropriate terrorism analysis and threat assessments to the ARTIC in support of Army requirements and the AT Program.

(14) Ensures sufficient USACIDC criminal intelligence capability to monitor and report on activities, intentions, and capabilities of domestic threat groups in accordance with applicable regulations and directives.

2–15. The Chief, National Guard Bureau

The CNGB will—

a. Publish guidance to all State Adjutants General concerning implementation of the AT Program, including all mandated Army AT standards.

b. Coordinate resource requirements for staffing and administering AT Program functions in the Army National Guard (ARNG).

c. Evaluate the AT posture and effectiveness of ARNG AT Programs in accordance with Army AT standards and provide guidance and assistance, as required.

d. Ensure funds are programmed/budgeted and ARNG personnel are identified for attendance at specialized AT training.

e. Ensure AT design measures have been considered and included, as appropriate, in ARNG construction projects.

f. Establish procedures for reporting FPCON changes implemented by ARNG units, facilities, and activities to the ARTIC. Ensure compliance by State Adjutants General with FPCON reporting procedures.

g. Ensure all ARNG Soldiers receive TARP and AT Level I Awareness training annually and prior to deployment.

h. Establish procedures for dissemination of threat information to ARNG units, facilities, and activities.

i. Establish procedures for submission of required reports in accordance with appendix C.

j. Coordinate with State Adjutants General to publish and disseminate guidance for all subordinate commands concerning implementation of the AT Program (including all mandated Army AT standards), to include state specific guidance concerning implementation of FPCON measures outlined in appendix B.

k. Ensure appointment of state command AT officers and establishment of state AT executive committees, AT working groups, and TWGs in accordance with paragraphs 5–10 (AT Standard 9), 5–11 (AT Standard 10), 5–12 (AT Standard 11), and 5–13 (AT Standard 12).

l. Establish procedures to ensure all ARNG units (battalion-level and above) have a Level II trained/certified antiterrorism officer (ATO).

2–16. Chief, Army Reserve

The CAR will—

a. Ensure appropriate coordination of resource requirements for staffing and administering AT Program functions in the U. S. Army Reserve (USAR).

b. Ensure evaluation of the AT posture and effectiveness of AT Programs in the USAR in accordance with Army AT standards and provide guidance and assistance, as required.

c. Ensure program/budget of funds and identification of USAR personnel for attendance at required AT training.

d. Ensure procedures are established for reporting FPCON changes implemented by USAR units, facilities, and activities to the Army Operations Center (AOC).

e. Ensure procedures are established for dissemination of threat information to USAR units, facilities, and activities.

f. Ensure procedures are established for submission of required reports in accordance with appendix C.

g. Ensure all USAR Soldiers receive TARP and AT Level I Awareness training annually and prior to deployment.

h. Publish guidance concerning USAR implementation of the AT Program, including all mandated Army AT standards.

i. Provide review and construction oversight of all AT design measures related to Military Construction, Army Reserve projects and ensure compliance with the UFC relative to the construction of new facilities and major renovation projects (when any of the applicable requirements are triggered) in support of the Army's AT Program.

2–17. Commander, U.S. Army Training and Doctrine Command

The Commander, TRADOC will—

a. Develop, implement, and continually update, based on lessons learned from recent threat incidents, appropriate training programs for AT, to include—

(1) Integration of AT training into all officer and noncommissioned officer professional military education and appropriate civilian management professional development courses to ensure the long-term development of knowledge and skills.

(2) Providing Level I Awareness training for all Soldiers undergoing initial entry training that familiarizes them with individual protective measures and other precautions to protect personnel, Family members, facilities, units, and equipment from terrorist attacks in accordance with paragraph 5–26 (AT Standard 25) and appendix D.

(3) Specialized training for personnel assigned to operations, MI, criminal investigation, and PM staff sections that have significant AT responsibilities. This includes personnel responsible for the following: protection of HRP; security of Army installations, facilities, and activities; threat assessment, AT plans, protection of personnel and units traveling or deployed; threat use of WMD; security of information; and investigation of terrorist attacks.

b. Develop AT training requirements in accordance with paragraphs 5–25 (AT Standard 24), 5–26 (AT Standard 25), 5–27 (AT Standard 26), 5–28 (AT Standard 27), and appendix D.

c. Develop individual and collective AT training.

d. Staff and resource the Army specified proponent for AT doctrine and training, the U.S. Army Military Police School (USAMPS) in accordance with AR 5–22 to coordinate programs within the TRADOC and HQDA.

e. Assist U.S. Army Special Operations Command (USASOC) in the development of doctrine and training supporting execution of AT operations unique to Army Special Operations Forces.

f. Develop AT doctrine, tactics, techniques, and procedures (TTP).

g. Collect information on evolving AT training, tactics, and procedures, as well as analyze and maintain a repository of lessons learned from past terrorist-related incidents in accordance with the CALL.

h. Ensure all personnel attending resident schooling receive required AT Awareness training in accordance with paragraph 5–26 (AT Standard 25) and appendix D prior to departure to gaining command.

i. Ensure that Level III AT training (O–5 and O–6 level commanders or civilian equivalent positions) is incorporated into the curriculum and taught at the Army pre-command courses (PCC) conducted at branch, component, and functional schools.

j. Develop and execute training for prospective drill sergeants, preparing them to teach face-to-face AT Level 1 Training in basic combat training.

2–18. Commander, U.S. Army Materiel Command

The Commander, AMC will—

a. Monitor research, development, and technology program of the Research, Development and Engineering Command in support of emergency response forces and ensure complete integration of technology and responders.

b. Provide chemical/biological analysis and assessments in response to Headquarters, DA and ACOM, ASCC, and DRU requirements.

c. Provide technical personnel support to DCS, G–3/5/7 designated assessment teams, as required.

d. Provide operational oversight and assessment of subordinate special installations.

2–19. Commander, U.S. Army North

The Commander, USARNORTH will—

a. Serve as the Army point of contact to U.S. Northern Command (USNORTHCOM) in the USNORTHCOM area of responsibility (AOR) for AT.

b. Maintain an operations order (OPORD) incorporating HQDA policies and Secretary of the Army Title 10 responsibilities.

c. Exercise tactical control (TACON) for FP over all Army forces in the USNORTHCOM AOR in accordance with USARNORTH OPORD, as approved by HQDA. This does not include Army personnel under the security responsibility of a Chief of Mission (COM).

d. Support HQDA program reviews of ACOMs, DRUs, and CNGB in the USNORTHCOM AOR.

e. Coordinate all assessments, directives and other instructions issued by USNORTHCOM through FP and operational channels with HQDA, ACOM, ASCC, DRU, ARNG, and the USAR prior to USARNORTH publication.

f. Develop and communicate FP priority intelligence requirements (PIR) for the AOR.

g. Coordinate and disseminate the flow of FP threat information with ACOMs located in the USNORTHCOM AOR (except for elements under a COM).

h. Receive appropriate CI reports with information on imminent threats to Army installations in CONUS. Evaluate eGUARDIAN and intelligence information reports for indications and warning of terrorist threats and disseminate to USNORTHCOM.

i. Provide USNORTHCOM AOR focused FP related intelligence to or from HQDA and ACOMs. Coordinate information with USNORTHCOM.

j. Provide representation to the ARTIC in support of Army Threat Working Group (ATWG).

k. Identify issues and coordinate with HQDA and USNORTHCOM for clarification and resolution of all AT standards/directives that could adversely affect operational Army forces or execution of Army Title 10 responsibilities.

2–20. Commander, U.S. Army Corps of Engineers

The Commander, USACE will—

a. Develop and disseminate AT protective design criteria and identify appropriate prescriptive measures for Army facilities.

b. Develop requirements and execute programs for research and studies supporting the incorporation of AT initiatives into Army facilities and installations.

c. Coordinate with the Commanding General (CG), INSCOM and the U.S. Army Criminal Investigations Command and support ACOMs, ASCCs, DRUs, and installations in the development of terrorist threat assessments in sufficient detail to serve as a basis for military construction design on a reimbursable basis. Such assessments should include long-term projections of worldwide threat capabilities and include a description of likely aggressor tactics, weapons, tools, and explosives.

d. Assist, as requested, ACOMs, ASCCs, DRUs, and installation commanders in conducting vulnerability assessments on a reimbursable basis.

e. Provide training for installation level AT planners, focused on physical and electronic security measures appropriate for potential threat tactics, weapons, tools, and explosives.

f. Ensure USACE engineers have incorporated AT measures for all new construction and modifications to existing structures and facilities, in coordination with appropriate Staff/geographic combatant command, considering local threat and vulnerability assessments.

g. Assist commanders to ensure that protective measures, to include mass notification/alert warning systems, electronic security and physical barriers, are incorporated into proposed military construction, Army projects in compliance with Army military construction (MILCON) policy.

h. Provide technical personnel support to DCS, G–3/5/7 designated assessment teams.

2–21. Commander, U.S. Army Special Operations Command

The Commander, USASOC will—

a. Develop doctrine and training supporting execution of AT operations unique to Army Special Operations Forces.

b. Coordinate counterterrorism (CT) doctrine and training with the Army specified functional proponent for AT (USAMPS), as appropriate.

2–22. Commander, U.S. Army Cyber Command

a. The Commander, ARCYBER will serve as the single point of contact for reporting and assessing Army cyberspace incidents, events, and operations in Army networks, and for synchronizing and integrating Army responses thereto in support of the Army's AT Program.

b. Plan coordinate, integrate, synchronize, direct, and conduct an integrated defense within all Army networks, and, as directed, within the DOD Information Networks in support of the Army's AT Program.

(1) Maintain defense of the DOD Information Network–Army (the Army's portion of the Department of Defense Information Network) against potential terrorist threats to the network and information systems that support the Army's AT Programs and activities.

(2) Assess specific or general ACOM and control vulnerabilities open to terrorist exploitation and attack in coordination with USACIDC via ARCYBER.

(3) Perform computer and network vulnerability assessments in coordination with USACIDC via ARCYBER based on Army commanders' operational requirements, applicable policies, and AT plan.

(4) Recommend courses of action to reduce or avoid terrorist threat to Army or Army associated computer and network information infrastructures.

(5) Provide information operations-related mission-specific assistance in contingency operations, planning, training, test, demonstration, experimentation, and exercise support.

(6) Produce and distribute terrorist threat advisories related to command, control, communications, and computers (C4) systems operations, and recommend protective countermeasures.

(7) Provide a comprehensive assessment of the cyber terrorism threat nexus to HQDA (DAPM–MPO–AT and DAPM–MPO–AC) annually no later than 1 August.

(8) Provide supported Army commanders with information concerning the cyber terrorist threat against their personnel, information, and critical resources consistent with the provisions of AR 381–10, and other applicable regulations and directives.

(9) Conduct liaison with national level intelligence analytical organizations to exchange foreign cyber terrorist threat information.

2–23. Commanding General, U.S. Army Intelligence and Security Command

The CG, INSCOM will—

a. Conduct foreign intelligence collection and CI activities to collect and disseminate information on foreign terrorist threats against the Army.

b. When appropriate, conduct investigations of international terrorist incidents with Army equities.

c. Maintain a capability to report and disseminate INSCOM-collected, time-sensitive information concerning the foreign terrorist threat against Army personnel, facilities, and other assets.

d. Provide supported Army commanders with information concerning the foreign threat against their personnel, facilities, and operations consistent with the provisions of AR 381–20 and other applicable regulations and directives.

e. Implement Army TARP worldwide to ensure that DA personnel are aware of what types of behaviors and matters related to espionage or terrorist associated insider threats should be reported.

f. Coordinate with ACOMs, ASCCs, DRUs, and the CNGB to ensure CI support for those DA organizations without organic CI capability within the provisions of DODI 5240.10 and AR 381–20.

g. Serve as the Army intelligence liaison representative to Federal, State, and local agencies and host country Federal, State, and local level agencies to exchange foreign terrorist threat information. Host country coordination should be in accordance with agreements between the ASCC commander and other U.S. agencies.

h. Establish procedures to ensure appropriate liaison at all levels between INSCOM, USACIDC, and PM/SO elements operating in support of the AT Program regarding domestic terrorism on Army installations.

i. Immediately notify the affected installation PM/SO, the installation's higher headquarters (that is, ACOM, ASCC, DRU, and CNGB), and HQDA (in accordance with app C) upon receipt of time-sensitive terrorist threat information.

j. Provide coordination on all waivers and exceptions to requirements contained in paragraphs 2–8*a* and 2–8*b*.

2–24. Army command, Army service component command, direct reporting unit, and Chief, National Guard Bureau

OCONUS ASCCs will develop, maintain, and update AOR specific ATO training that supplements USAMPS certifying instruction. This training will be in addition to USAMPS mobile training teams ATO training in coordination with USAMPS. The block of instruction should also be used at the discretion of ASCC senior leaders to improve ATO understanding of the AOR. ACOM, ASCC, and DRU commanders, and CNGB will—

a. Establish and implement a command specific AT communication plan. This plan can be a part of other command guidance to include operations center procedures.

b. Incorporate AT into their plans and operations.

c. Publish guidance (policy supplement, OPORD, AT Plan) to subordinate elements (major subordinate commands, units, installations, facilities, and activities) for execution of AT standards.

d. Publish an AT Strategic Plan that guides the command's AT Program efforts by articulating the Army's AT strategic goals and performance objectives and provides a construct to implement, measure, and report on their accomplishment. Strategic Plans will be reviewed annually and updated as appropriate.

e. When possible, publish AT plans that include instructions for subordinate elements on the use of AT cover sheets for requirements supporting contracts, grants and agreements (assistance agreements, cooperative agreements, grants, and technology investment agreements).

f. Provide programmatic oversight and assessment of subordinate elements' (that is, major subordinate commands, units, installations, facilities, and activities) AT Programs.

g. Ensure subordinate elements designate a focal point to coordinate requirements for, and receive and disseminate time-sensitive threat information received from Federal, State, local, HN, USACIDC, and U.S. intelligence agencies.

h. Ensure their subordinate elements, which are tenants of Army garrisons, DOD installations, or other government agency installations or activities comply with host AT requirements, participate in the host AT planning process, and provide personnel support for the implementation of random antiterrorism measures (RAM) and FPCON levels coordinated and agreed to in host AT plans.

i. Validate intelligence production and threat assessment support requests submitted by subordinate organizations.

j. Ensure, in coordination with INSCOM, that CI support is provided to those subordinate organizations without organic CI capability within the provisions of DODI 5240.10 and AR 381–20.

k. Establish a process to track movements into or through SIGNIFICANT or HIGH threat level areas for subordinate units of 50 personnel or more.

l. Submit AT mission requirements and distribute funding.

m. Implement and execute the Army AT tasks and all the Army AT standards in accordance with implementing guidance identified in chapters 4 and 5 (see app F).

n. Additionally, ACOM and DRU commanders who execute responsibilities for installations and facilities will—

(1) Provide operational oversight/technical guidance and assessments for their command-managed installation base operations (BASOPS) AT Programs. These actions will be taken after coordination and agreement with the respective ASCC commander exercising TACON (for FP) over their installations.

(2) Ensure all installation and/or garrison resource managers fully understand the Management Decision Execution Program (MDEP) for antiterrorism (VTER), law enforcement (QLPR), physical security (QPSM), and installation preparedness program (VIPP) requirements and other MDEPs that may potentially support AT Programs.

(3) Submit AT requirements to higher headquarters and distribute BASOPS funding (MDEPs: VTER, QLPR, QPSM, and VIPP) to installations.

(4) Ensure AT is incorporated into the MILCON Project Prioritization System.

o. Coordinate with the appropriate geographical combatant commander (GCC) to prioritize and submit Combatant Commander Initiative Fund (CCIF) requests.

p. Assign antiterrorism coordinators (ATCs) to units not requiring a certified ATO to supplement the AT Program as determined necessary. ATCs will be used to supplement an ATO in risk management, integrating AT into the contract support process, and increase AT awareness as a component of all protection plans including active shooter threats. Commands must track ATC training to ensure sufficient qualifications using the USAMPS training support package available on the Army Antiterrorism Enterprise Portal (ATEP).

2–25. Senior commanders

Senior commanders of Army installations will—

a. Provide overall AT guidance and executive-level oversight of the installation AT Program that include the approval of the installation AT plans and requirements within the installation or stand-alone facilities' (SAF's) APP Integrated Protection Plan.

b. Conduct an annual program review of the installation AT Program.

c. Conduct an annual exercise of the installation AT Plan.

d. Review for concurrence on garrison command AT requirements.

e. Submit operational reporting (OPREP)–3 reports of incidents possibly affecting FP through their chain of command to HQDA AOC. The senior commander will simultaneously submit the OPREP–3 to their chain of command, HQDA, and the ASCC assigned responsibility for the geographic General Officer Command.

f. Ensure local implementation of FPCONs is compliant with the ASCC minimum baseline while assuming an adequate FP posture necessary to protect personnel and other vital assets from local threats. Commands and personnel residing on installations, whether on a permanent or temporary basis, will support and comply with the FP directives of the senior commander, or Joint base commander, regardless of Service.

2–26. Garrison commanders

Garrison commanders will—

a. Execute the installation AT Program in support of the senior commander.

b. Provide guidance and direction to the garrison ATO.

c. Provide daily operational oversight and technical guidance for installation AT missions.

d. Conduct AT manpower and funding requirements analysis, submit AT requirements through the planning, programming, budgeting, and execution, and forward them to their respective senior commanders for approval prior to submitting AT requirements to their higher headquarters.

e. Ensure all tenant units/activities are participants in the AT planning process, the AT working group, and are included in AT plans, providing guidance and assistance as required, this includes physical security personnel participation in real property planning boards and real property master planning area development plan practicums.

f. Implement and execute the Army AT tasks and all the Army AT standards with the exception of Standard 32 in accordance with implementing guidance identified in chapters 4 and 5 (see app E).

g. Garrison commanders without organic intelligence support will coordinate such support through their senior commander to meet the requirements of Standard 2.

2–27. Commanders of units, battalion-level and above

Commanders of units, battalion-level and above will implement and execute the Army AT tasks and all the Army AT standards with the exception of Standards 10, 11, 12, 21, and 32 in accordance with the implementing guidance identified in chapters 4 and 5 (see app E).

2–28. Commanders/directors of U.S. Army tenant units/activities on U.S. Army, Department of Defense, or other Government Agency installations/facilities

Commanders/directors will—

a. Participate in the host installation/facility AT planning process and AT working group. During this planning process, any tenant unit/activity personnel support requirements will be identified that are required for the implementation of host installation FPCON levels.

b. Comply with host installation/facility AT requirements.

c. Provide personnel support as specified in host installation/facility AT plans, as approved by the senior commander at Army installations/facilities or the commander/director at DOD or other Government agency installation/facilities.

d. Company-level units and below that are not located on the same installation as their parent units are not required to develop/maintain their own AT Program. Commanders of such units will implement the policies and procedures specified in the AT plan/orders of their parent unit. Specific guidance covering these units will be documented in the AT plan/orders of the parent unit.

e. Tenant activities that are populated by less than ten (10) DOD personnel daily are not required to develop/maintain their own AT Program. Commanders/Directors of such tenant activities will implement the policies and procedures specified in the AT plan/orders of their parent organization. Specific guidance covering these organizations will be documented in the AT plan/orders of the parent organization.

f. Tenant activities that are not identified in paragraphs 2–28*d* and 2–28*e*, 2–24 (ACOM, ASCC, DRU) or 2–27 (units, battalion and above) will implement and execute Army AT tasks and all the Army AT standards with the exception of Standards 2, 10, 11, 12, 19, and 32 in accordance with implementing guidance identified in chapter 4 and 5 (see app F). Although not required to implement and execute Standards 2 and 10, commanders/directors of such tenant activities will establish appropriate procedures to send/receive terrorist threat information and warnings to/from the host installation/facility and they will request representation at the host installation/facility ATWG.

2–29. Commanders/directors of stand-alone facilities/owned or leased facilities

For purposes of this regulation, these requirements apply to all Army organizations that are not located on an Army, other Service, or other Government agency installation/facility. These organizations include but are not limited to Reserve Officer Training Corps Detachments, Recruiting Centers and Stations, U.S. Military Entrance Processing Stations, Armed Forces Reserve Centers, Army Reserve Centers, USACE headquarters, medical facilities, and administrative facilities, and ARNG armories. Commanders/directors will—

a. Implement and execute Army AT tasks and appropriate Army AT standards as outlined in this regulation.

b. Apply applicable FPCON measures as directed by the commander and GCC.

c. Document specific guidance covering these organizations in the AT plan/orders of the parent organization.

d. Implement the policies and procedures specified in the AT plan/orders of their parent organization.

e. Direct SAFs to conduct coordination (as applicable and reasonable) with local authorities in support of the SAFs AT Program.

Chapter 3
The Army Antiterrorism Program

3–1. Overview

a. AT is the Army's defensive program to protect against terrorism. The combination of AT, CT, terrorism consequence management, and intelligence support constitute the overall Combating Terrorism Program. The AT Program focuses on risk management, planning (including the AT plan), training and exercises, resource generation, comprehensive program review, and the conduct of the RAM. AT planning coordinates specific AT security requirements into the efforts of adjunct security programs (that is, intelligence support to AT, law enforcement, physical security, and information operations).

b. AT is an integral part of Army efforts to defeat terrorism. Terrorists can target Army elements at any time in any location. By effectively preventing and, if necessary, responding to terrorist attacks commanders protect all activities and people allowing Army missions to proceed unimpeded. AT is neither a discrete task nor the sole responsibility of a single branch. All bear responsibility. As that statement suggests, AT must be integrated into all Army operations and considered at all times. Installations, recruiting duty, Corps of Engineers projects or combat action should consider the AT principles in every assigned task. Awareness must be built into every mission, every Soldier, and every leader. Integrating AT represents the foundation crucial for Army success.

3–2. The terrorist threat

Terrorism is not a recent phenomenon in the U.S. or overseas. Because terrorists cannot challenge the U.S. in conventional warfare, they prefer to attack targets they perceive as weak or soft. Bombings, shootings, and kidnappings are the common terrorist methods, but terrorists have also used arson, hostage taking, hijacking/skyjacking, assassination, WMD, and instances of Web site tampering to further their cause. Not all of these have been attempted against the Army, but the potential exists. The nature and types of threats to the Army vary widely with geographic location, criticality of the assets, vulnerability of the target, and level of hostile intent. Terrorists implement asymmetric attacks to further their objectives. Asymmetric attacks are those attacks that place an adversary's strengths against our weaknesses, versus a conventional force-on-force scenario. The most devastating form of these attacks will be conducted with the use of WMD, composed primarily of chemical, biological, and radiological weapons and high yield conventional explosives.

3–3. U.S. Government policy on terrorism

The U.S. Government policy on terrorism is unequivocal, firm opposition to terrorism in all its forms wherever it takes place. The U.S. Government will act in concert with other nations, and unilaterally when necessary, to resist terrorism by any legal means available. Our Government will not make concessions to terrorists, including ransoms, prisoner releases or exchanges, or policy changes. Terrorism is considered a potential threat to national security, and other nations that practice or support terrorism will not do so without consequence.

3–4. U.S. Government terrorism responsibilities

a. DOS has primary responsibility to deal with Foreign Consequence Management and terrorism involving Americans living, working, and traveling abroad, other than incidents on U.S. flag vessels in international waters. However, commanders maintain an inherent responsibility to protect Army personnel, Family members, Army facilities, and other assets while OCONUS.

b. The Department of Justice is the primary agency for crisis management in responding to terrorist incidents within the United States (including the District of Columbia, the Commonwealth of Puerto Rico, and all U.S. possessions and territories) and in maritime areas subject to U.S. jurisdiction. Unless otherwise specified by the Attorney General, the FBI will be the primary agency for investigating and apprehending terrorists in such incidents.

c. The Department of Homeland Security (DHS) has primary responsibility within the U.S. to prevent and deter terrorist attacks and protect against and respond to threats and all hazards to the nation. They ensure safe and secure borders, control the entry of lawful immigrants and visitors, and promote the free-flow of commerce. DHS agencies with key AT missions include:

(1) The Transportation Security Administration (TSA) is charged with preventing terrorist attacks and protecting the U.S. transportation network. It has exclusive responsibility for direction of law enforcement activity affecting the safety of persons aboard aircraft in flight (excluding military aircraft). "In flight "is defined as that period when an aircraft's exterior doors are closed. The TSA is responsible for communicating terrorist threat information to commercial air carriers and their passengers. DA will provide the TSA threat information within its operational area of interest, consistent with appropriate DOD and DA policies.

(2) The Federal Emergency Management Agency is the primary agency for coordinating federal consequence management (providing support to victims and damaged facilities from terrorist attacks) within CONUS.

(3) The U.S. Coast Guard (USCG) is responsible, within the limits of U.S. territorial seas, for reducing the risk of a maritime terrorist incident by diminishing the vulnerability of ships and facilities through the implementation of security measures and procedures. The USCG is also responsible for AT planning in U.S. ports.

3–5. U.S. Government "No Double Standard" policy

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

b. Commanders may disseminate terrorist threat information immediately to DOD Elements and Personnel for threats directed solely against the DOD. In foreign countries and areas, the threat information also will be passed up the chain of command to the lowest level that has direct liaison with the DOS or the appropriate U.S. Embassy(ies) (or for non-combatant commander assigned forces, the U.S. Defense Representative (USDR)). Within the United States, its Territories,

and Possessions, the threat information will be passed up the chain of command to the lowest level that has direct liaison with the DHS. Except when immediate notice is critical to the security of DOD Elements and Personnel, the appropriate DOS/U.S. Embassy(ies)/DHS should be informed of the threat information before release to DOD Elements and Personnel. When immediate notice is critical to the security of DOD elements and personnel, commanders may immediately disseminate the information to, and implement appropriate AT protective measures for, DOD elements and personnel; and as soon as possible, inform the DOS/U.S. Embassies or the DHS, as appropriate, through the chain of command.

c. Commanders also will inform the DOS/U.S. Embassy(ies) or the DHS of any changes to FPCON Levels or the security posture that significantly affects the HN/U.S. public. When FPCONs are changed based upon received threat information, both the threat information and notice of the changed FPCON will be passed up the chain of command to the lowest level that has direct liaison with the DOS/U.S. Embassy(ies) (or for non-combatant command assigned forces, the USDR) or the DHS. Coordination and cooperation with the DOS/U.S. Embassy or the DHS in these cases is NOT a request for concurrence. Rather, it is informing the COM or Secretary of Homeland Security of the DOD response to a given terrorist threat. Although the COM or Secretary of Homeland Security may not agree with the commander's assessment, the ultimate responsibility for protection of DOD Elements and Personnel rests with the commanders in the chain of command. In areas outside the purview of the DHS, the DOS is responsible to determine whether to release the threat information to U.S. citizens abroad and to deal with the sensitivities of the HN(s). In the areas under the purview of the DHS, the Secretary of Homeland Security is responsible to determine whether to release the threat information to the U.S. public.

3–6. U.S. Army antiterrorism policy

In support of the DOD policy on terrorism, it is DA policy that—

a. All DA personnel, their families, installations, facilities, information, and other material resources will be protected from terrorist acts through a high priority, comprehensive AT program.

b. Commanders at all levels have the responsibility and authority to enforce appropriate security measures to ensure the protection of DA elements and personnel subject to their control and will ensure AT awareness and readiness of all DA elements and personnel (including dependent Family members) assigned or attached.

c. Where specific GCC and DA AT standards/requirements conflict, the GCC AT standard/requirement will take precedence.

d. All DA military personnel, DA Civilians, and DA Family members will comply with theater, country, and special clearance requirements (DODD 4500.54E and DOD 4500.54–G) before overseas travel.

e. Commanders will ensure inclusion of appropriate AT training and awareness requirements in all contracts requiring an AT/OPSEC cover sheet, as specified in paragraph 5–25. Army officials responsible for developing and negotiating contracts with contractor operators of Government facilities will ensure that appropriate language for completing AT Level I Awareness training requirements is included in all operating contracts. Commanders will provide a means to ensure all assigned contractors complete the requirements for AT Level I awareness training as specified by the terms of the contract. Contractors are required to comply with the terms of the contract. Commanders are required to offer AT training to contractors under the terms specified in the contract. Contractors working within a U.S. military facility or in proximity of U.S. Forces will receive incidental benefit from measures undertaken to protect U.S. Forces.

f. Operating contractors at Government-owned contractor operated facilities will comply with the provisions of this regulation, and with ACOM, major subordinate command, DRU, and GCC directives and guidance, which supplement or amend AR 525–13. Army officials responsible for developing and negotiating contracts with contractor operators of government facilities will ensure that this provision is included in all operating contracts.

g. As set forth in paragraph 3–5, compliance with the "No Double Standard" policy on dissemination of terrorist threat information is maintained.

3–7. U.S. Army terrorist threat/incident reporting

a. Suspected or known terrorist related information is a critical information requirement for the Army. Commanders at all levels will report up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism against Army personnel (Soldiers, Civilian employees, or their Family members), units, installations, activities, facilities, civil works and like projects, or other assets for which they have responsibility, including the provision of such information to appropriate interagency officials.

b. This will be accomplished in accordance with the reporting requirements specified in paragraph 5–35, AT standard 34, terrorist threat/incident reporting and appendix C.

Chapter 4
Army Antiterrorism Framework

4–1. General

This chapter provides a framework that defines eight AT tasks commanders should use to achieve the Army's objectives to deter terrorist incidents, employ counter measures, mitigate effects, and conduct incident recovery.

4–2. Antiterrorism Task 1. Establish an antiterrorism program

Commanders will communicate the spirit and intent of all AT policies throughout the chain of command or line of authority by establishing AT Programs that provide standards, policies, and procedures to reduce the vulnerabilities from terrorist attack. Army AT standards that should be addressed when accomplishing this task include—

a. Standard 1. AT Program elements.
b. Standard 7. AT plan.
c. Standard 8. AT Program coordination.
d. Standard 9. ATO.
e. Standard 10. AT working group.
f. Standard 12. AT executive committee.
g. Standard 30. AT resource requirements.
h. Standard 33. AT communication planning, AT awareness, and suspicious activity reporting.
i. Standard 34. Terrorist threat/incident reporting.

4–3. Antiterrorism Task 2. Collection, analysis, and dissemination of threat information

Commanders will develop a system to collect, analyze, and disseminate terrorism threat information and apply the appropriate FPCON. Army AT standards that should be addressed when accomplishing this task include—

a. Standard 2. Intelligence support to the Army AT Program.
b. Standard 4. Terrorism threat assessment.
c. Standard 11. Threat working group.
d. Standard 22. FPCON measures.

4–4. Antiterrorism Task 3. Assess and reduce critical vulnerabilities (conduct antiterrorism assessments)

Commanders will continuously conduct assessments of their AT efforts, to include overall program review, assessment of individual physical and procedural security measures to identify vulnerabilities, and unit pre-deployment assessments. Army AT standards that should be addressed when accomplishing this task include—

a. Standard 3. AT risk management.
b. Standard 5. Criticality assessment.
c. Standard 6. Terrorism vulnerability assessment.
d. Standard 31. Comprehensive program review.
e. Standard 32. Comprehensive program review teams.

4–5. Antiterrorism Task 4. Increase antiterrorism awareness in every Soldier, Civilian, and Family member

Commanders will ensure that all personnel are aware of the terrorist threat and adequately trained in the application of protective measures. AT training will be integrated into unit collective training regardless of unit location. Army AT standards that should be addressed when accomplishing this task include:

a. Standard 16. AT measures for HRP (training requirements).
b. Standard 23. AT training and exercises.
c. Standard 24. Formal AT training.
d. Standard 25. Level I AT Awareness training.
e. Standard 26. Level II ATO training.
f. Standard 27. Level III Pre-command training.
g. Standard 28. Level IV AT executive seminar.
h. Standard 29. AOR-specific training for Army personnel and in-transit forces.
i. Standard 33. Incorporation of AT into the Command Information Program.

4–6. Antiterrorism Task 5. Maintain defenses in accordance with force protection condition

Commanders will ensure that AT specific security procedural and physical measures are employed to protect personnel, information, and material resources from terrorist threats. Army AT standards that should be addressed when accomplishing this task include—

a. Standard 13. AT physical security measures.
b. Standard 14. RAM.
c. Standard 15. AT measures for off-installation facilities, housing, and activities.
d. Standard 16. AT measures for HRP.
e. Standard 17. AT construction and building considerations.
f. Standard 18. AT measures for logistics and other contracting.
g. Standard 19. AT measures for critical asset security.
h. Standard 22. FPCON measures.

4–7. Antiterrorism Task 6. Establish civil/military partnership for terrorist incident crisis

Commanders will coordinate with local civilian communities to establish relationships to formulate partnerships to combat and defend against terrorism. The Army AT standard that should be addressed when accomplishing this task is: Standard 8, AT Program coordination.

4–8. Antiterrorism Task 7. Terrorism threat/incident response planning

Commanders and heads of agencies/activities will develop response plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents. Army AT standards that should be addressed when accomplishing this task include:

a. Standard 20. Terrorist incident response planning.
b. Standard 21. Terrorism consequence management measures.

4–9. Antiterrorism Task 8. Conduct exercises and evaluate/assess antiterrorism plans

Commanders will institute an exercise program that develops, refines, and tests the command's AT response procedures to terrorist threats/incidents and ensure AT is an integral part of exercise planning. The Army AT standard that should be addressed when accomplishing this task is: Standard 23, AT training and exercises.

Chapter 5
Army Antiterrorism Standards and Implementing Guidance

5–1. General

a. This chapter defines the standards developed to ensure the synchronization and integration of all elements of the Army AT Program. Successful execution of these standards will ensure compliance with the mandatory standards required by DODI O–2000.16, Volume 1.

b. All of the AT standards are discussed below. Each contains a statement of the standard and implementing instructions.

c. Commanders should develop more specific standards and supplemental guidance as appropriate to the local situation.

5–2. Standard 1. Antiterrorism program elements

a. *Army standard 1.* The minimum required elements of an AT Program are: 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).

b. *Implementing guidance.* Commanders will develop and maintain their AT Program elements in an iterative manner and will continuously refine them to ensure the relevance and viability of all defensive measures employed to reduce vulnerabilities to terrorist capabilities.

5–3. Standard 2. Intelligence support to the Army antiterrorism program

a. *Army standard 2.* Commanders will develop a system to monitor, report, collect, analyze, (at the appropriate level) and disseminate terrorist threat information.

b. *Implementing guidance.* Commanders will—

(1) Establish an AT Program supported by all-source intelligence with PIR, Commander's Critical Information Requirements (CCIR), and focused collection, analysis, and dissemination to protect personnel, Family members, facilities, civil works and other projects, and information in all locations and situations.

(2) Ensure production and analysis requirements are focused and based on their PIR and CCIR. PIR and CCIR must be reviewed for currency, revalidated at least annually, and updated whenever appropriate to meet changing threats and/or requirements.

(3) Ensure terrorist intelligence information is developed, collected, analyzed, and disseminated in a timely manner. Current intelligence will be integrated into the AT training program.

(4) Ensure the appropriate law enforcement and intelligence organizations within their command collect and analyze criminal and terrorist threat information respectfully.

(5) Provide units in transit with tailored terrorist threat information.

(6) Coordinate with designated support intelligence organizations to integrate counter surveillance, surveillance detection, counterintelligence, and other specialized skills as a matter of routine in their AT Program.

(7) Identify an official as the focal point for the integration of operations and local or HN intelligence, CI, and criminal intelligence information.

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

(9) Ensure collection operations are being conducted consistent with the requirements of AR 381–10, AR 381–12, AR 380–13, DODD 5200.27, and other applicable regulations and directives.

(10) Ensure the command has appropriate connectivity to receive threat-related information from all available sources (for example, ARTIC, FBI, ACIC, USACIDC, provost marshal, local law enforcement, Intelink-S, and Intelink).

(11) Ensure the command uses the Defense Intelligence Analysis Program to validate and receive intelligence community (IC) support for terrorism analysis and products to support their AT Programs that are beyond the capabilities of the intelligence organizations under their command.

(12) If commanders do not have organic intelligence or law enforcement elements to meet the requirements of this standard, they will coordinate such support through their higher headquarters.

5–4. Standard 3. Antiterrorism risk management

a. Army standard 3. Commanders will integrate risk management in the planning, coordinating, and developing of AT plans, orders, operations, and exercises. Risk management allows commanders to assess and control the risks associated with any mission or operation.

b. Implementing guidance.

(1) Leaders at all levels must be aware of how to integrate risk management into troop leading procedures and AT planning when conducting any mission or operation in accordance with ATP 5–19 and DA Pam 190–51. Effective integration of risk management will enable the leader to identify terrorist threat capabilities, assess the initial risk of the hazards, and develop controls to eliminate the hazards, or reduce the hazard risk level to the point at which the cost of additional measures outweighs the potential benefit.

(2) Commanders will conduct risk assessments to integrate threat assessment (Standard 4), criticality assessment (Standard 5), and vulnerability assessment (Standard 6) information in order to make conscious and informed decisions to commit resources or enact policies and procedures that either mitigate the threat or define the risk. While conducting risk assessments, commanders will consider the factors of threat, criticality, and vulnerability of facilities, programs, and systems. Risk assessments will address the following four elements:

(a) The terrorist threat (threat assessment).

(b) The criticality of assets (criticality assessment).

(c) The vulnerability of facilities, programs, and systems to terrorist threats, including use of chemical, biological, radiological, nuclear and high yield explosive materials (CBRNE) or similar capabilities (vulnerability assessment).

(d) The ability to conduct activities to deter terrorist incidents; to employ countermeasures; to mitigate the effects of a terrorist incident; and to recover from a terrorist incident.

(3) Commanders will review their risk assessment process and procedures annually. An annual AT self-assessment, a comprehensive AT Program review conducted by their higher headquarters, or a joint mission assurance assessment (JMAA) satisfies this requirement.

5–5. Standard 4. Annual threat assessment

a. Army Standard 4. Commanders will establish a Terrorism Threat Assessment process to identify the full range of known or estimated terrorist threat capabilities (including CBRNE and WMD).

b. Implementing guidance.

(1) ASCC commanders assigned to GCCs and the Commander, USACIDC in close coordination with ARTIC and ACIC will incorporate terrorist and threat information into an Annual Threat to the Army Assessment, providing the basis for the Army's annual comprehensive threat statement.

(2) No later than 1 June, the identified ASCCs and ARCYBER will provide threat assessment production points of contact to the ARTIC and ACIC. Annual threat assessments will cover the period 1 June to 31 May. A copy of the annual terrorism threat statement will be forwarded to HQDA (DAPM–MPO–AT and DAPM–MPO–AC) annually no later than 1 August, or the first business day thereafter. Commanders will—

(a) Utilize the DOD Terrorist Threat Level classification system to identify the threat in a specific overseas country. Army commanders will use this threat statement as the basis for developing AT plans. Threat levels are estimates, with no direct relationship to specific FPCON. An explanation of the FPCON and DOD terrorist threat level classification system is located at appendix B.

(b) Ensure AT and threat information is distributed, as appropriate.

(c) Implement effective processes to integrate and fuse all sources of available threat information from local, State, Federal, HN law enforcement agencies; the appropriate local, State, Federal, HN 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.

(d) 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, graduation ceremonies, and events open to the public (that is, armed forces day celebrations).

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

(f) Ensure Terrorism Threat Assessments are a part of leader's reconnaissance in conjunction with deployments. Follow-on terrorism threat assessments will be conducted for all deployments as determined by the commander, or directed by higher headquarters.

(g) Due to AR 381–10 restrictions on U.S. person information, consolidated (MI and criminal intelligence data) threat statements cannot be filed, stored, or maintained as an intelligence product. These statements must be filed, stored, and maintained within law enforcement or operations channels (that is, provost marshal, USACIDC, Deputy Chief of Staff for Operations and Plans (DCSOPS)/G–3/Directorate of Plans, Training, Mobilization and Security (DPTMS) and so forth).

(h) Ensure Annual Threat to the Army Assessment requirements are accomplished in accordance with the current standard operating procedures and production timeline.

5–6. Standard 5. Criticality assessment

a. Army standard 5. Commanders will establish an AT criticality assessment process as part of their responsibilities for synchronizing and integrating Army priorities and initiatives across their command. The commander will determine the programs and activities to include in the criticality assessment, as well as priorities, ensuring a doctrinally based process that supports the command's mission(s) and support activities.

b. Implementing guidance.

(1) Commanders will coordinate for the appropriate protection of critical assets not owned by the command and refer all shortfalls to the higher headquarters in the chain of command for resolution.

(2) Use criticality assessment results to develop appropriate protective and response measures for command assigned critical assets and functions based on command directed factors that may include—

(a) Effect of loss.

(b) Recoverability.

(c) Mission functionality.

(d) Substitutability.

(e) Reparability.

(3) Update the criticality assessment annually.

(4) Ensure tenant involvement with host installation criticality assessment process.

(5) Coordinate critical assets and functions list with higher headquarters.

(6) ACOM, ASCC, DRU, ARNG, and U.S. Army Reserve Command commanders will review subordinates' criticality assessments through the command AT Program review process, evaluate command level critical assets and functions and develop appropriate protective measures for those assets based on the factors above.

(7) Include HQDA and GCC identified assets and functions identified through the DODI 3020.45, Volume 1 process into overall command planning. Mission critical assets prioritized as defense critical infrastructure will be placed at the top of any local critical asset list.

(8) Installation and facility commanders will, utilizing the working group and executive committee forums, develop and update annually the installation/facility level critical asset list. Include HQDA and GCC identified assets and functions into the overall installation/facility asset list.

(9) Develop protective measures for those assets based on the factors above and ensure tenant assets and functions are considered within the larger installation/facility critical asset list.

5–7. Standard 6. Terrorism vulnerability assessment

a. Army standard 6. Terrorism vulnerability assessments will be conducted to provide a vulnerability-based analysis of mission-essential assets, resources, and personnel that are susceptible to terrorist attack.

b. Implementing guidance.

(1) Commanders will conduct terrorism vulnerability assessments at least annually or more frequently if the terrorist threat assessment or mission requirements dictate. Commands will provide the appropriate vulnerability assessments guidance to SAF. Terrorism vulnerability assessments will be conducted at a minimum for any Army installation, facility, or activity that fall under any one of the following categories:

(a) Any Army installation, facility, or activity populated daily by DOD personnel.

(b) Any Army installation, facility, or activity possessing responsibility for emergency response or physical security plans and programs, or determined to be critical infrastructure.

(c) Any Army installation, facility, civil work project, or activity possessing authority to interact with local non-military or HN agencies or having agreements with other agencies or HN agencies to procure these services.

(d) Deploying units, whether the deployment is for an exercise or operational mission/support. Pre-deployment terrorism vulnerability assessments will include assessment of sea and air ports of embarkation and debarkation; movement routes (sea, air, ground, and rail); assembly, staging, and reception areas; base camps, support structures (contract and HN), and local operating communities. Terrorism vulnerability assessments will be part of leader's reconnaissance in conjunction with deployments. Follow-on terrorism vulnerability assessments will be conducted for all deployments as determined by the commander or directed by higher headquarters.

(e) Off-installation DOD housing, schools, daycare centers, transportation systems, and routes used by DOD personnel and their Family members when the Terrorism Threat Level is SIGNIFICANT or higher, based on the local threat.

(f) Any events or activity determined to be a special event or other activity involving DOD personnel (that is, battle assemblies, drill assemblies, Independence Day and Armed Forces Day Celebrations). Commanders have the flexibility to determine if the scope of an event will require a vulnerability assessment. A terrorism vulnerability assessment will be integrated into the planning process for these types of events, and considerations for the protection and control of large volumes of pedestrian and vehicle traffic should be included.

(2) Information derived from vulnerability assessments will be classified pursuant to the requirements outlined in the Defense Threat Reduction Agency (DTRA) DOD Vulnerability Assessment.

(3) Vulnerabilities identified from higher headquarters assessments (for example, JMAA) will be populated into the DOD System of Record within 120 days from the completion of the assessment. The Mission Assurance Risk Management System (MARMS) directly supports the Secretary of Defense's Mission Assurance (MA) responsibilities as defined in the DOD MA Strategy and Implementation Framework. The objective of MARMS is to enable resilience while supporting all critical processes required to protect assets and ensure continued defense critical mission execution. MARMS will function as an integration framework spanning multiple security domains undergirding risk-informed decision making, resource investment, and improved synchronization across all levels of the DOD enterprise.

(4) Within 90 days of the completion of an assessment, commanders will prioritize/track identified vulnerabilities, develop a plan of action to mitigate or eliminate the vulnerabilities, and report all vulnerabilities documented by any assessment to the first general officer or civilian equivalent director in the chain of command and to their higher headquarters (ACOM, ASCC, or DRU).

(5) Higher headquarters commanders will track all reported vulnerabilities of their subordinate organizations and/or installations to resolution/closure.

(6) Vulnerabilities identified from assessments found in paragraph 5–7*b*(1)(*a*) through 5–7*b*(1)(*f*) will be populated into the DOD System of Record within 120 days from the completion of the assessment.

(7) Terrorism vulnerability assessments will serve as a basis and justification for AT plans, enhancements, program/budget requests, and establishment of FPCONs.

(8) Continuous assessment of daily routine and activities in operational environments will be accomplished to ensure the threat is known and appropriate measures are in place to mitigate the vulnerabilities.

5–8. Standard 7. Antiterrorism plan

a. Army standard 7. Commanders will develop and maintain comprehensive, proactive AT plans, orders, or other implementing guidance. These plans, orders, and other guidance will implement all applicable Army AT standards. AT plans, orders, and other implementing guidance will not be considered complete unless signed by the commander and exercised.

b. Implementing guidance.

(1) ACOM, ASCC, and DRU commanders and CNGB will publish guidance (that is, policy supplement, OPORD, AT Plan) to subordinate elements (that is, major subordinate commands, units, installations, facilities, and activities) for execution of AT standards.

(2) At a minimum, an AT plan will be developed at garrison, SAF, and unit (battalion or higher) levels, and also for training and operational deployments (50 or more personnel), training exercises (50 or more personnel), and special events (that is, Independence Day and Armed Forces Day celebrations) and SAFs. SAF owning commands will provide specified guidance to SAFs for AT Plan requirements as well as FPCON and RAM requirements based on the current threat to the SAF and higher headquarters guidance. AT requirements will be included in the deployment order as an annex or as a part of associated movement security plan.

(3) At a minimum, AT plans will address—

(a) The essential AT Program elements (see Standard 1) and standards addressed in this regulation.

(b) Specific threat mitigation measures to establish a local baseline defensive posture. The local defensive posture will facilitate systematic movement to and from elevated security postures, including the application of RAM.

(c) AT physical security measures.

(d) AT measures for HRP, when appropriate.

(e) AT measures for protection from potential insider threats.

(f) AT construction and building considerations.

(g) AT measures for logistics and other contracting.

(h) AT measures for Critical Asset Security.

(i) AT measures for in-transit movements when appropriate.

(j) Terrorism incident response measures.

(k) Terrorism consequence management measures, including CBRNE and WMD planning, and measures to deal with toxic industrial hazards (TIH), that is, toxic industrial chemical/toxic industrial material (TIC/TIM).

(l) FPCON implementation measures, including site-specific AT measures.

(m) Master planning.

(4) At a minimum, an AT plan will be reviewed annually.

5–9. Standard 8. Antiterrorism program coordination

a. Army standard 8. Commanders will coordinate AT matters with all subordinate, supporting, supported, and tenant units; HN authorities; and local, State, and Federal authorities pursuant to existing law and DA policy to support AT planning and program implementation.

b. Implementation guidance.

(1) Commanders will—

(a) Include all tenants and supported Reserve Component (RC) units/activities in the AT planning process and ensure they are included in AT plans, providing guidance and assistance, as required.

(b) Ensure their subordinate units, which are tenants of other installations/facilities, comply with host installation/facility AT requirements, participate in the host installation/facility AT planning process, and provide personnel support for the implementation of host installation/facility FPCON levels specified in the host installation/facility AT plans.

(c) Coordinate and synchronize AT plans with other protection plans.

(d) Develop and maintain planning and coordinating relationships between the SAF and local authorities for sharing threats/warnings. Additionally, SAFs may supplement annual threat assessment at higher commands with local threat information.

(2) Commanders OCONUS will—

(a) Comply with applicable status of forces agreement when planning and executing AT operations.

(b) Coordinate AT efforts with HN authorities and the U.S. Country Team.

(c) Coordinate AT plans with the appropriate GCC and U.S. Embassy or Consulate. Provide copies of approved AT plans to appropriate higher headquarters and Country Team officials in accordance with GCC established policy.

5–10. Standard 9. Antiterrorism officer

a. Army standard 9. Commanders will appoint in writing, a Level II-certified commissioned officer, noncommissioned officer, or civilian staff officer as the ATO.

b. Implementing guidance.

(1) ACOM, ASCC, and DRU commanders and CNGB will appoint an ATO (minimum grade of O–4 or equivalent civilian grade) within the operations function or a special staff organization that is best suited to execute the program (DCSOPS/G–3/and so forth). Commanders should consider establishing the ATO as a full time position at these levels.

(2) Garrison commanders will appoint an ATO (minimum grade of O–3 or equivalent civilian grade) in writing within the operations function or a location that is best suited to execute the program (G–3/DPTMS/and so forth). Commanders should consider establishing the installation/garrison ATO as a full time position.

(3) All units, battalion and above, will have an ATO appointed in writing (minimum grade of E–6 or higher at battalion and brigade level and E–8 or higher or equivalent civilian grade at division or corps level).

(4) A deploying unit having 300 or more individuals assigned or under the operational control of a designated commander will have a Level II-certified ATO (minimum grade of E–6 or higher or equivalent civilian grade).

(5) Commanders with SAFs having DOD personnel assigned, occupied, or under the operational control of a designated commander or director will determine the need for assigning an ATO/ATC.

(6) USACE commanders and directors will appoint an ATO (minimum grade of E–6 or higher or equivalent civilian grade) within the operations function or a location that is best suited to execute the program (G–3/5/7/DPTMS/and so forth).

(7) Commanders may assign ATCs to supplement ATO in circumstances where units or activities separated from the main headquarters or where ATOs are not required, but can support large organizations with AT related activities. The Administrative Assistant to the Secretary of the Army (for HQDA activities), ACOM, ASCC, and DRU commanders, Directors, CNGB, the CAR and are responsible for ensuring ATCs are trained using the USAMPS approved training located on the Army ATEP.

5–11. Standard 10. Antiterrorism working group

a. Army standard 10. Commanders will establish an ATWG that meets 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.

b. Implementing guidance.

(1) ATWGs will be established at all ACOMs; ASCCs; DRUs; CNGB; Army garrisons; and stand-alone facilities.

(2) The ATWG may be consolidated for efficiencies into an organization's protection working group.

(3) Formal ATWGs are not required to be established at units (battalion level and below), but the working group functions will be integrated into unit planning and operations (that is, routine command/staff meetings, long range planning calendar briefings, quarterly training briefings). SAF leaders may determine the function of the ATWG in routine staff functions. Include community participation in the ATWG, as appropriate.

(4) Units will participate in the host installation/garrison ATWG.

(5) ATWG membership will include the following:

(a) Commander or designated representative (that is, Deputy Commander, Chief of Staff (CoS), G–3, and so forth).

(b) ATO.

(c) Representatives of the commander's principal staff.

(d) CBRNE expertise.

(e) Tenant unit representatives.

(f) Other representatives as required supporting AT planning and program implementation.

5–12. Standard 11. Threat working group

a. Army standard 11. Commanders will establish a TWG that meets 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.

b. Implementing guidance.

(1) TWGs will be established at all ACOMs; ASCCs; DRUs; CNGB; the Army Reserve; and Army garrisons.

(2) Formal TWGs are not required to be established at units (battalion level and above), but the working group functions will be integrated into unit planning and operations (that is, routine command/staff meetings, long range planning calendar briefings, quarterly training briefings).

(3) SAF owning commands will provide guidance to SAFs regarding TWGs establishment and participation.

(4) TWG membership will include the following:

(a) Commander or designated representative (that is, Deputy Commander, CoS, G–3, and so forth).

(b) ATO/ATC and the local community and DOD services as appropriate (that is, classification of the meeting).

(c) Representatives of the commander's principal staff.

(d) Tenant unit representatives.

(e) Appropriate representatives from direct-hire, contractor, local, State, Federal, and HN law enforcement agencies and the IC.

5–13. Standard 12. Antiterrorism executive committee

a. Army standard 12. Commanders will conduct the AT executive-level committee as part of the Command's Protection Executive Committee that meets at least semi-annually which will develop and refine AT Program guidance, policy, and standards; to act upon the recommendations of the ATWG or protection working group and TWG; and to assist in determining resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities. The Command's Protection Executive Committee includes and encompasses all other protection-related executive councils and approval authority boards to facilitate the integration, coordination, and synchronization of APP efforts.

b. Implementing guidance.

(1) Antiterrorism executive committees (ATECs) will be established at all ACOMs; ASCCs; DRUs; CNGB headquarters and Army garrisons.

(2) Membership should include the commander, his or her staff principals, and the ATO.

5–14. Standard 13. Antiterrorism physical security measures

a. Army standard 13. The principles of the DA Physical Security Program (AR 190–13) will be applied and fully integrated into AT Plans to ensure employment of a holistic security system to counter terrorist capabilities.

b. Implementing guidance.

(1) Commanders will ensure that well-designed AT physical security measures are multi-layered and include the integration and synchronization of the following essential elements:

(a) Detection (human, animal, or sensors to alert security personnel of possible threats and unauthorized entry attempts at or shortly after occurrence).

(b) Assessment (electronic audiovisual means, security patrols, or fixed posts to localize and determine the size and intentions of unauthorized intrusion or activity).

(c) Delay/denial (active and passive security measures including barriers to impede intruder efforts).

(d) Communication (command and control procedures).

(e) Response (trained and properly equipped security forces).

(2) Commanders will ensure that integrated facilities, physical security equipment, trained personnel, and procedures are 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 and commercial delivery companies), HRP protection, barrier plans, and facility standoff distances.

(3) Commanders will ensure that their plan is executable with assets on hand and that execution/emplacement timelines are factored into the plan.

5–15. Standard 14. Random antiterrorism measures

a. Army standard 14. RAM will be conducted as an integral part of all AT Programs. RAM is particularly important for our units, installations, facilities, activities, and civil work projects due to the static nature of our forces, and missions often result in the establishment of identifiable routines.

b. Implementing guidance.

(1) Commanders will ensure that RAM is conducted as an integral part of all AT Programs.

(2) Garrison commanders will have a formally documented RAM Program, under the supervision of the AT officer. Their RAM program will include tenant activities and commands in RAM planning and execution.

(3) All commanders will utilize the concept of RAM in providing AT for their unit or organization.

(4) To maximize effectiveness and deterrence value, commanders should implement RAM without set pattern, either in terms of measures selected, time, place, or other variables.

(5) RAM will consist of the random implementation of higher FPCON measures or intensified site-specific FPCON measures in consideration of the local terrorist capabilities. Random use of other physical security measures will be used to supplement FPCON measures.

(6) Commanders will employ RAM, in conjunction with site-specific FPCON measures, in a manner that portrays a robust, highly visible and unpredictable security posture from which terrorists cannot easily discern security AT patterns or routines.

5–16. Standard 15. Antiterrorism measures for off-installation facilities, housing, and activities

a. Army standard 15. All AT Programs will include specific AT measures for off-installation Government facilities, housing, transportation services, daycare centers, and other activities used by or involving mass gathering of Army personnel and their Family members.

b. Implementing guidance.

(1) All commanders will ensure these AT measures include but are not limited to: emergency notification and recall procedures.

(2) Garrison commanders will ensure these AT measures include but are not limited to: guidance for selection of off-installation housing, temporary billeting, and other facility use (including compliance with United Facilities Criteria (UFC) 04–010–01 for leased, newly constructed, and expeditionary buildings); physical security measures; CBRNE defensive measures; and shelter in place, relocation, and evacuation procedures.

(3) Garrison commanders will develop Mutual Assistance Agreements (MAA) or other similarly structured protocols with the appropriate local, State, Federal, and HN authorities to coordinate security measures and assistance requirements to ensure the protection of Army personnel and their Family members at off-installation facilities and activities. Consult with the servicing Office of the Staff Judge Advocate for advice regarding MAA.

5–17. Standard 16. Antiterrorism measures for high-risk personnel

a. Army standard 16. Personnel who are at a greater risk than the general population, by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat will be identified and assessed. Personnel requiring additional security to reduce or eliminate risks will be formally designated as HRP to make them eligible for special control/security measures. Appropriate measures will be taken to provide enhanced protection to HRP. HRP and their families will be made aware of risks and trained in individual protective measures. Additionally, support staff such as drivers, aides, and protective service details will be trained and equipped.

b. Implementing guidance.

(1) The designation and protection of Army HRPs will be accomplished in accordance with DODI O–2000.22 and AR 190–58.

(2) Responsible commanders will 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 high-risk billets (HRB), facilities, or countries requiring such protection; and have been thoroughly indoctrinated on the duties and responsibilities of protective service personnel.

(3) Responsible commanders will comply with the provisions of DOD C–4500.51 for the acquisition and use of nontactical armored vehicles in support of HRP security operations.

5–18. Standard 17. Antiterrorism construction and building considerations

a. Army standard 17. The construction and building standards prescribed in DOD 5200.8–R, UFC 4–010–01 and 4–010–02 will be fully complied with regarding the adoption of and adherence to common criteria and minimum construction standards to mitigate vulnerabilities.

b. Implementing guidance.

(1) Commanders will develop a prioritized list of AT factors for site selection. These criteria will be used to determine if facilities either currently occupied or under consideration for occupancy by Army personnel provide adequate protection of occupants against the effects of a terrorist attack. Commanders will develop these lists designed to address the appropriate level threat and vulnerability assessment and based on guidance contained in DODI 2000.12.

(2) Circumstances may require the movement of Army personnel or assets to facilities the U.S. Government had not previously used or surveyed. In such cases, commanders will include AT standards as a key consideration in evaluating the suitability of these facilities for such use.

(3) Requests for waivers or exceptions to the requirements of UFC 4–010–01 and UFC 4–010–02 will be in accordance with appendix F.

5–19. Standard 18. Antiterrorism measures for logistics and other contracting

a. Army standard 18. AT measures will be incorporated into the logistics and contracting actions (requirements development, source selection/award, and contract execution) when the provisions of the contract or services provided affect the security of Army elements, personnel, or mission-essential cargo, equipment, assets, or services. The evaluation process for future contracts will include consideration of the potential contractor's past performance with AT requirements.

b. Implementing guidance. Commanders will, in direct coordination with their supporting contracting officer, establish a mechanism to ensure the following measures are incorporated into contracting actions—

(1) Commanders at all levels will use the appropriate AT cover sheet to ensure that contracts, grants and agreements (assistance agreements, cooperative agreements, grants, and technology investment agreements) include required AT related protections.

(2) Implement a verification process, whether through contractually required background checks or other similar processes applicable to the area of operation that demonstrates the trustworthiness of Defense contractor and sub-contractor employees. This includes U.S. citizens, foreign nationals, and HN personnel.

(3) Develop and implement site-specific risk mitigation measures to maintain positive control of Defense contractor or sub-contractor access to and within installations, sensitive facilities, and classified areas.

(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 Army personnel and mission-essential assets.

(5) Ensure contracts comply with AT provisions of the Defense Federal Acquisition Regulation Supplement.

(6) Ensure contracts incorporate AT Level I Awareness I training requirements (para 5–26*b*(2)(*b*)).

(7) Acting as the organizational focal point for AT related measures, the ATO will coordinate with other members of the staff to verify that all measures have been properly incorporated into contracts.

(8) ATO verification will be annotated on an AT/OPSEC cover sheet. In organizations that do not have an ATO assigned, an ATC may sign the AT/OPSEC cover sheet after completing training administered by the appropriate HQDA activities, ACOM, ASCC, DRU, ARNG, and Army Reserve representatives.

(9) Appendix G contains guidance for the review and verification that AT measures have been properly incorporated into contracts.

5–20. Standard 19. Antiterrorism measures for critical asset security

a. Army standard 19. Risk management measures will be developed and implemented to reduce the vulnerabilities of critical assets, facilities, resources, and personnel to terrorist attack and integrate these measures into overall AT Program efforts. Critical assets, resources, and personnel are those identified by applying the AT criticality assessment process in Army Standard 5, and the UFC, and include distributive information and computer-based systems and networks.

b. Implementing guidance. Commanders will—

(1) Develop and implement AT risk management measures for critical assets (including distributive information and computer-based systems and networks), resources, and personnel in accordance with DODI 2000.12 and AR 525–26.

(2) Develop and implement risk management measures for those assets designated as Defense Critical Assets per DODD 3020.40, including distributive information and computer-based systems and networks .

(3) Coordinate with local, State, Federal, or HN authorities responsible for the security of non-DOD assets deemed essential to the functioning of Defense Critical Infrastructure and overall capability of the Army to execute National Military Strategy.

(4) Commands owning SAFs will provide guidance to SAFs to ensure appropriate compliance with this standard.

5–21. Standard 20. Terrorism incident response measures

a. Army standard 20. Commanders and heads of agencies/activities will include in AT plans terrorism incident response measures that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents. The Army is managing response measures in accordance with the National Incident Management System. Therefore AT incident response measures must be incorporated into command installation response and recovery plans.

b. Implementing guidance.

(1) Terrorist incident response measures in AT plans will, at a minimum, address management of the FPCON system, implementation of all FPCON measures, and requirements for terrorist related reports. Plans will be affordable, effective, and attainable; tie security measures together; and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. At the garrison level, the plans must tie into other installation response plans.

(2) Garrison commanders will identify high-risk targets (HRTs), mission essential vulnerable areas (MEVAs) and ensure planning provides for focus on these areas.

(3) Garrison commanders will—

(a) Incorporate AT threat information sharing into response and recovery plans in accordance with AR 525–27.

(b) Identify HRTs, MEVAs.

(c) Ensure planning provides for focus on these areas. Facility managers whose facility has been identified as a HRT will be informed, and will ensure facility security plans are formulated on this basis.

(4) Commanders will—

(a) Develop procedures to ensure periodic review, update, and coordination of AT plans with other protection stakeholders.

(b) Ensure CBRNE, medical, fire, and police assets are integrated into consequence management/AT plans.

(c) Integrate near real-time threat or attack information sharing plans/programs into the overall Installation Protection Plan.

(5) CONUS commanders (to include Alaska and Hawaii) will—

(a) Notify the local FBI office concerning threat incidents occurring at Army installations, facilities, activities, and civil work projects or like activities.

(b) Take appropriate action to prevent loss of life and/or mitigate property damage before the FBI response force arrives. On-site elements or USACIDC elements will be utilized to safeguard evidence, witness testimony, and related aspects of the criminal investigation process pending arrival of the FBI response force. Command of U.S. Army elements will remain within military channels.

(c) If the FBI declines jurisdiction over a threat incident occurring in an area of exclusive or concurrent Federal jurisdiction, take appropriate action in conjunction with USACIDC elements to resolve the incident. In such cases, commanders will request advisory support from the local FBI office.

(d) If the FBI declines jurisdiction over a threat incident occurring in an area of concurrent or proprietary Federal jurisdiction, coordinate the military response with USACIDC elements, state and local law enforcement agencies, as appropriate. In such cases, commanders will request advisory support from the local FBI office.

(6) OCONUS commanders will—

(a) Where practicable, involve HN security and law enforcement agencies in AT reactive planning and request employment of HN police forces in response to terrorist attacks.

(b) Coordinate reactions to incidents of a political nature (such as a government protest; attempted or assassination of a government official; or a chemical, biological, radiological, and nuclear threat/attack) with the U.S. Embassy and the HN, subject to instructions issued by the combatant commander with geographical responsibility.

(c) In SIGNIFICANT and HIGH terrorist threat level areas, plans to respond to terrorist incidents will contain procedures for the notification of all DOD personnel and their dependents. Such plans will provide for enhanced security measures and/or possible evacuation of DOD personnel and their dependents.

(7) USACIDC will investigate threat incidents in accordance with paragraph 2–14*c*.

(8) AT plans, orders, standing operating procedures (SOP), terrorism threat, criticality, and vulnerability assessments, and coordination measures will consider the potential threat use of WMD. Commanders will assess the vulnerability of installations, facilities, and personnel within their AOR to potential threat of terrorist using WMD and CBRNE weapons to include TIH.

5–22. Standard 21. Terrorism consequence management measures

a. Army standard 21. Terrorism consequence management, CBRNE and public health emergency preparedness, and emergency response measures will be included as an adjunct to the overall disaster planning and preparedness to respond to a terrorist attack. These measures will focus on mitigating vulnerabilities of Army personnel, families, facilities, and material to terrorist use of WMD and CBRNE weapons to include TIH, as well as overall disaster planning and preparedness to respond to a terrorist attack. These measures will include integration and full compliance with DOD emergency responder guidelines (DODI 3020.52); mass notification system standards (UFC 4–021–01); establishment of medical surveillance systems (DODD 6490.02E); deployment of CBRNE sensors and detectors; providing collective protection; and providing individual protective equipment in the following priority:

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

(2) Essential personnel. Personnel deemed essential to the performance of essential military operations (whether military, civilian, contractor, HN personnel, and 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 (that is, hours to days), escape protection may be necessary to sustain essential operations (that is, escape, survive, and restore essential operations).

(3) 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.

b. Implementing guidance. Commanders will—

(1) Develop and implement site-specific CBRNE preparedness and emergency response measures that are synchronized with a corresponding FPCON level.

(2) Establish MAA or other similar protocols with the appropriate local, State, Federal, or HN authorities to support AT plan execution and augment incident response and post-incident consequence management activities.

(3) Ensure a garrison can warn populations 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.

(4) Develop and implement site-specific public health emergency response measures that are synchronized with FPCON levels in accordance with DODI 6200.03 and DODD 3020.40.

(5) AT planning considerations for SAFs will be included in the Emergency Action Plan.

5–23. Standard 22. Force protection condition measures

a. Army standard 22. The DOD FPCON system is an effects-based progressive level of protective security measures implemented in response to terrorist threats.

b. Implementing guidance. When changing DOD and GCC FPCON mandatory measures, execute FPCON change reporting requirements in accordance with GCC directives and courtesy copy the AOC.

(1) Commanders and directors will—

(a) Develop a process to raise or lower FPCON measures based on threat information or guidance/approval from higher headquarters and in accordance with DODI O–2000.16, Volume 2.

(b) Establish a review mechanism to lower the FPCON level back to the GCC FPCON baseline, as soon as the threat environment permits to avert the counterproductive effect on security and overall mission accomplishment from a prolonged elevated FPCON level.

(c) Develop and implement site-specific FPCON measures for stationary and in-transit units to supplement the FPCON measures in appendix B.

(d) Ensure site-specific FPCON measures permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement (SROE) and the Standing Rules for the Use of Force (SRUF).

(e) Ensure processes are in place to notify all organic, tenant, and supported units, to include RC units of FPCON transition procedures and measures.

(f) Consider as an effective alternative to executing the higher-level FPCON measures (in some circumstances based upon local conditions and the threat environment) implementing a lower-level FPCON and supplementing with commanders' supplemental FPCONs or other local security, mitigating measures and RAM.

(g) Ensure the capability exists to implement all FPCON measures, either through on-hand assets or availability of local assets.

(h) Ensure AT plans, orders and site-specific AT measures linked to a FPCON receive the appropriate classification as necessary in accordance with local classification policy or AR 380–5.

(i) Ensure AT measures linked to a FPCON, but are separated from the AT plan or order, receive the appropriate classification as necessary in accordance with local classification policy or AR 380–5.

(j) Ensure required FPCON reports are submitted through the service chain of command or in accordance with appendix C, if at the ASCC level.

(2) The GCC is responsible for establishing the baseline FPCON for the AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented.

(3) If determined that certain FPCON measures or other AT procedural requirements are inappropriate for current operations, or proper threat mitigation, commanders may request a waiver.

(4) Develop command specific FPCON measures based on GCC FPCON guidance. The FPCON measures will be documented in the AT plan.

(5) Subordinate commanders may raise a higher-level commander's FPCON for those personnel and assets for which they have AT responsibility. Subordinate commanders will not lower a higher-level commander's FPCON level without written concurrence at the command level established by the GCC.

(6) Organizations owning maritime watercraft (vessels) will implement Shipboard FPCON mandatory measures based on threat information or guidance from higher headquarters and in accordance with DODI O–2000.16 Volume 2, and AR 56–9, as appropriate.

c. Force protection condition waiver process.

(1) Waiver requests will be submitted in writing through the chain of command to the waiver-level authority dictated by GCC. Information copies of the waiver requests will be sent to the ASCC operations center for forwarding to the GCC's joint operations center.

(2) Locally approved waivers, to include mitigating measures or actions, must be forwarded to the ASCC operations center or service chain of command with information copies to ASCC operations center for submission to the GCC's joint

operations center in accordance with GCC mandated timelines, and to the AOC as soon as practical but no-later-than 5 working days after approval.

5–24. Standard 23. Antiterrorism training and exercises

a. Army standard 23. AT training will be 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.

b. Implementing guidance. Commanders will—

(1) Ensure AT training is included in mission rehearsals and pre-deployment training for all units (platoon level or above) prior to deployment. Multi-echelon individual training using vignettes and AT scenarios is required.

(2) Ensure units, which are deploying to or moving through or to HIGH threat areas, conduct pre-deployment training that is supported by measurable standards, including SROE/SRUF, AOR-specific threat orientation, deterrence-specific SOP TTP/exercises, lessons learned, and the operation and use of security equipment.

(3) Conduct a comprehensive AT plan exercise annually.

(4) The annual AT plan exercise will encompass all aspects of the AT plan including the following areas:

(a) Implementation of AT measures through FPCON DELTA at parts of the command, installation, unit, or SAF.

(b) Terrorist use of WMD and CBRNE weapons to include TIH.

(c) Initial response and consequence management capabilities.

(d) Threat attacks on Army information systems.

(e) Use and evaluation of attack warning systems.

(f) Medical mass casualty scenarios.

(g) Active shooter scenario.

(h) Memorandums of agreement (MOAs), memorandums of understanding (MOUs), MAA, and similarly structured protocols with local and HN response agencies.

(5) AT exercise documentation will be maintained for no less than 3 years to ensure incorporation of lessons learned in the AT plan.

(6) Develop an annual AT training and exercise program integrated in to the overall organization-training program to provide the necessary individual and collective training to prepare for the annual AT and operational exercises.

(7) Higher headquarters ATO will provide SAFs with exercise guidance.

(8) Exercise AT considerations at applicable FPCONs and synchronize with local emergency responders.

5–25. Standard 24. Formal antiterrorism training

a. Army standard 24. The Army's formal AT Training Program will incorporate the training elements specified in DODI O–2000.16. These elements include Level I through Level IV training, AOR-specific training, and HRP AT training (see Standard 16 for HRP training requirements).

b. Implementing guidance.

(1) Commanders will ensure all assigned personnel complete appropriate formal training and education.

(2) Individual records will be updated to reflect completion of the AT training prescribed by this regulation.

(3) Commanders, at all levels, who receive individuals not properly trained will provide the required AT training as soon as practicable following the arrival of such individuals. Concurrently, they will report the deficiency through their chain of command to the losing unit's chain of command, which will institute appropriate corrective action to prevent the recurrence of the discrepancy.

(4) The minimum training requirements for Level I through Level IV AT training are located at appendix D.

5–26. Standard 25. Level I antiterrorism awareness training

a. Army standard 25. Commanders will ensure that all personnel are aware of the terrorist threat and adequately trained in the application of protective measures.

b. Implementing guidance.

(1) Level I AT Awareness training will be provided to all Soldiers in initial entry basic training and in general military subject training for all new-hire Army Civilian personnel. All Army accessions (military or civilian) must receive this initial training under the instruction of a qualified Level I AT Awareness Instructor (Level II trained and certified ATO).

(2) Post-accession Level I AT Awareness training will be provided annually to all DA personnel. Annual post-accession Level I AT Awareness training may be accomplished by one of two means:

(a) Under the instruction of a qualified Level I AT Awareness instructor (Level II trained and certified ATO).

(b) 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 COM authority must receive Level I AT Awareness training from a qualified instructor. The completion of a DOD-sponsored and certified computer-based distance learning instruction for Level I AT Awareness will not satisfy DOS COM requirements.

(3) All face-to-face Level I Awareness training will include training on active shooter response and detection, social media, and insider threat.

(4) Commanders—

(a) Ensure that every Soldier, DA employee, and local national or third country citizen in a direct-hire status by the DA, regardless of grade or position, completes annual Level I AT Awareness training requirements prescribed by this regulation.

(b) Ensure all new-hire Army Civilian and (as appropriate), contractor personnel, in accordance with contract requirements, receive AT Level I Awareness training by a certified Level II trained ATO.

(c) Provide AT information to Defense contractors through the contracting officer as required in the Defense Federal Acquisition Regulation Supplement (DFARS), Section 252.225–7043. Offer AT Awareness training to Defense contractor employees as specified in the contract.

(d) Ensure that dependent Family members ages 14 and older (or younger at the discretion of the sponsor) traveling outside CONUS on official business (that is, on an accompanied permanent change of station move) complete Level I AT Awareness training as a part of their pre-departure requirements. Furthermore, commanders will encourage dependent Family members to complete Level I AT Awareness training before any travel OCONUS (for example, leave) or to any locale where the Terrorism Threat Level is MODERATE or higher.

(e) Will use the Digital Training Management System to record and track AT Level I Awareness training. Compliance will be validated during assessments of subordinate units and elements.

(f) Document Level I AT Awareness training for all assigned personnel in the unit's individual training records in accordance with AR 350–1, paragraph 5–4.

(g) Incorporate AT Awareness training in their Command Information Program.

5–27. Standard 26. Level II antiterrorism officer training

a. Army standard 26. Commanders will ensure all ATOs are formally trained and certified. Level II training will prepare ATOs to manage AT Programs, advise the commander on all AT issues, and administer Level I AT Awareness training.

b. Implementing guidance.

(1) Formal AT training will be provided by USAMPS to individuals who perform duties as an ATO at the unit and garrison/SAF levels.

(a) ATO Basic Course (unit ATO - battalion/brigade).

(b) ATO Advanced Course (unit ATO - division/corps, installation ATO, higher headquarters ATO).

(2) Commanders will identify those key positions that require formal or refresher AT training prior to assumption of duties. Requirements will be forwarded through the chain of command to DCS, G–1 who will ensure assignment orders clearly delineate special instructions for training prior to assignment to the gaining theater/command. For personnel not in transit, commanders will review and forecast training needs through established training channels.

(3) Commanders will designate these individuals in writing and ensure they receive formal certifying training at the TRADOC-designated course within 180 days of assumption of these duties. All ATOs must be certified and complete a formal TRADOC approved Level II AT officer refresher training course every 3 years.

(4) As an exception, the first O–6, or civilian equivalent, in the chain of command is the lowest level authorized to designate ATOs who have not attended formal training provided by the USAMPS. Commanders can only certify those individuals who have received formal training in AT (for example, other DOD Level II approved ATO courses) or by virtue of previous assignments and experience, have extensive knowledge in AT.

(5) OCONUS ASCC commanders will develop AOR-specific AT Level II training to supplement certifying HQDA required Level II ATO training. The ASCC AOR-specific Level II training may be used separately from the HQDA required Level II ATO training to instruct ATO in theater in AOR specific considerations. It should be used to instruct ATO assigned to regionally aligned forces units prior to deployment.

5–28. Standard 27. Level III pre-command antiterrorism training

a. Army standard 27. Level III Pre-Command AT Training will be provided to all O–5 and O–6 commanders or civilian equivalent director position. Instruction, using the TRADOC-developed PCC training support package, will provide commanders or civilian equivalent director position with knowledge, skills, and abilities necessary to direct and supervise the Army AT Programs.

b. Implementing guidance. O–5 and O–6 level commanders or civilian equivalent director position will receive AT training in the Army pre-command (PCC) training courses conducted at branch, component, and functional schools.

5–29. Standard 28. Level IV antiterrorism executive seminar

a. Army standard 28. Level IV AT Executive Training will be made available to O–6 through O–8 officers and civilian equivalent/senior executive service. This training will provide the requisite knowledge to enable development of AT policies and facilitate oversight of all aspects at the operational and strategic level.

b. Implementing guidance.

(1) Executive level AT training is provided through an executive level seminar sponsored by the Joint Chiefs of Staff providing focused updates, detailed briefings, guest speakers, and panel discussions. Seminar will include a tabletop AT war-game focusing on power projection, WMD, AT, intelligence, FPCON management, and implementation of AT actions.

(2) Executive level AT training is requested through the individual's higher headquarters to HQDA AT Branch.

5–30. Standard 29. Area of responsibility–specific training for Department of Defense personnel and in-transit forces

a. Army standard 29. AOR-specific AT Awareness training will be conducted to orient all Army personnel (including Family members ages 14 and older) assigned permanently or temporarily transiting through, or performing exercises or training in an OCONUS GCC's AOR. GCCs are responsible for the development of this AOR–specific information, and it is in addition to annual Level I AT Awareness training.

b. Implementing guidance.

(1) Commanders will ensure all Soldiers and DA Civilians associated with their command receive an AOR update prior to traveling OCONUS or within 3 months of an OCONUS permanent change of station. AOR specific training is available through the GCCs.

(2) Commanders will offer all Defense contractors associated with their command an AOR update prior to traveling OCONUS.

(3) Commanders will maintain a memorandum for record documenting an individual's training.

(4) Additionally, Family members, ages 14 years or older, will receive similar training prior to traveling outside the 50 United States, its territories, and possessions when on official Government orders.

5–31. Standard 30. Antiterrorism resource requirements

a. Army standard 30. Commanders will identify AT resource requirements using the planning, programming, budgeting, and execution process and will implement the DA-approved methodology for documenting and prioritizing AT resource requirements.

b. Implementing guidance.

(1) Commanders will submit prioritized AT requirements through their chain of command to HQDA in accordance with DA Program Objective Memorandum Resource Formulation Guide and timelines using Schedule 75.

(2) Commanders will ensure funding requirements supporting the AT Program are prioritized based on the threat, documented vulnerabilities, regulatory requirements, and/or command directives. Funds supporting the AT Program will be tracked and accounted for in accordance with applicable regulations and directives.

(3) When faced with emergent or emergency AT requirements, commanders may submit them through their combatant commander pursuant to the requirements specified in Chairman of the Joint Chiefs of Staff instruction (CJCSI) 5261.01G.

5–32. Standard 31. Comprehensive antiterrorism program review

a. Army standard 31. Comprehensive AT Program reviews will be conducted to evaluate the effectiveness and adequacy of AT Program implementation.

b. Implementing guidance.

(1) The focus of a comprehensive AT Program review is to determine the activities' ability to protect personnel, information, and critical resources by detecting or deterring threat attacks, and failing that, to protect by delaying or defending against threat attacks. Additionally, these assessments will verify compliance with applicable Army and GCC standards.

(2) Commanders will conduct a self-assessment of their AT Programs within 60 days of assumption of command and annually thereafter or whenever there are significant changes in threat, vulnerabilities, or asset criticality. This assessment will be conducted using either the Internal Control Evaluation Checklist at appendix H locally developed checklist that is tailored to meet the specific AT requirements of a particular command (ACOM, ASCC, DRU, or ARNG), garrison, unit,

tenant unit/activity, or SAF. All locally developed checklists must be approved by the developing unit's higher headquarters (ACOM, ASCC, DRU, or ARNG). The incorporation of additional tasks is authorized. An assessment from a higher headquarters or JMAA can be used to meet the annual assessment requirement.

(3) ACOM, ASCC, and DRU commanders are required to conduct a comprehensive AT Program review of subordinate commands a minimum of once every 3 years. The program review should focus on the essential AT Program elements (see Army Standard 1) and as a minimum, assess the following functional areas:

(a) Physical security.
(b) Engineering.
(c) Plans, operations, training, and exercises.
(d) Resource management.
(e) Military intelligence.
(f) Criminal intelligence.
(g) Information operations.
(h) Law enforcement.
(i) Threat options.
(j) OPSEC.
(k) Medical.
(l) Executive protection/high risk personnel.

(4) Commanders of deploying units will conduct a comprehensive AT Program review in conjunction with pre-deployment vulnerability assessments (see Standard 6). The purpose of this self-assessment 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.

(5) Every Army garrison and SAF AT Program will be assessed by their higher headquarters for compliance with this regulation at a minimum of once every 3 years.

(6) All ACOM, ASCC, and DRU AT Programs will be assessed by HQDA for compliance with this regulation at a minimum of once every 3 years.

(7) Vulnerabilities identified during initial self-assessments, annual self-assessments, or comprehensive AT Program reviews will be populated into the DOD System of Record within 120 days from the completion of the assessment or program review.

5–33. Standard 32. Antiterrorism program review teams

a. Army standard 32. ACOM, ASCC, and DRU commanders and CNGB will form AT Program Review Assessment Teams to execute the AT Program review requirements established in paragraph 5–32.

b. Implementing guidance.

(1) AT Program Review Assessment Teams will be comprised of individuals with sufficient functional expertise to satisfactorily assess and evaluate the effectiveness and adequacy of AT Program implementation at the level (headquarters, unit, command, garrison, SAF, and so forth.) for which the program review is being conducted.

(2) Commanders will establish AT Program Review Assessment Team that include, at a minimum, compliance with the requirements prescribed in this regulation, accepted TTP, and best AT practices. As a guide, commanders should review the DTRA AT Vulnerability Assessment Team Guidelines and adapt them as appropriate to meet the specific requirements of their commands.

5–34. Standard 33. Incorporation of antiterrorism into command information programs

a. Army standard 33. Commanders will promote AT awareness throughout all levels of their command and leverage every member of their command as a sensor to help identify and prevent potential acts of terrorism.

b. Implementing guidance.

(1) ACOM; ASCC; DRU; CNGB; and CAR will—

(a) Establish and implement a separate command-specific AT Communication Plan. This plan can be part of other Command guidance to include Operations Center procedures. Each command plan should be coordinated with the command public affairs officer (PAO) and be an integral part of the command information program. The AT Communication Plan will include a threat overview, facts, assumptions, specified tasks, implied tasks, essential tasks, a mission statement, and a concept of operations for executing AT communications and AT awareness efforts. Each command plan will be tailored to their specific Army communities and audiences and provide guidance for disseminating AT awareness information.

(b) Establish and implement iWATCH and Army and AT Awareness Programs throughout all levels of their command. The programs will be designed to educate all members of the command on AT awareness efforts, the iWATCH, emphasizing indicators of terrorism activity and the procedures to report suspicious activity.

(c) Ensure subordinate elements implement command specific iWATCH Army programs and share AT awareness information.

(d) Establish a process to assess the commands compliance with DODI 2000.26 and DODD 5400.11.

(e) Direct subordinate elements that are tenant activities on Army installations to know local suspicious activity reporting procedures.

(2) Commanders at all levels will—

(a) Disseminate and promote existing reporting protocols for threat reporting, including centralized reporting sites for suspicious activity, including suspicious insider activity, such as IWATCH, ISALUTE and AT awareness products.

(b) Ensure suspicious activity reports and information received within the reports are managed, processed and shared appropriately through the TWG process and local and higher authorities as appropriate per the policy requirements of DODI 2000.26 and DODD 5400.11.

(c) Where applicable, designate the Directorate of Emergency Services or the Provost Marshal Office as the office of primary responsibility for receiving and reporting suspicious activity reports per DODI 2000.26.

5–35. Standard 34. Terrorist threat/incident reporting

a. Army standard 34. Commanders at all levels will report up and down the chain of command all information pertaining to suspected terrorist threats, or acts of terrorism against Army personnel (Soldiers, Civilian employees, or their Family members), units, installations, activities, facilities, civil works and like projects, or other assets for which they have responsibility, including the provision of such information to appropriate interagency officials. At a minimum the reporting will include—

(1) Terrorist Threat Warning Report (TTWR). A TTWR will be transmitted when a command receives credible information concerning an imminent, planned terrorist attack against Army personnel (Soldiers, Civilian employees, or their Family members), facilities, and civil works and like projects, or other assets. Information is "credible" if it is considered serious enough to warrant a FPCON change or implementation of additional security measures which are designed to counter a specific threat.

(2) Terrorist Incident Report (TIR). A TIR will be submitted when a terrorist incident or suspected terrorist incident occurs, involving Army personnel (Soldiers, Civilian employees, or their Family members), facilities, civil works and like projects, or other assets. A "suspected terrorist incident" is one in which involvement by terrorists has not been verified by lead agencies conducting the investigation.

(3) Terrorist Threat/Incident After Action Report (TAAR). TAARs, containing comprehensive discussion of lessons learned, will be forwarded to HQDA (DCS, G–3/5/7 (DAMO–ODF) and PMG (DAPM–MPO)) and CALL.

b. Implementing guidance.

(1) ASCCs assigned to GCCs will maintain a Terrorist Threat/Incident reporting system within their respective commands and all Army elements for which they have AT responsibility. Within the USNORTHCOM AOR, Army reporting and supporting commands will be included in the ASCC reporting system.

(2) Commanders at all levels will submit TTWR, TIR, and Terrorist Incident AAR in accordance with the procedures established by the ASCC.

(3) ASCCs assigned to GCCs will report all TTWR, TIR, and TAAR to HQDA in accordance with appendix C.

5–36. Standard 35. Mission Assurance Risk Management System

The MARMS directly supports the Secretary of Defense's MA responsibilities as defined in the DOD MA Strategy and Implementation Framework. The objective of MARMS is to enable resilience while supporting all critical processes required to protect assets and ensure continued defense critical mission execution. MARMS will function as an integration framework spanning multiple security domains undergirding risk-informed decision making, resource investment, and improved synchronization across all levels of the DOD enterprise.

Appendix A

References

Section I

Required Publications

Unless otherwise indicated, all publications are available at http://armypubs.army.mil.

AR 380–13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations (Cited in para 5–3*b*(9).)

AR 381–10
U.S. Army Intelligence Activities (Cited in para 2–22*b*(8).)

AR 381–12
Threat Awareness and Reporting Program (Cited in para 2–9*g*.)

AR 381–20
Army Counterintelligence Program (Cited in para 2–23*d*.)

AR 525–26
Infrastructure Risk Management (Army) (Cited in para 5–20*b*(1).)

AR 525–27
Army Emergency Management Program (Cited in para 5–21*b*(3)(*a*).)

CJCSM 3150.05D
Joint Reporting System Situation Monitoring Manual (Cited in para C–1*f*.)

DFARS Sections 252.225–7043
Defense Federal Acquisition Regulation Supplement (Cited in para 5–26*b*(4)(*c*).)

DOD 5200.8–R
Physical Security Program (Cited in para 5–18*a*.)

DODD 3002.01
Personnel Recovery in the Department of Defense (Cited in app B–2d(6).)

DODD 5200.27
Acquisition of Information Concerning Persons and Organizations Not Affiliated With The Department of Defense (Cited in para 5–3*b*(9).)

DODD 5205.16
Interim Policy Guidance for DOD Physical Access Control (Cited in app B–9*d*.)

DODD 5210.56
Arming and The Use of Force (Cited in app B–11*c*.)

DODD 5400.11
DOD Privacy Program (Cited in para 5–34*b*(1)(*d*).)

DODI O–2000.16, Volume 1
DOD Antiterrorism (AT) Program Implementation: DOD AT Standards (Cited on the title page.)

DODI O–2000.16, Volume 2
DOD Antiterrorism (AT) Program Implementation: DOD Force Protection Condition (FPCON) System (Cited in para 5–23*b*(1)(*a*).)

DODI 2000.12
DOD Antiterrorism (AT) Program (Cited in title page.)

DODI 2000.26
Suspicious Activity Reporting (SAR) (Cited in para 5–34*b*(1)(*d*).)

DODI 3020.45
Mission Assurance (MA) Construct (Cited in para 5–6*b*(7).)

DTM 09–012
Interim Policy Guidance for DOD Physical Access Control (Cited in app B–5f.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 5–22
The Army Force Modernization Proponent System

AR 11–2
Managers' Internal Control Program

AR 15–1
Department of the Army Federal Advisory Committee Management Program

AR 25–2
Information Assurance

AR 25–22
The Army Privacy Program

AR 25–30
Army Publishing Program

AR 56–9
Watercraft

AR 190–5
Motor Vehicle Traffic Supervision

AR 190–11
Physical Security of Arms, Ammunition, and Explosives

AR 190–13
The Army Physical Security Program

AR 190–14
Carrying of Firearms and Use of Force for Law Enforcement and Security Duties

AR 190–30
Military Police Investigations

AR 190–45
Law Enforcement Reporting

AR 190–51
Security of Unclassified Army Property (Sensitive and Nonsensitive)

AR 190–56
The Army Civilian Police and Security Guard Program

AR 190–58
Designation and Protection of High Risk Personnel

AR 195–2
Criminal Investigation Activities

AR 335–15
Management Information Control System

AR 350–1
Army Training and Leader Development

AR 380–5
Department of the Army Information Security Program

AR 380–53
Communications Security Monitoring

AR 381–11
Intelligence Support to Capability Development

AR 420–1
Army Facilities Management

AR 525–2
The Army Protection Program

AR 530–1
Operations Security

AR 600–20
Army Command Policy

ATP 3–37.2
Antiterrorism

ATP 3–39.10
Police Operations

ATP 3–39.32
Physical Security

ATP 5–19
Risk Management

CJCS Guide 5260
A Self-Help Guide to Antiterrorism (Available at http://www.jcs.mil/library/cjcs-guides/.)

CJCS 5261.01G
Combating Terrorism Readiness Initiatives Fund

CJCSI 3100.01D
Joint Strategic Planning System (Available at http://www.jcs.mil/library.aspx.)

DA Pam 25–403
Guide to Recordkeeping in the Army

DA Pam 190–51
Risk Analysis for Army Property

DOD Antiterrorism Officer Guide
(Available at https://army.deps.mil/army/sites/pmg/prog/atep/at%20doctrine%20and%20trainin
g/DoD%20ATO%20Guide%2C%20Nov12(Updated).pdf and Chapter 3 update available at:
https://army.deps.mil/army/sites/pmg/prog/atep/at%20doctrine%20and%20trainin

DOD Guide 4500.54–G
DOD Electronic Foreign Clearance Guide (https://www.fcg.pentagon.mil.)

DOD 5200.08–R
Physical Security Program

DODD 3020.40
Mission Assurance (MA)

DODD 4500.54E
DOD Foreign Clearance Program (FCP)

DODD 6490–02E
Comprehensive Health Surveillance

DODI 3020.52
DOD Installation, Chemical, Biological, Radiological, Nuclear and High-Yield Explosives (CBRNE) Preparedness Standards

DODI 5240.10
Counterintelligence (CI) in the Combatant Commands and other DOD Components

DODI 6200.03
Public Health Emergency Management within the Department of Defense

DODM 4500.36
Acquisition, Management, and Use of DOD Non-Tactical Vehicles

Joint Travel Regulations
Uniformed Service Members and DOD Civilian Employees(Available at https://www.defensetravel.dod.mil/docs/perdiem/jtr.pdf)

JP 1–06
Financial Management Support in Joint Operations (Available at http://www.jcs.mil/doctrine/joint-doctine-pubs/.)

UFC 2–100–01
Installation Master Planning (Available at https://www.wbdg.org/)

UFC 4–010–01
DOD Minimum Antiterrorism Standards for Buildings with Change 1 (Available at https://www.wbdg.org/.)

UFC 4–010–02
DOD Minimum Antiterrorism Standoff Distances for Buildings (FOUO) (Available at https://www.wbdg.org/.)

UFC 4–021–01
Design and O&M: Mass Notification Systems with Change 1 (Available at https://www.wbdg.org/.)

32 CFR Part 37
Technology Investment Agreements

10 USC 1072
Definitions

10 USC 3013
Secretary of the Army

15 USC
Commerce and Trade

31 USC 6101
Definitions

31 USC 6104
Catalog of Federal domestic assistance programs

31 USC 6105
Oversight responsibility of Director

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (http://armypubs.army.mil).

DA Form 11–2
Internal Control Evaluation Certification

DA Form 2028
Recommended Changes to Publications and Blank Forms

Appendix B

Force Protection Conditions and Threat Levels

B–1. Force protection condition system

The FPCON System discussed here is mandated in DODD 2000.12 and DODI O–2000.16, Volume 2.

a. The FPCON system describes progressive levels of an effects based model (deter, detect, delay, deny, and defend) of security measures for implementation in response to threats to U.S. Army personnel, information, and critical resources. Antiterrorism plans and orders must be constructed to address the threat and implement the measures described in this appendix.

b. The FPCON system is comprised of three elements, DOD baseline, GCC supplemental, and locally developed RAMs.

c. The FPCON system may have limited application to Army elements that are tenants on installations, facilities, or buildings that are not controlled by U.S. Military commanders or DOD Civilians exercising equivalent authority.

d. There are five FPCON Levels; Normal, Alpha, Bravo, Charlie and Delta.

e. DOD FPCON measures are mandatory and cumulative (for example, if a commander declares FPCON Charlie, all DOD FPCON Alpha, Bravo, and Charlie mandatory measures must be implemented, unless otherwise directed by the FPCON declaring authority.)

f. Organizations will execute mandated supplemental measures in accordance with the GCC guidance in the area of operation where they are stationed or reside.

B–2. Force protection condition Normal

FPCON Normal applies at all times as a general threat of terrorist attacks, hostile acts, or other security threats always exists in the world.

a. The FPCON Normal mandatory measures prescribed are always in effect, regardless of the FPCON level a commander declares.

b. Commanders use FPCON Normal to focus their efforts on educating their personnel on the terrorist and hostile adversary threats, deterring and detecting these threats, and reporting indications of these and other suspicious activities, to maintain a level of protection against terrorist attacks and hostile acts.

c. During FPCON Normal, commanders ensure their personnel are knowledgeable on terrorist and hostile actor threats; understand the individual actions they can take to protect themselves and others from terrorist attack; know procedures for reporting suspicious activities and incidents; deter and detect general, non-specific threats of terrorist attacks and hostile acts and prepare to implement additional FPCON measures designed to delay, deny, and defend against these threats.

d. The following measures will be implemented:

(1) *Normal 1.* Regularly inform all personnel of the general threat situation and the reason for any change in FPCON measures.

(2) *Normal 2.* Commensurate with mission requirements, reduce installation and facility access points, to include ground, water, and air avenues, for vehicles and personnel, based upon the threat.

(3) *Normal 3.* Establish and implement procedures to report indications of terrorist or hostile actor surveillance of DOD elements and personnel.

(4) *Normal 4.* Implement methods to obtain intelligence and counterintelligence updates on terrorist and other hostile threats.

(5) *Normal 5.* Institute RAM to enhance deterrence and detection efforts and other security program requirements.

(6) *Normal 6.* Ensure all assigned military personnel, DOD Civilian personnel, and contractors receive the appropriate personnel recovery training pursuant to DODD 3002.01.

B–3. Force protection condition Alpha

FPCON Alpha applies to a non-specific threat of a terrorist attack or hostile act directed against DOD elements and personnel. Commanders must be able to sustain applicable FPCON Alpha measures indefinitely. The following measures will be implemented:

a. Alpha 1. Increase the number of RAM to enhance deterrence and detection efforts and other security program requirements.

b. Alpha 2. Conduct random inspections of privately owned vehicles and personnel entering DOD owned or controlled installations and facilities, including items in the vehicles and items that are carried by personnel.

c. Alpha 3. Implement notification and communications procedures. Notify personnel of all FPCON changes when they occur. Test emergency notification and communications procedures and equipment.

B–4. Force protection condition Bravo

FPCON Bravo applies when an increased or more predictable threat of a terrorist attack or hostile act exists and is directed against DOD elements and personnel. Commanders must be able to sustain all applicable FPCON BRAVO measures indefinitely and must understand FPCON BRAVO will likely affect missions and base support operations during prolonged implementation.

a. Bravo 1. Increase the frequency of inspections of privately owned vehicles and their occupants' hand-carried items that are attempting entry onto DOD owned or controlled installations or facilities.

b. Bravo 2. Randomly inspect all types of commercial deliveries, to include fast food deliveries. Advise family members to check home deliveries.

c. Bravo 3. Enhance off-installation security for DOD facilities (including schools, daycare centers, recruiting centers, reserve forces centers, and critical infrastructure).

B–5. Force protection condition Charlie

The following measures will be implemented when a terrorist or hostile act incident occurs within the commander's area of interest, or intelligence is received indicating a hostile act or some form of terrorist action or targeting against DOD elements, personnel, or facilities is likely.

a. Charlie 1. Increase standoff distance to the extent possible around critical facilities, soft targets, and mass gathering facilities which are vulnerable to attack, as dictated by the threat and the anticipated tactics.

b. Charlie 2. Conduct inspections of all commercial vehicles, to include their drivers and occupants, entering DOD owned or controlled installations or facilities.

c. Charlie 3. Employ threat specific search capabilities (for example, explosive detection capabilities such as military working dogs, explosive detection technology, or chemical, biological, radiological, and nuclear detectors (if threat warrants)) at installation and facility access control points, where permitted.

d. Charlie 4. Employ lighting, barriers, and obstacles as appropriate.

e. Charlie 5. Establish the appropriate number of installation and separate facility perimeter access points, to include access points to defense critical infrastructure as applicable, to support the enforcement of entry control. This includes ground, water, and air avenues, for ground vehicles, waterborne vessels, aircraft, and personnel.

f. Charlie 6. Discontinue use of the Trusted Traveler program for vehicle occupant identification, in accordance with Directive-Type Memorandum (DTM) 09–012.

g. Charlie 7. Cease all flying, except for operational sorties that installation commanders (or superior commanders) specifically authorize. Commanders may consider deploying Unmanned Aircraft System, provided they have Secretary of Defense approval in accordance with the 17 February 2015, Deputy Secretary of Defense Memorandum.

B–6. Force protection condition Delta

The following measures will be implemented when a terrorist attack or hostile act has occurred or is anticipated against specific installations or operating areas. FPCON DELTA should be maintained on a limited basis and only be declared so long as the necessary response capabilities are required.

a. Delta 1. Limit access to installations, separate facilities, and defense critical infrastructure where appropriate, to mission-essential personnel and other personnel as determined by the commander.

b. Delta 2. Search all vehicles and personnel entering installations or facilities, including their hand-carried items (for example, suitcases, backpacks, briefcases, purses, gym bags, packages), not identified by the commander as operationally exempted (for example, credentialed members of the military criminal investigative organizations or members of the military department counterintelligence organizations).

c. Delta 3. Restrict all non-essential movement.

d. Delta 4. Implement procedures to positively identify all personnel entering and circulating on installations and in facilities with no exceptions.

B–7. Shipboard force protection condition mandatory measures

a. The Shipboard FPCON mandatory measures prescribed in DODI O–2000.16 Volume 2, are mandatory for each FPCON level, and are cumulative; meaning commanding officers of maritime vessels (in the case of this regulation, vessels operated by Army component commands) must maintain the mandatory FPCON measures in the declared FPCON level and all lower FPCON levels. Commanding officers of vessels operated by Army component commands may specify supplemental FPCON measures to implement based on the local threat.

b. Commanding officers of vessels operated by Army component commands will coordinate through the appropriate chain of command with the GCCs to declare necessary FPCON levels for their AORs, vessels and commands to establish,

implement, and maintain appropriate in-port FPCON measures to achieve the five effects prescribed in DODI O–2000.16 Volume 2.

c. Patrol vessels guarding port facilities, ocean terminals, wharves, piers, or shore lines will adhere to the supported installations' FPCON level and measures.

d. Army vessels, including the various classes, are defined in AR 56–9.

e. For the purposes of this regulation any vessel owned, operated, chartered, or leased by the DOD (with the exception of contractor-owned, contractor-operated vessels) to include any pre-commissioned DOD vessel which has a commanding officer or vessel master (that is, a civilian or military equivalent to a commanding officer) and that meets the definition of a Class A vessel in AR 56–9.

f. Commanding officers or vessel master will ensure their GCC supplemental Shipboard FPCONs are implemented in addition to DOD Shipboard FPCONs.

B–8. Force protection condition Normal

FPCON Normal shipboard mandatory measures are protective measures that complement and enhance the day to day requirements for access control, pier security, and waterside security. FPCON Normal mandatory measures are always in effect, as a general threat of terrorist acts, hostile acts, or other non-violent security threats always exist.

a. Normal 1: Physically and visually verify the identity of personnel and their purpose for access in accordance with DTM 09–012.

b. Normal 2: Ensure all personnel with access to Army vessels who do not possess an approved DOD access credential are properly vetted against authoritative data sources pursuant to DTM 09–012 and DOD 5200.08–R.

c. Normal 3: Monitor threats and intelligence, and maintain an incident response capability for the current most likely and most dangerous threats.

B–9. Force protection condition Alpha

Upon declaring FPCON Alpha, implement the following measures:

a. Alpha 1: Commanding officers of vessels operated by Army component commands, will maintain a deliberate and visible RAM program to enhance deterrence and detection efforts (DODI O–2000.16 Volume 2 for examples of supplemental Shipboard FPCON measures).

b. Alpha 2: Establish and implement procedures to inspect hand-carried material and vehicles, including, but not limited to, frequency of inspection and any planned increase in frequency at higher FPCON.

c. Alpha 3: Ensure all personnel are knowledgeable of FPCON requirements and that they understand their role in the implementation of these measures.

d. Alpha 4: Educate all personnel on suspicious activity reporting procedures prescribed in DODI 2000.26 and the insider threat to DOD elements and personnel pursuant the 21 November 2012 Presidential Memorandum and to DODD 5205.16.

e. Alpha 5: Periodically test mass notification systems.

f. Alpha 6: Establish waterside access control procedures that include at a minimum measures to impede small craft from approaching and accessing U.S. vessels.

g. Alpha 7: Establish a minimum standoff distance of 100 feet in non U.S. Military-controlled ports in the CONUS, and 400 feet in all ports outside of CONUS, between U.S. vessels and all vehicles, loading areas, and dumpsters on piers. When this is not feasible, inspect 100 percent of vehicles that park or approach within the required standoff.

B–10. Force protection condition Bravo

Upon declaring FPCON BRAVO, implement the following measures:

a. Bravo 1: Coordinate with host-nation husbanding agent or service provider, or local port authority as appropriate, to establish an exclusion zone around the ship and request their assistance in controlling unauthorized craft as necessary.

b. Bravo 2: Post armed sentries on the pier, consistent with the local risk assessment, in accordance with the commanding officer's direction, local rules, regulations, and any applicable status of forces agreements.

c. Bravo 3: Instruct watches to conduct frequent, random searches of the pier, (including access points and pilings) and conduct visual inspections of the ship's hull and ship's boats.

B–11. Force protection condition Charlie

Upon declaring FPCON Charlie, implement the following measures:

a. Charlie 1: Employ explosive detection capabilities (for example, military working dogs, explosive detection technology) at access control points to piers.

b. Charlie 2: Increase the frequency of inspections of privately owned vehicles and commercial vehicles entering piers and loading areas.

c. Charlie 3: Establish, maintain and brief a security detail on the threat and rules of engagement in accordance with DODD 5210.56. Keep key personnel who may be needed to implement security measures on call.

B–12. Force protection condition Delta

Upon declaring FPCON Delta, implement the following measures:

a. Delta 1: Restrict vehicle, watercraft, and pedestrian access to DOD vessels (except for first responders and mission-essential personnel).

b. Delta 2: Search all personnel and vehicles entering piers and personnel attempting access to DOD vessels.

c. Delta 3: Employ all necessary weapons to defend against attack including crew served weapons.

d. Delta 4: Consider getting underway.

B–13. Threat levels

a. The decision to implement a particular FPCON is a command decision based on an assessment of the threat, vulnerability of personnel or facilities, criticality of personnel or facilities, availability of security resources, impact on operations and morale, damage control considerations, international relations, and the potential for U.S. Government actions to trigger a threat response. Frequently, information concerning threat groups is limited to general descriptions of their capabilities and intentions. Often, specific tactics and targets are not identified until it is too late to implement deterrent measures or until after an attack has taken place. For this reason, the absence of specific information concerning the immediate threat should not preclude implementing a higher FPCON and/or additional security measures when general information indicates an increased vulnerability or heightened risk to personnel and/or facilities.

b. Threat levels are developed by intelligence staff officers and should be used as one source of information in determining the appropriate FPCON for a command, installation, facility, area, or unit. Such assessments will be based on the standardized joint-Service criteria promulgated by DOD and the Joint Chiefs of Staff.

(1) Threat levels are determined by assessing the situation using the following four threat factors:

(a) Operational capability. The acquired, assessed, or demonstrated level of capability of a terrorist group to conduct terrorist attacks.

(b) Intentions. The stated desire or history of terrorist attacks against U.S. interests by a terrorist group.

(c) Activity. The actions a terrorist group is conducting and whether that activity is focused on serious preparations for an attack.

(d) Operating environment. The overall environment and how it influences the ability, opportunity, and motivation of a terrorist group to attack DOD interests in a given location.

(2) The following terminology will be used to describe the various threat levels to ensure uniformity throughout DOD:

(a) High. Terrorists are operationally active and use large casualty producing attacks as their preferred method of operation. The operating environment favors the terrorist.

(b) Significant. Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.

(c) Moderate. Terrorists are present but there are no indications of anti-U.S. activity. The operating environment favors the HN/U.S.

(d) Low. No group is detected or the group activity is non-threatening.

(3) There is no automatic link between a threat level and a FPCON, although implementation of FPCON Delta suggests receipt of targeting information (intelligence that terrorist action against a specific location is likely). However, commanders should consider the threat level as a key element in determining the appropriate FPCON for their organizations.

(4) DOD analytic agencies often differ in assigning threat levels to the same countries or areas. This occurs because analysts occasionally disagree concerning conclusions that could be drawn from available intelligence. Different threat levels may also be possible due to differing perspectives among organizations. For example, the Navy is concerned about ships, port areas, and areas frequented by their personnel. These areas may be quite different from areas of concern to Army commanders, even in the same country.

c. Explanation of differences between DOD and DOS threat level classification systems—

(1) The DOD and DOS threat systems are two entirely different systems. They differ in purpose and use different methodologies to determine threat levels. The DOD analysis focuses strictly on the terrorism threat level whereas the DOS analysis covers a larger array of four broad threat categories, only one of which, political violence, deals with the terrorism threat.

(2) The DOD terrorism threat level assessment considers only those indicators and warnings pertaining to terrorism threats. The DOD terrorism threat level assessment is intended to declare a terrorism threat level for a particular country or area. DOD terrorism threat level assessments are event driven and include information regarding the terrorist threat to DOD personnel, facilities, and materiel. The DOD terrorism threat level assessment is used to inform DOD personnel and dependents under the AT Program of a combatant commander, through the combatant commander's information channels.

(a) The DOD terrorism threat level assessment methodology uses all source analysis. The system is flexible and threat levels are revised as terrorism indicators, warnings, and activities occur or change.

(b) DOD uses four factors in analyzing the terrorist threat level: operational capability, intentions, activity, and operational environment.

(c) DOD uses a 4-step scale to describe the severity of the terrorist threat. The four steps from lowest to highest are low, moderate, significant, and high.

(d) DOD, through the Defense Intelligence Agency (DIA), and the combatant commanders can issue terrorism threat level assessments.

(e) The DOD terrorism threat level assessment is not used to indicate the potential of a specific terrorist attack. DIA, the Services, or the combatant commanders issue formal, specific terrorism warnings separately.

(3) The DOS threat assessment process evaluates all source information relative to four broad threat categories and then develops the composite threat list (CTL) for all active foreign service posts staffed by direct hire U.S. personnel and DOD elements (either permanent or TDY personnel), to include accompanying dependents, and facilities which operate under the authority of a COM. One of the primary purposes of the CTL is to aid in prioritizing posts for receipt of security resources, that is, equipment, TDY personnel, funding, and so forth. The higher the threat level, the higher the priority for the implementation of a standard set of security enhancements. A higher threat level immediately justifies the use of additional resources to attain the assigned standards for protection at that particular level of threat.

(a) The four CTL threat categories are political violence (includes terrorist threats/incidents, war, coups, civil disorders, insurgencies, and narco-terrorism); CI (the threat posed to U.S. intelligence by foreign intelligence service); technical (the threat posed by anti-U.S. technical intelligence); and crime (the residential crime environment affecting the official U.S. community).

(b) Each of the four categories is assigned a threat level for a specific post but the only one dealing with terrorism is the first category (political violence). The CTL threat levels from lowest to highest are no data, low, medium, high, and critical.

(c) DOS disseminates its post specific threat categories and threat levels in the CTL, which is published semiannually. The CTL is designed to aid DOS/diplomatic security in prioritizing overseas security programs and ensuring that limited resources are effectively used and applied to overseas security policy board coordinated interagency standards.

(d) The CTL reflects an evaluation of threat levels for a particular period of time, and these levels may be raised or lowered during scheduled reviews (April and October) as situations change. The list does not attempt to reflect the day-to-day security environment of a given locality but rather is intended to provide a longer-term picture for planning and resource allocation purposes.

(e) DOS has the capability to immediately warn personnel under COM authority to specific terrorist threats. In those instances, when threat information is considered sufficiently credible by DOS/diplomatic security to warrant an immediate response, security resources will be committed as necessary to deal with the particular situation, regardless of the assigned CTL threat levels.

(f) DOS threat levels are the result of post inputs and coordination within diplomatic security, DOS, and other U.S. Government agencies at the national level (exactly which agencies are consulted varies according to the threat category). However, as the CTL is intended to assist DOS/diplomatic security for planning and operational purposes, the final arbiter for disputed threat levels are the Director of Diplomatic Security.

(4) All commanders will ensure the DOD assessment is addressed as “DOD Terrorism Threat Assessment.” Refer to the DOS assessment as “DOS Composite Threat List.”

(5) Per DOD policy, when the combatant commander declares or changes a terrorism threat level assessment for a particular country, the combatant commander will ensure that all DOD personnel and their dependents in the country for whom he has AT responsibility are informed of this assessment. This includes informing the USDR.

(a) In locations where combatant commander forces are present in significant numbers, and there is a difference between the DOD terrorism threat level assessment and the DOS CTL threat level (for the political violence category), DOD has directed that the following procedure be used to provide clarification: DOD, through DIA, will publish a message in coordination with DOS diplomatic security, noting the difference and providing an explanation for the difference. The message will be disseminated to the Services, combatant commanders, and to the appropriate USDR. The combatant com-

mander through the USDR will have the responsibility to inform all DOD personnel under COM authority of the information contained in the message. A higher DOD threat assessment will not require action by DOS to increase AT measures but is intended only to inform DOD personnel under COM authority of DOD's assessment of the threat.

(b) There is also a possibility of differences in terrorism threat level assessments between DOD (DIA) and the combatant commanders for a particular country. DIA, as the DOD lead agent, is responsible to clarify or resolve the differences. If there is a valid reason for the difference DIA will inform DOS.

Appendix C

Required Reports

C–1. Terrorist threat warning report [Requirement Control Symbol exempt: AR 335–15, para 5–2e(2)]

a. TTWR reporting requirements in this section apply to ASCCs assigned to GCCs.

b. Upon receipt of credible information concerning a planned terrorist attack against U.S. Army personnel (Soldiers, Civilian employees, or their Family members), facilities, and civil works and like projects, or other assets, a TTWR will be provided immediately by the ASCC via telephone to the AOC (phone DSN (312) 225–4695 or commercial (01) (703) 695–4695). Information is "credible" if it is considered serious enough to warrant a FPCON change or implementation of additional security measures which are designed to counter a specific threat. The initial report will include date, time, and location and brief description of the threatened attack and response.

c. A follow-up report will be transmitted within 6 hours of receiving the information by email message to the AOC usarmy.pentagon-e.hqda.mbx.armywatch@mail.mil (unclassified) or usarmy.pentagon.hqda.mbx.armywatch@mail.smil

.mil (classified). Simultaneously, courtesy copies of the follow-up report will be provided to:

(1) AT Division, PMG at usarmy.pentagon.hqda.list.aoc-at-division@mail.mil (unclassified) or usarmy.pentagon.hqda.list.aoc-at-division@mail.smil.mil (classified).

(2) ARTIC, PMG at usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@mail.mil (unclassified) or usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@mail.smil.mil (classified).

(3) Headquarters, USACIDC at usarmy.belvoir.usacidc.mbx.watch-analytical-center@mail.mil (unclassified) or usarmy.belvoir.usacidc.mbx.watch-analytical-center@mail.smil.mil (classified).

(4) U.S Army Counterintelligence Center at usarmy.meade.902-mi-grp.list.acic-fptab1@mail.mil (unclassified) or usarmy.meade.902-mi-grp.list.acic-fptab1@mail.smil.mil (classified).

(5) ACOMs and DRUs who have units and activities that may be affected by the specified threat will be included as courtesy copy addressees.

d. The ASCC will confirm receipt on all follow-up reports.

e. Further updates should be submitted when additional substantive information concerning the terrorist threat becomes available. Such reports will be submitted upon receiving the information by email message directly from ASCC receiving the information to the addressees in paragraph C–1. All courtesy copy addressees for the initial report will be provided in this and future updates.

f. All TTWR will use an OPREP–3 (see Chairman of the Joint Chiefs of Staff manual (CJCSM) 3150.05D located at https://jsportal.sp.pentagon.mil/sites/matrix/del/sitepages/home.aspx) or similar format (that is, the sending command's report format).

g. Updates will provide additional information, as available, concerning the following:

(1) Type of incident threatened.
(2) Possible targets.
(3) Type of weapons/explosive devices to be used.
(4) Likely perpetrators.
(5) Source of information.
(6) Local FPCON prior to receipt of threat.
(7) U.S. and HN actions taken, if any, since receiving the threat.
(8) Any additional amplifying information.

C–2. Terrorist incident report [Requirement Control Symbol exempt: AR 335–15, para 5–2e(2)]

a. TIR reporting requirements in this section apply to ASCCs assigned to GCCs.

b. Upon receipt of information that a terrorist incident or suspected terrorist incident has occurred involving Army personnel (Soldiers, Civilian employees, or their Family members), facilities, civil works and like projects, or other assets, an initial TIR will be provided immediately by the ASCC via telephone to the AOC (phone DSN (312) 225–4695 or commercial (01) (703) 695–4695). A "suspected terrorist incident" is one in which involvement by terrorists has not been verified by lead agencies conducting the investigation. Initial reports will include the date and time of the attack, number of personnel participating in the attack, specifics of demands, casualties to U.S. Army personnel, a general description of damage to U.S. Army facilities, and actions taken in response to the incident. Updated telephonic reports will be provided to the AOC every even hour for the duration of an incident.

c. Within 6 hours of an actual or suspected terrorist incident involving U.S. Army personnel or facilities, an updated TIR will be submitted by email message to the AOC at usarmy.pentagon-e.hqda.mbx.armywatch@mail.mil (unclassified) or usarmy.pentagon.hqda.mbx.armywatch@mail.smil.mil (classified). Simultaneously, courtesy copies of the follow-up report will be provided to—

(1) AT Division, PMG.
(2) ARTIC, PMG.
(3) Headquarters, USACIDC.
(4) U.S. Army Counterintelligence-Law Enforcement Center.

d. The ACOM or DRU with responsibility for the location of the incident will be included as courtesy copy addressees.

e. The TIR will be as complete as possible, with omitted information transmitted as soon as known. The ASCC will confirm receipt on all follow-up reports.

f. A complete description of the terrorist incident, including the following will be included in the report:

(1) Type of incident and location.
(2) Date and time of incident.
(3) Detailed description of incident.
(4) Weapons/explosives used.
(5) Likely perpetrators.
(6) Claims of responsibility.
(7) Number of personnel killed and number of personnel injured and their conditions.
(8) Threats received prior to the incident that could be related.
(9) Local FPCON prior to the incident.
(10) Other AT measures in effect prior to the incident.
(11) U.S. and HN actions taken since the incident.
(12) Any amplifying information available.

C–3. Terrorist threat/incident after action report [Requirement Control Symbol exempt: AR 335–15, para 5–2e(7)]

a. Terrorist Threat/Incident AAR reporting requirements in this section apply to ASCCs assigned to GCCs.

b. Terrorist Threat/Incident AAR, containing comprehensive discussion of lessons learned, will be forwarded by ASCCs, to HQDA, DCS, G–3/5/7 (DAMO–ODF) and Office of the Provost Marshal General (OPMG) (DAPM–MPO)) and the CALL within 45 days of a reported terrorist threat or terrorist incident.

C–4. Force Protection Condition Report [Requirement Control Symbol exempt: AR 335–15, para 5–2e(2)]

a. FPCON reporting requirements in this section apply to ASCCs assigned to GCCs.

b. ASCCs are responsible for monitoring and reporting FPCONs and FPCON changes of all Army elements (commands, units, installations, activities) for which they have AT responsibility.

c. ASCCs will maintain a reporting system within their respective commands and all Army elements for which they have AT responsibility.

d. ASCC-wide FPCON changes will be reported to HQDA in accordance with the following procedures:

(1) If the change involves FPCONs Normal, Alpha, and or Bravo, an initial report will be provided telephonically to the AOC within 6 hours (phone DSN (312) 225–4695 or commercial (01) (703) 695–4695). If the change involves FPCONs Charlie and/or Delta, initial report will be provided immediately.

(2) A follow-up report (OPREP–3 or similar format) will be provided by email message to the AOC.

(3) Simultaneously, courtesy copies of the follow-up report will be provided to:

(a) AT Division, OPMG.
(b) ARTIC, OPMG.

(4) Message will include a complete explanation of the rationale for implementing the change. General statements such as “change is due to an increase in the terrorist threat” are not acceptable.

(5) FPCON changes will describe by the FPCON and the additional measures from higher levels, as appropriate (for example, FPCON Alpha in accordance with paragraphs B–3, B–5 through B–7, and C–4). The use of FPCON “Plus” will not be used.

(6) ASCCs will report FPCON changes implemented by their subordinate commands in accordance with the following guidance:

(a) ASCCs will report FPCON changes of subordinate commands if they involve a change to/from FPCONs Alpha, Bravo, Charlie and/or Delta. This does not absolve Army commanders from maintaining oversight over FPCON postures of all their subordinate commands.

(b) Initial report will be provided telephonically to the AOC in accordance with paragraph C–4*d*(1).

(c) A follow-up report will be provided to the AOC in accordance with paragraph C–4*d*(2).

(7) Unless reported in the daily situation report to the AOC, ASCCs will provide monthly FPCON reports to HQDA in accordance with the following procedures:

(a) ARTIC, OPMG.

(b) Simultaneously provide courtesy copies to—

1. ARTIC, OPMG: usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@mail.mil (unclassified) or usarmy.pentagon.hqda-dcs-g-2.list.dami-artic@mail.smil.mil (classified).
2. AT Division, OPMG.

(c) Monthly reports will include the following:

1. Overall ASCC FPCON. In most cases, this is the baseline FPCON level established by the GCC.
2. Any measures implemented from higher FPCON as part of baseline. Do not include RAM (list by measure number).
3. Exceptions to the overall ASCC FPCON (with rationale), including countries, subordinate commands, or installations that have implemented a FPCON other than the ASCC FPCON.

Appendix D

Antiterrorism Training Requirements

D–1. Level I, Antiterrorism awareness training

a. View a DA, 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 AT Awareness training course are not required to view an awareness video.

b. Level I AT Awareness Instruction will include at least the following:

(1) Introduction to terrorism.

(2) Terrorist tactics and operations.

(3) Individual protective measures.

(4) Personal protective measures for CBRNE attacks to include sheltering in place or evacuation, indicators of CBRNE attack (including TIH), impromptu methods of decontamination, and so forth.

(5) Terrorist surveillance techniques.

(6) Improvised explosive device attacks.

(7) Kidnapping, hostage survival, and personnel recovery.

(8) Explanation of terrorist threat levels and FPCON System levels and measures.

(9) Active shooter.

(10) Social media (that is, terrorist use of, and OPSEC).

(11) Insider threat.

(12) Familiarization with CJCS Guide 5260.

(13) Supplemental training focusing on emerging terrorist threat tactics and capabilities.

c. All DOD personnel should be provided and retain personal copies of Chairman of the Joint Chiefs of Staff (CJCS) Guide 5260 and CJCS Pocket Card 5260. Local reproduction of both CJCS issuances is authorized.

D–2. Level II, Antiterrorism officer training

a. The training described below applies to E–6 to O–5 military personnel or GS–5 and above DOD Civilian employees certified to serve as the commander's AT advisor and provide AT instruction.

b. Training required: Attend an Army approved AT Officers Course based a TRADOC (U.S. Army Military Police School) approved program of instruction that teaches a minimum of the following topics (requirements are identified by installation ATO (I), Unit ATO (U), or both (I/U)):

(1) (I/U) Understanding AT Roles and Responsibilities.

(a) (I) Understand DOD, Army, and applicable Agency/Field Activity Policy.

(b) (I/U) Understand current AT standards.

(c) (I/U) Access references to DOD issuances (directives/instructions) at http://www.dtic.mil/whs/directives.

(d) (I/U) Understand online DOD System of Record used to track vulnerabilities.

(e) (I) Understand necessary coordination with HN, GCCs, DOS, U.S. Embassies, and other government agencies.

(2) (I/U) Understanding minimum required AT Program elements:

(a) (I/U) Risk management.

(b) (I/U) AT planning.

(c) (I/U) Training and exercises.

(d) (I/U) Resource application.

(e) (I/U) Comprehensive program reviews.

(3) (I/U) How to Organize AT Groups:

(a) (I) Command and staff relationships on an installation.

(b) (U) Command and staff relationships in contingency and Joint Operations.

(c) (I) ATWG.

(d) (I) TWG.

(e) (I) ATEC.

(f) (U) Establishing the ATWG, TWG, and ATEC in a contingency environment.

(g) (U) Understanding operations center functions.

(4) (I/U) Risk Management Considerations.

(a) (I/U) Threat assessments.

1. (I/U) Identify terrorism.

2. (I) Terrorist tactics and operations.

3. (U) Terrorist tactics and operations in a contingency environment.
4. (I) Domestic and international terrorist threat.
5. (I) Intelligence and CI integration.
6. (I/U) Practical exercise-conducting a threat assessment.

(b) (I/U) Criticality assessments.

1. (I) Assessment methodology for an Installation.
2. (I/U) Practical exercise-conducting a criticality assessment.

(c) (I/U) Vulnerability assessments.

1. (I) Assessment methodology for an installation.
2. (U) Assessment methodology in a tactical environment.
3. (I/U) Practical exercise - conducting a vulnerability assessment.

(d) (I/U) Risk assessments.

1. (I/U) Assessment methodology.
2. (I/U) Practical exercise-conducting a risk assessment.

(5) (I/U) Create and Execute AT Programs.

(a) (I/U) Use of terrorism threat levels and FPCON.

(b) (I/U) Site specific protective measures.

(c) (U) Establishing access control points/entry control points in contingency operations.

(d) (U) Barrier planning in contingency operations.

(e) (U) Establishing electronic detection and security capability in contingency operations.

(f) (I/U) Mitigating vulnerabilities.

(g) (I/U) Use of RAM.

(6) (I/U) Prepare AT plans.

(a) (I/U) Templates and planning tools.

(b) (I/U) Minimum essential AT plan elements.

(c) (I/U) How to develop and write plans.

(d) (U) How to integrate AT plans with base defense/tactical operations.

(e) (I) CBRNE (including TIH) and WMD Considerations.

(f) (I) Vehicle bomb search planning.

(g) (I/U) Vehicle Inspection Checklist.

(h) (U) Deployment/in-transit considerations.

(7) (I/U) Determine AT resource management.

(a) (I/U) Vulnerability identification and management, resource application, and prioritization using the DOD System of Record.

(b) (I/U) CCIF.

(c) (I/U) Identify physical security and construction requirements.

(d) (I/U) Identify communications systems requirements.

(8) (I/U) Conduct AT training.

(a) (U) Conduct and oversee Level I AT Awareness training.

(b) (I) Develop AT exercise plans.

(c) (I/U) Obtain AOR-specific updates for deployments and travel areas.

(9) (I) Case studies - installation based.

(10) (U) Case studies - contingency operations.

(11) (I) Legal considerations.

(12) (I) Interagency and HN responsibilities and jurisdictions.

(13) (I) Special law enforcement considerations.

(14) (I/U) Access to DOD AT lessons learned databases.

(15) (I) Familiarization with HRB/HRP requirements.

(16) (I) AT considerations in contracting.

(17) Methodologies to ensure adherence to common criteria and minimum construction standards

c. Review of the following Army, DOD and Joint Staff and applicable Military Department, Defense Agency, or DOD Field Activity publications:

(1) (I/U) AR 525–13.

(2) (I) DODI 2000.12.

(3) (I/U) DODI O–2000.16.

(4) (I/U) DODI 0–2000.22.

(5) (I/U) DODI 2000.26.
(6) (I/U) DODI 3020.52.
(7) (I/U) CJCS Guide 5260.
(8) (I/U) Antiterrorism Officer Guide.
(9) (I/U) UFC 4–010–01 and 4–010–02.
(10) (I/U) DODD 4500.54E Change 1.
(11) (I/U) DOD Electronic Foreign Clearance Guide.
(12) (I/U) Joint publication (JP) 3–07.2.

D–3. Level III, Pre-command antiterrorism training

a. The training described below applies to O–5/O–6 commanders/command select (and civilian equivalent director position).

b. Level III, Pre-command AT training will be conducted in the Army pre-command (PCC) training courses conducted at branch, component, and functional schools and include the following:
(1) Understanding AT responsibilities and minimum AT Program elements.
(a) Understanding policy.
(b) Staff AT roles.
(c) Duties and responsibilities of the ATO.
(d) Risk management and risk assessments.
(e) AT planning.
(f) AT training and exercises.
(g) AT resource allocation.
(h) Comprehensive AT Program review.
(i) Installation integration with U.S. Country Team.
(j) Explanations of Homeland Security Presidential Directive 5, Presidential Policy Directive 8, and how DOD agencies and installations are integrated into and affected by the National Frameworks for Protection, Prevention, Mitigation, Response, and Recovery.
(k) All pre-command AT training recipients should made aware of the requirements and location of JP 3–07.2.
(2) Ensuring preparation of AT plans.
(a) Baseline FPCON posture.
(b) Mitigating CBRNE (including TIH)/WMD attack/risks.
(c) MOUs, MOAs, and MAAs.
(3) Ensuring conduct of AT planning.
(a) AT plans and training.
(b) Level I training.
(c) Level II training.
(4) Organizing AT groups.
(a) ATWG.
(b) TWG.
(c) ATEC.
(5) Understanding the local threat picture.
(a) Potential sources of law enforcement-derived FP information.
(b) Fusion of intelligence, counterintelligence, and law enforcement information.
(c) Terrorism threat levels.
(6) Building a sustainable AT Program (DOD System of Record capabilities).
(7) Executing resource responsibilities.
(a) AT resourcing program.
(b) Role of DOD System of Record in resource process.
(c) Construction standards.
(8) Understanding use of force and rules of engagement (terrorist scenarios and hostile intent decision making).

c. Review of the following Army, DOD and Joint Staff publications:
(1) (I/U) AR 525–13.
(2) (I) DODI 2000.12.
(3) (I/U) DODI O–2000.16.
(4) (I/U) DODI 3020.52.
(5) (I/U) DODI 2000.12.

(6) (I/U) CJCS Guide 5260.
(7) (I/U) UFC 4–010–01 and 4–010–02.
(8) DOD 4500.54E.

D–4. Level IV, Antiterrorism executive seminar training

a. The training described below applies to O–6 to O–8 commanders (and civilian equivalent director/ senior executive service civilian employee position) responsible for AT Programs, policy, planning and execution.

b. Training required: Executive level seminar hosted by the J–3 Deputy Director for AT/Homeland defense, J–34. The training provides pertinent briefings, current updates and panel discussion topics. Seminar includes a tabletop AT and Consequence Management war games that facilitate interaction & discussion on power projection, WMD, FPCON management and AT implementation.

Appendix E

Antiterrorism standards/command-level matrix

The following matrix (table E–1) portrays which AT standards must be implemented by higher headquarters (ACOM, ASCC, and DRU), installation/garrison, unit, tenant, and SAF commanders as specified in paragraphs 2–24 through 2–29.

Table E–1
Antiterrorism standards/Command-level Matrix—Continued

AT Standard	ACOM, ASCC, DRU	Installation and garrison	Unit	Tenant	SAF
Standard 1, AT Program Elements	X	X	X	X	X
Standard 2, Intelligence Support to the Army AT Program	X	X	X		X
Standard 3, AT Risk Management	X	X	X	X	X
Standard 4, Terrorist Threat Assessment	X	X	X	X	X
Standard 5, Criticality Assessment	X	X	X	X	X
Standard 6, Terrorist Vulnerability Assessment	X	X	X	X	X
Standard 7, AT Plan	X	X	X	X	X
Standard 8, AT Program Coordination	X	X	X	X	X
Standard 9, ATO/Antiterrorism Coordinator	X	X	X	X	X
Standard 10, Antiterrorism Working Group	X	X			X
Standard 11, Threat Working Group	X	X			X
Standard 12, AT Executive Committee	X	X			
Standard 13, AT Physical Security Measures	X	X	X	X	X
Standard 14, Random Antiterrorism Measures	X	X	X	X	X
Standard 15, AT Measures for Off-Installation Facilities, Housing, and Activities	X	X	X	X	X
Standard 16, AT Measures for HRP	X	X	X	X	X
Standard 17, AT Construction and Building Considerations	X	X	X	X	X
Standard 18, AT Measures for Logistics and Other Contracting	X	X	X	X	X
Standard 19, AT Measures for Critical Asset Security	X	X	X		
Standard 20, Terrorism Incident Response Measures	X	X	X	X	X
Standard 21, Terrorism Consequence Management Measures	X	X		X	X
Standard 22, FPCON Measures	X	X	X	X	X
Standard 23, AT Training and Exercises	X	X	X	X	X
Standard 24, Formal AT Training	X	X	X	X	X
Standard 25, Level I AT Awareness Training	X	X	X	X	X
Standard 26, Level II ATO Training	X	X	X	X	X
Standard 27, Level III Pre-Command AT Training	X	X	X	X	X
Standard 28, Level IV Executive Seminar	X	X	X	X	X
Standard 29, AOR-specific Training for DOD Personnel and In-transit Forces	X	X	X	X	X

Table E–1
Antiterrorism standards/Command-level Matrix—Continued

Standard 30, AT Resource Requirements	X	X	X	X	X
Standard 31, AT Program Review	X	X	X	X	X
Standard 32, AT Program Review Teams	X				
Standard 33, Incorporation of AT into Command Information Programs	X	X	X	X	X
Standard 34, Terrorist Threat/Incident Reporting	X	X	X	X	X

Appendix F

Unified facilities code requirement waiver and exception

F–1. Unified facilities code requirement waiver and exception process

a. The ASA (IE&E) is designated as the approval authority for granting Army waivers and exceptions to the requirements contained in paragraphs 2–9*a* and 2–9*b*.

b. DCS, G–9 is responsible for mandating compliance with UFC 4–010–01 and UFC 4–010–02 for construction of new facilities and major renovations.

c. The Army UFC waiver exceptions process does not apply to buildings located outside of the United States, where GCC has sole waiver and exception authority.

d. All commanders (or civilian equivalent positions) seeking waivers and exceptions to requirements contained in paragraphs 2–9*a* and 2–9*b* for any building or portion of a building (permanent, temporary or expeditionary-owned, leased, privatized or otherwise occupied, managed or controlled by DOD) will submit requests per paragraph F–3.

e. Waivers and exceptions will be considered individually. Blanket waivers and exceptions will not be authorized. Requests for waivers and exceptions will be made by installation or activity commanders (or civilian equivalent position), endorsed by senior commanders and the chain of command (responsible ACOM, ASCC, DRU, ARNG, or the USAR) to the DCS, G–9 for HQDA coordination. Upon completion of HQDA coordination, DCS, G–9 will prepare a recommendation and forward waiver requests to ASA (IE&E) for final approval. The installation/activity and the endorsing headquarters will retain the approved waiver or exception, including documents listed in paragraphs F–2 and F–3.

F–2. Waivers

a. Waivers may be requested where UFC standard(s) not being met can be corrected in no more than 5 years. Waivers will be granted for a period of 5 years and may be extended after a review of the circumstances necessitating the extension.

b. Waivers require justification. Waiver extensions will state first extension, second extension and so forth.

F–3. Exceptions

a. Exceptions may be requested where UFC AT standard(s) are not being met and cannot be corrected in less than 5 years. Approved exceptions are considered permanent but must be reviewed at least every 5 years (or earlier) when a significant change occurs in the threat or occupancy level or use of the building. Reviews will verify the need for exception extensions and will be conducted by installation or activity commanders (or equivalent civilian position) and endorsed by senior commanders and the chain of command (responsible ACOMs, ASCCs, DRUs, ARNG or the Army Reserve). Provide copies of the review to DCS, G–9.

b. Exceptions are granted when meeting the UFC AT standards(s) is not possible. However, mitigation efforts must be implemented.

c. For new construction or existing building undergoing major modifications/renovations, approval for exceptions will be rare. However, where a particular standard cannot be met, requesting officials must provide specific and strong justification and mitigating measures, affording equivalent security to those facilities under standard criteria.

d. Requests for waivers and exceptions will contain compensatory measures currently in effect or recommended. Approvals for waivers and exceptions will specify required compensatory measures. Equivalent protection exceptions do not require compensatory measures.

e. Requests for waivers or exceptions to requirements within paragraphs 2–9*a* and 2–9*b* will be coordinated between the ATO, supporting engineer, supporting Staff Judge Advocate, Directorate of Emergency Services, DPTMS, and Provost Marshal Office or equivalent positions of the installation or activity.

F–4. Waiver and exceptions requests for transitional buildings

a. Will only be considered where it is important to bring such a building into compliance with UFC AT standards due to short-term occupancy or when it is impractical to vacate a non-compliant building renovation.

b. Remaining occupied during renovation must include a mitigation plan for brining into compliance which has been coordinated and certified by the USACE Protective Design Center.

c. A request for a waiver or exception will include—

(1) A statement identifying the problem/deficiencies constituting standards below those cited in paragraphs 2–9*a* and 2–9*b*.

(2) Compensatory measures planned for the building(s) to make up for noncompliance with required UFC AT standards.

(3) Completed risk assessments and mitigation plans for bringing the building(s) into compliance with UFC AT standards.

(4) Reasons the activity or installation cannot comply with the requirements of the UFC including engineering analysis (where applicable).

(5) Documentation of coordinated efforts with the affected staff agencies (ATO, DPTMS, Directorate of Emergency Services PM/SO, supporting judge advocate general, and supporting engineers (or equivalent positions of the installation or activity)).

(6) The commander's statement of corrective action taken or planned to meet UFC AT standard(s) requiring the waiver or exception.

(7) Each successive commander's recommendation and endorsement.

F–5. Headquarters, Department of the Army Staff Coordination

Prior to a waiver of exception request being forwarded to ASA (IE&E), DCS, G–9 will coordinate with the following organizations for review/concurrence:

a. Office of the DCS, G–3/5/7 (G–34).

b. Office of the DCS, G–2.

c. OPMG.

d. Office of The Judge Advocate General.

e. Headquarters, USACE (request review and certifications by USACE Protective Design Center).

Appendix G

Guidance for Review/Verification of Antiterrorism Measures for Contracting

G–1. Review/verification process

a. Paragraph 5–19 requires organizational ATO review of each requirements package prior to submission to the supporting contracting activity and coordination with other staff elements, as appropriate, during the review.

b. Should the requiring activity not have an appointed ATO, a properly appointed and trained ATC may review a requirements package.

c. These procedures apply to all Army organizations in request and receipt of contracted services in Army operations world-wide to include the prime contractor and all sub-contractors as well as joint operations where the Army is the lead contracting agency.

G–2. Contract requirements package antiterrorism/operations security review cover sheet

a. The purpose of the cover sheet is to document review of the requirements package statement of work quality assurance surveillance plan and any applicable source selection evaluation for AT and other related protection matters, that include AT, OPSEC, information assurance, physical security, law enforcement, intelligence and foreign disclosure.

b. The contract requirements package AT /operations security review cover sheet process will act as the default review (except for supply contracts) under the simplified acquisition level threshold, field ordering officer actions and Government card purchases. Command policy may require this form for supply contracts under the simplified acquisition level threshold.

c. The cover sheet will be signed by the reviewing ATO and OPSEC officer (or ATC as necessary) and will be included as part of the requirements package.

d. Commands may modify the AT/OPSEC cover sheet to fit local command circumstances, policies, and procedures, however, the revised format must comply with Army AT policy expressed in Standard 18 of this regulation and address the categories identified in paragraph G–3.

e. Instructions for using the AT/OPSEC cover sheet are available on the ATEP located in the "AT in Contracting" folder at https://army.deps.mil/army/sites/pmg/opmg/ops/antiterror/atep/default.aspx.

G–3. Antiterrorism/operations security standard contract language/contract clause applicability and statement of work language

a. When the current contract language is not sufficient to meet AT requirements, the ATO/ATC will need to provide standard contract language to address specific AT requirements.

b. Standard contract language is readily available on the ATEP located in the "AT in Contracting" folder at https://army.deps.mil/army/sites/pmg/prog/atep/at%20in%20contracting/forms/allitems.aspx.

c. Standard contract language may be applied to the following categories:

(1) AT Level I AT Awareness training.

(2) Access and general protection/security policy and procedures—

(a) Contractors requiring common access cards.

(b) Contractors not eligible for common access cards, but requiring assess to a DOD facility or installation.

(3) AT Awareness training for U.S. based contractor personnel traveling overseas.

(4) iWATCH training.

(5) Army Training Certification Tracking System registration for contractor employees who require access to government information systems.

(6) Contracts that require a formal OPSEC program.

(7) Requirement of OPSEC training.

(8) Information assurance/information technology training.

(9) Information assurance/information technology certification.

(10) Contractor authorized to accompany the force clause.

(11) Contractor requiring performance or delivery in a foreign country.

(12) Handling to access to classified information.

(13) Threat Awareness Reporting Program.

d. ATOs will ensure coordination with the contracting officer representative regarding any necessary mitigation procedures to a reviewed contract.

Appendix H

Internal Control Evaluation

H–1. Function
The function covered by this evaluation is the management of Army AT Programs.

H–2. Purpose
The purpose of this evaluation is to assist commanders in evaluating the key internal controls outlined below. It is not intended to cover all controls.

H–3. Instructions
Answers must be based on the actual testing of key internal controls (for example, document analysis, direct observation, sampling, simulation, exercise, other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least annually in accordance with paragraph 5–32. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

H–4. Test questions
a. Standard 1. AT Program Elements.

(1) Does the AT Program contain the minimum required elements: risk management (Standard 3); planning (Standard 7); training and exercises (Standard 23); resource application (Standard 30); and comprehensive program review (Standard 31)?

(2) Are the AT Program elements developed and maintained in an iterative manner?

(3) Are the AT Program elements continuously refined to ensure the relevance and viability of all defensive measures employed to reduce vulnerabilities to terrorist capabilities?

(4) Are AT meetings, exercises, included in the organization's long range planning calendar?

b. Standard 2. Intelligence Support to the AT Program.

(1) Is the AT Program supported by all-source intelligence with PIR, CCIR, and focused collection, analysis, and dissemination to protect personnel, family members, facilities, civil works and other projects, and information in all locations and situations?

(2) Are production and analysis requirements focused and based on PIR and CCIR? Are PIR and CCIR reviewed for currency, revalidated at least annually, and updated whenever appropriate to meet changing threats and/or requirements?

(3) Is terrorist intelligence information developed, collected, analyzed, and disseminated in a timely manner?

(4) Is current intelligence integrated into the AT training program?

(5) Do the appropriate intelligence organizations collect and analyze threat information?

(6) Do the appropriate law enforcement organizations collect and analyze criminal threat information?

(7) Are units in transit provided with tailored terrorist threat information?

(8) Are counter surveillance, surveillance detection, counterintelligence, and other specialized skills integrated as a matter of routine in all AT Programs?

(9) Is an official identified as the focal point for the integration of operations and local or HN intelligence, CI, and criminal intelligence information?

(10) Are proactive techniques incorporated to deter and detect terrorists, particularly in support of assets or activities in areas designated with SIGNIFICANT or HIGH threat levels? Do these activities include: in-transit forces, HRP, special events, and high-value military cargo shipments?

(11) Are collection operations being conducted consistent with the requirements of AR 381–10, AR 381–12, AR 380–13, DODD 5200.27, and other applicable regulations and directives?

(12) Does the command have appropriate connectivity to receive threat-related information from all available sources (for example, ARTIC, FBI, ACIC, USACIDC, provost marshal, local law enforcement, Intelink-S, and Intelink)?

(13) Does the command use the DOD Intelligence Production Program to validate and receive IC support for terrorism analysis and products to support their AT Programs that are beyond the capabilities of the intelligence organizations under their command?

(14) If commanders do not have organic intelligence or law enforcement elements to meet the requirements of this standard, has such support been coordinated through their higher headquarters?

c. Standard 3. AT Risk Management.

(1) Is risk management integrated in the planning, coordinating, and developing of AT plans, orders, operations, and exercises?

(2) Are leaders at all levels aware of how to integrate risk management into troop leading procedures and AT planning when conducting any mission or operation in accordance with ATP 5–19 and DA Pam 190–51?

(3) Are risk assessments conducted to integrate threat assessment (Standard 4), criticality assessment (Standard 5), and vulnerability assessment (Standard 6) information in order to make conscious and informed decisions to commit resources or enact policies and procedures that either mitigate the threat or define the risk?

(4) While conducting risk assessments, does the commander consider factors of threat, asset criticality, and vulnerability of facilities, programs, and systems?

(5) Do the risk assessments analyze the following elements: the terrorist threat; the criticality of assets; the vulnerability of facilities, programs, and systems to terrorist threats, including use of CBRNE or similar capabilities; and the ability to conduct activities to deter terrorist incidents; to employ countermeasures; to mitigate the effects of a terrorist incident; and to recover from a terrorist incident?

d. Standard 4. Terrorism threat assessment.

(1) Is a terrorism threat assessment process established that identifies the full range of known or estimated terrorist threat capabilities (including CBRNE and WMD), methods of operation, and possible courses of action?

(2) Are terrorism threat assessments updated on an annual basis?

(3) Are terrorism threat assessments tailored to local conditions and address terrorist groups' operational capabilities, intentions, and activity, and whether the operational environment is conducive to terrorist activity?

(4) Is the DOD Terrorist Threat Level classification system used to identify the threat in a specific overseas country?

(5) For ACOM, ASCC, and DRU commanders—

(a) Is terrorist threat information, based on the annual comprehensive DA annual terrorist threat statement, incorporated into command annual terrorist threat assessment?

(b) Are copies of the command annual terrorist threat assessment forwarded to their subordinate elements within 90 days of receipt of the DA annual threat statement?

(6) Are terrorism threat assessments prepared and classified in accordance with AR 381–11?

(7) Are the results of terrorist threat assessments disseminated to all affected organizations (for example, organic, tenant, and supported RC units)?

(8) Are effective processes implemented to integrate and fuse all sources of available threat information from local, State, Federal, HN law enforcement agencies; the appropriate local, State, Federal, HN 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?

(9) Are specific terrorism threat assessments prepared 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 graduation ceremonies, and events open to the public (that is, armed forces day celebrations)?

(10) Are terrorism threat assessments: integrated into the risk management process; a major source of analysis and justification for recommendations to raise or lower FPCON levels, implementation of RAM, AT enhancements including Physical Security Program changes, program and budget requests; and a basis for conducting terrorism vulnerability assessments?

(11) Are terrorism threat assessments a part of leader's reconnaissance in conjunction with deployments?

(12) Are follow-on threat assessments conducted for all deployments as determined by the commander, or directed by higher headquarters?

(13) Are consolidated (MI and criminal intelligence data) terrorism threat assessments filed, stored, and maintained within operational channels (that is, provost marshal, USACIDC, DCS, G–3/5/7/DPTMS/and so forth) due to AR 381–10 restrictions on U.S. person information?

e. Standard 5. Criticality assessment.

(1) Is a criticality assessment conducted to identify, classify, and prioritize mission-essential assets, facilities, resources, and personnel?

(2) Is a criticality assessment conducted to identify, classify, and prioritize non mission-essential assets such as high-population facilities, mass gathering activities, and any other facility, equipment, service, or resource deemed sufficiently important by the commander warrant protective measures to ensure continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration?

(3) Is the criticality assessment updated annually?

(4) Is the criticality assessment used to produce a prioritized AT Critical Facilities List, which is based on the following factors: relative importance; effect of loss; recoverability; mission functionality; substitutability; and reparability?

(5) Is the criticality assessment used to provide the basis for identifying those assets, facilities, resources, and personnel that require specific protective measures and priorities for resource allocation when developing and updating the AT plan?

(6) Did the program consider the possibility of redundancy for critical functions/assets?

f. Standard 6. Terrorism vulnerability assessment.

(1) Are terrorism vulnerability assessments conducted at least annually or more frequently if the terrorist threat assessment or mission requirements dictate?

(2) Are terrorism vulnerability assessments conducted at a minimum for, but not limited to—

(a) Any installation, facility, or activity populated daily by DOD personnel?

(b) Any installation, facility, or activity possessing responsibility for emergency response or physical security plans and programs, or determined to be critical infrastructure?

(c) Any Army installation, facility, civil work project, or activity possessing authority to interact with local non-military or HN agencies or having agreements with other agencies or HN agencies to procure these services?

(d) Any deploying units, whether the deployment is for an exercise or operational mission/support?

(e) Any off-installation DOD 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 Standard 3?

(f) Any events or activity determined to be a special event involving a gathering of 300 or more DOD personnel (that is, battle assemblies, drill assemblies, Independence Day, and Armed Forces Day celebrations)?

(3) For deploying units—

(a) Are terrorism vulnerability assessments a part of unit leader's reconnaissance?

(b) Are follow-on terrorism vulnerability assessments conducted for all deployments as determined by the commander or directed by higher headquarters?

(4) For special events involving a gathering of 300 or more DOD personnel—

(a) Are terrorism vulnerability assessments integrated into the planning process for special events?

(b) Are considerations for the protection and control of large volumes of pedestrian and vehicle traffic included?

(5) Is classified information, derived from terrorism vulnerability assessments, done in accordance with the requirements outlined in the DTRA JMAA Security Classification Guide?

(6) Are terrorism vulnerability assessments conducted consistent with the principles outlined in DODI 2000?

(7) Within 90 days of the completion of a terrorism vulnerability assessment—

(a) Are identified vulnerabilities prioritized/tracked?

(b) Is a plan of action developed to mitigate or eliminate the vulnerabilities?

(c) Are all vulnerabilities documented by any assessment or any higher headquarters vulnerability assessment reported to the first general officer or civilian equivalent director in the chain of command and to their higher headquarters (ACOM, ASCC, or DRU)?

(8) Are higher headquarters (ACOM, ASCC, or DRU) tracking all reported vulnerabilities of their subordinate organizations and/or installations to resolution/closure?

(9) Are terrorism vulnerability assessment results populated into the DOD System of Record within 120 days from the completion of the assessment?

(10) Are higher headquarters assessment results populated into the DOD System of Record within 120 days from the completion of the assessment?

(11) Do terrorism vulnerability assessments serve as a basis and justification for AT plans, enhancements, program/budget requests, and establishment of FPCONs?

(12) Is continuous assessment of daily routine and activities in operational environments accomplished to ensure the threat is known and appropriate measures are in place to mitigate the vulnerabilities?

g. Standard 7. AT Plan.

(1) Are the required comprehensive, proactive AT plans, orders, or other implementing guidance developed and maintained in the applicable organizations within the command: installation/garrison, SAF, unit (battalion or higher) levels, units participating in training and operational deployments (50 or more personnel), units participating in training exercises (50 or more personnel), and special events (that is, Independence Day and Armed Forces Day celebrations)?

(2) Are the required comprehensive, proactive AT plans, orders, or other implementing guidance signed by the commander and exercised?

(3) At a minimum, does the AT plan address: the essential AT Program elements (see Standard 1) and standards addressed in this regulation; specific threat mitigation measures to establish a local baseline defensive posture; the local defensive posture will facilitate systematic movement to and from elevated security postures, including the application of RAM; AT physical security measures; AT measures for HRP when appropriate; AT construction and building considerations; AT measures for logistics and other contracting; AT measures for Critical Asset Security; AT measures for in transit

movements when appropriate; terrorism incident response measures; terrorism consequence management measures, including CBRNE and WMD planning, and measures to deal with TIH, that is, TIC/TIM; and FPCON implementation measures, including site-specific AT measures?

h. Standard 8. AT Program Coordination.

(1) Are AT matters coordinated with all subordinate, supporting, supported, and tenant activities; HN authorities; and local, State, and Federal authorities pursuant to existing law and DA policy to support AT planning and program implementation?

(2) Are all tenants and supported RC units/activities included in the AT planning process and are they included in AT plans, providing guidance and assistance as required?

(3) Do your subordinate elements, which are tenants of other installations/facilities, comply with host installation/facility AT requirements, participate in the host installation/facility AT planning process, and provide personnel support for the implementation of host installation/facility FPCON levels specified in the host installation/facility AT plans?

(4) Are AT plans coordinated with local, State, and Federal authorities to ensure a complete understanding of how and what military or civilian support will be rendered in an event of a terrorist incident?

(5) For OCONUS commanders—

(a) Are all applicable HN agreements complied with when planning and executing AT operations?

(b) Is liaison established with HN authorities to ensure a complete understanding of what HN support is available and how it will be rendered in an event of a terrorist incident?

(c) Are AT plans coordinated with the appropriate GCC and U.S. Embassy or Consulate.

(d) Are copies of approved AT plans provided to appropriate higher headquarters and Country Team officials in accordance with GCC established policy?

i. Standard 9. ATO.

(1) For ACOM, ASCC, and DRU commanders and CNGB: Is an ATO (minimum grade of O–4 or equivalent civilian grade) appointed in writing within the operations function or a special staff organization that is best suited to execute the program (DCS, G–3/5/7 and so forth)?

(2) For garrison commanders: Is an ATO (minimum grade of O–3 or equivalent civilian grade) appointed in writing within the operations function or a location that is best suited to execute the program (DCS, G–3/5/7/DPTMS and so forth)?

(3) For battalion and brigade-level commanders: Is an ATO appointed in writing (minimum grade of E–6 or higher or equivalent civilian grade)?

(4) For division and corps-level commanders: Is an ATO appointed in writing (minimum grade of E–8 or higher or equivalent civilian grade)?

(5) For a deploying unit having 300 or more individuals assigned or under the operational control of a designated commander: Is a Level II-certified ATO appointed (minimum grade of E–6 or higher or equivalent civilian grade)?

(6) For SAFs: Has the commander determined the need to assign an ATO or ATC?

(7) For USACE commanders and directors: Is an ATO (minimum grade of E–6 or higher or equivalent civilian grade) appointed in writing within the operations function or a location that is best suited to execute the program DCS, G–3/5/7/DPTMS and so forth?

j. Standard 10. ATWG.

(1) For commanders of ACOMs; ASCCs; DRUs; headquarters, ARNG; Army garrisons; and SAFs (populated daily by 300 or more personnel): Is an ATWG established?

(2) Does it meet semi-annually or more frequently, depending upon the level of threat activity?

(3) Does it oversee the implementation of the AT Program?

(4) Is it utilized to develop and refine AT plans?

(5) Does it address emergent or emergency AT Program issues?

(6) Does ATWG membership include the commander or designated representative (that is, Deputy Commander, CoS, G–3, and so forth); ATO; representatives of the commander's principal staff; CBRNE expertise; tenant unit representatives: and other representatives as required supporting AT planning and program implementation?

(7) For unit commanders (battalion level and above): Are the functions of an ATWG integrated into unit planning and operations (that is, routine command/staff meetings, long range planning calendar briefings, quarterly training briefings)?

k. Standard 11. TWG.

(1) For commanders of ACOMs; ASCCs; DRUs; HQ, ARNG; Army garrisons; and SAFs (populated daily by 300 or more personnel): Is a TWG established?

(2) Does it meet quarterly or more frequently, depending upon the level of threat activity?

(3) Is it utilized to develop and refine terrorism threat assessments and coordinate and disseminate threat warnings, reports, and summaries?

(4) Does it include a formal process for fusing all intelligence/information?

(5) Does TWG membership include the commander or designated representative (that is, Deputy Commander, CoS, G–3/5/7, and so forth); ATO; representatives of the commander's principal staff; tenant unit representatives; and appropriate representatives from direct-hire, contractor, local, State, Federal, and HN law enforcement agencies and the IC?

(6) For unit commanders (battalion level and above): Are the functions of a TWG integrated into unit planning and operations (that is, routine command/staff meetings, long range planning calendar briefings, quarterly training briefings)?

l. Standard 12. AT Executive Committee (ATEC).

(1) For commanders of ACOMs; ASCCs; DRUs; HQ, ARNG; Army garrisons; and SAFs (populated daily by 300 or more personnel): Is an ATEC or similarly structured corporate body established?

(2) Does it meet at least semi-annually?

(3) Is it utilized to develop and refine AT Program guidance, policy, and standards?

(4) Does it act upon the recommendations of the ATWG and TWG?

(5) Does it assist in determining resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities?

(6) Does membership include the commander, his staff principals, and the ATO?

m. Standard 13. AT Physical Security Measures.

(1) Are the principles of the DA Physical Security Program (AR 190–13) applied and fully integrated into AT Plans to ensure employment of a holistic security system to counter terrorist capabilities?

(2) Are AT physical security measures multi-layered?

(3) Do AT physical security measures 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 audiovisual 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 intruder efforts); communication (command and control procedures); and response (trained and properly equipped security forces)?

(4) Are integrated 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 and commercial delivery companies), HRP protection, barrier plans, and facility standoff distances?

(5) Are the AT physical security measures that are incorporated into the AT plan executable with assets on hand, and are the execution and emplacement timelines factored into the AT plan?

n. Standard 14. Random AT Measures (RAM).

(1) Are RAM conducted as an integral part of all AT Programs?

(2) For garrisons: Does the garrison have a formally documented RAM Program, under the supervision of the AT officer?

(3) For garrisons: Does the RAM program include tenant units and commands in RAM planning and execution?

(4) Does the commander utilize the concept of RAM in providing AT for their unit?

(5) Are RAM implemented without set pattern, either in terms of measures selected, time, place, or other variables to maximize effectiveness and deterrence value?

(6) At a minimum, do RAM consist of the random implementation of higher FPCON measures or intensified site-specific FPCON measures in consideration of the local terrorist capabilities?

(7) Is the random use of other physical security measures used to supplement FPCON measures?

(8) Are RAM, in conjunction with site-specific FPCON measures, employed in a manner that portrays a robust, highly visible and unpredictable security posture from which terrorists cannot easily discern security AT patterns or routines?

o. Standard 15. AT Measures for off-installation housing, facilities, and activities.

(1) Does the AT Program include specific AT measures for off-installation facilities, housing, transportation services, daycare centers, and other activities used by or involving mass gathering of Army personnel and their dependent family members?

(2) All commanders: Do these AT measures include emergency notification and recall procedures?

(3) Garrison commanders: Do these AT measures include guidance for selection of off-installation housing, temporary billeting, and other facility use (including compliance with United Facilities Criteria (UFC) 04–010–01 for leased, newly constructed, and expeditionary buildings); physical security measures; CBRNE defensive measures; and shelter in place, relocation, and evacuation procedures?

(4) Garrison commanders: Are MAAs or other similarly structured protocols developed with the appropriate local, State, Federal, and HN authorities to coordinate security measures and assistance requirements to ensure the protection of Army personnel and their family members at off-installation facilities and activities?

p. Standard 16. AT Measures for HRP.

(1) Are personnel who are at a greater risk than the general population, by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat identified as HRPs?

(2) Are HRPs designated and protected in accordance with DODI O–2000.22 and AR 190–58?

(3) Do designated HRPs, including designated HRP family members, receive appropriate high-risk training (personal protection, evasive driving, AT awareness, and hostage survival)?

(4) Are the provisions of DOD C–4500.51, "DOD Non-Tactical Armored Vehicle Policy", complied with for the acquisition and use of non-tactical armored vehicles in support of the HRP security operations?

q. Standard 17. AT building and construction considerations.

(1) Are the construction and building standards prescribed in DOD 5200.8–R, UFC 4–010–01, and UFC 4–010–02 fully complied with regarding the adoption of and adherence to common criteria and minimum construction standards to mitigate vulnerabilities?

(2) Are lists targeted to address the appropriate level threat and vulnerability assessment and based on guidance contained in DODI 2000.12?

(3) In circumstances that require the movement of Army personnel or assets to facilities the U.S. Government had not previously used or surveyed, are procedures established that include AT standards as a key consideration in evaluating the suitability of these facilities for such use?

(4) For deploying commanders—

(a) Is a prioritized list of AT factors developed for site selection teams?

(b) Are these criteria used to determine if facilities either currently occupied or under consideration for occupancy by Army personnel provide adequate protection of occupants against the effects of a terrorist attack?

r. Standard 18. AT Measures for Logistics and Other Contracting.

(1) Has coordination been accomplished with the command's supporting Army contracting officer to ensure that AT measures have been incorporated into contracting actions?

(2) Does the commander have a mechanism in place to ensure the following items have incorporated into contracting actions?

(a) AT measures are incorporated into the logistics and contracting actions (requirements development, source selection/award, and contract execution) when the provisions of the contract or services provided affect the security of Army elements, personnel, or mission-essential cargo, equipment, assets, or services.

(b) The evaluation process for future contracts includes consideration of the potential vendor's past compliance with AT requirements.

(c) A verification process is implemented, whether through contractually required background checks or other similar processes that demonstrates the trustworthiness of Defense contractor and sub-contractor employees (U.S. citizens, foreign nationals, and HN personnel).

(d) Site-specific risk mitigation measures are developed and implemented to maintain positive control of Defense contractor or sub-contractor access to and within installations, sensitive facilities, and classified areas.

(e) Contract review procedures are developed and implemented to ensure contracts comply with AT provisions of the Defense Federal Acquisition Regulation Supplement.

(f) AT Level I AT Awareness training requirements are incorporated into contracts.

s. Standard 19. AT Measures for Critical Infrastructure Security.

(1) Are AT risk mitigation measures developed and implemented for critical assets (including distributive information and computer-based systems and networks), resources, and personnel per and AR 525–26?

(2) Are risk mitigation measures developed and implemented for those assets designated as Defense Critical Infrastructure (including distributive information and computer-based systems and networks), per DODD 3020.40?

(3) Has coordination been accomplished with local, State, Federal, or HN authorities responsible for the security of non-DOD assets deemed essential to the functioning of Defense Critical Infrastructure and overall capability of the Army to execute National Military Strategy?

t. Standard 20. Terrorist Incident Response Measures.

(1) Are response plans developed that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents?

(2) Do response plans, at a minimum, address management of the FPCON system, implementation of all FPCON measures, and requirements for terrorist related reports?

(3) Are plans affordable, effective, and attainable; tie security measures together; and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other?

(4) OCONUS: In SIGNIFICANT or HIGH terrorist threat level areas, do response plans contain current residential location information for all DA personnel and their dependents?

(5) Do such plans provide for enhanced security measures and/or possible evacuation of DA personnel and their dependents?

(6) Are procedures developed to ensure periodic review, update, and coordination of reactive plans with appropriate responders?

(7) Are CBRNE, medical, fire, and police response procedures integrated into consequence management/AT plans?

(8) Do plans include procedures for an attack warning system and using a set of recognizable alarms and reactions for potential emergencies, as determined by the terrorist threat, criticality and vulnerability assessments?

(9) Is the attack warning system exercised and are personnel trained and proficient in recognition?

(10) In conjunction with the alarm warning system, are drills on emergency evacuations/ movements to safe havens/shelters-in-place conducted?

(11) For garrison commanders—

(a) Are HRT and MEVAs identified and does planning provide focus on these areas?

(b) Are facilities managers informed their facility is identified as a HRT, and are procedures in effect that ensure these facility security plans are formulated on this basis?

(12) For CONUS commanders—

(a) Do AT Plans specify that the local FBI office be notified concerning terrorist incidents occurring at Army installations, facilities, activities, and civil work projects or like activities; that appropriate action be taken to prevent loss of life and/or mitigate property damage before the FBI response force arrives; that on-site elements or USACIDC elements will be utilized to safeguard evidence, witness testimony, and related aspects of the criminal investigation process pending arrival of the FBI response force; and that command of U.S. Army elements will remain within military channels?

(b) Do AT Plans address procedures that are implemented if the FBI declines jurisdiction of a threat incident that occurs in an area of exclusive or concurrent Federal jurisdiction or an area of concurrent or proprietary Federal jurisdiction?

(13) OCONUS commanders—

(a) Are HN security and law enforcement agencies involved in AT response planning, and is the employment of HN police forces requested in response to terrorist attacks?

(b) Are reactions to incidents of a political nature coordinated with the U.S. Embassy and the HN, subject to instructions issued by the combatant commander with geographical responsibility?

(c) In SIGNIFICANT and HIGH terrorist threat level areas, do terrorist incident response plans contain residential location information for all DA personnel and their dependents and do such plans provide for enhanced security measures and/or possible evacuation of DA personnel and their dependents?

(14) Do AT plans, orders, SOPs, threat assessments, and coordination measures consider the potential threat use of WMD and CBRNE weapons to include TIH?

(15) Is the vulnerability of installations, facilities, and personnel assessed to terrorist use of WMD and CBRNE weapons to include TIH?

(16) Are clear command, control, and communication lines established between local, State, Federal, and HN emergency assistance agencies to detail support relationships and responsibilities?

(17) Is the response to WMD use by terrorists synchronized with other crisis management plans that deal with large-scale incident response and consequence management?

u. Standard 21. Terrorism Consequence Management Measures.

(1) Are terrorism consequence management, CBRNE and public health emergency preparedness, and emergency response measures included as an adjunct to the overall disaster planning and preparedness to respond to a terrorist attack?

(2) Do these measures focus on mitigating vulnerabilities of Army personnel, Families, facilities, and material to terrorist use of WMD and CBRNE weapons to include TIH, as well as overall disaster planning and preparedness to respond to a terrorist attack?

(3) Do these measures include integration and full compliance with DOD emergency responder guidelines (DODD 3020.52); mass notification system standards (UFC 4–021–01); establishment of medical surveillance systems (DODD 6490.02E); deployment of CBRNE sensors and detectors; providing collective protection; and providing individual protective equipment in the following priority: (1) emergency responders and first responders, (2) critical personnel, (3) essential personnel, and (4) all other personnel?

(4) Are site-specific CBRNE preparedness and emergency response measures developed and implemented that are synchronized with a corresponding FPCON level?

(5) Are Mutual Aid Agreements or similarly structured protocols established with the appropriate local, State, Federal, or HN authorities to support AT plan execution and augment incident response and post-incident consequence management activities?

(6) Does a garrison warn populations in affected areas of CBRNE hazard identification immediately, but no longer than 10 minutes after detection? Does the warning include instructions to remain in place or evacuate?

(7) Are site-specific public health emergency response measures developed and implemented that are synchronized with FPCON levels in accordance with DODI 6200.03 and DODD 3020.40?

v. Standard 22. FPCON Measures.

(1) Is a process based on threat information and/or guidance from higher headquarters developed to raise or lower FPCON measures?

(2) Are FPCON transition procedures and measures disseminated to and implemented by all subordinate and tenant commanders?

(3) For any FPCON measures that have been determined to be inappropriate, or for proper threat mitigation, has a waiver been requested?

(4) Are waiver requests submitted in writing to the first general officer or civilian equivalent in requesting commander's chain of command for final approval?

(5) Are information copies of the waiver requests sent to the ASCC operations center, GCC's joint operations center, and the AOC?

(6) Are approved waivers, to include mitigating measures or actions, forwarded to the ASCC operations center, GCC joint operations center, and the AOC within 24 hours?

(7) Is the determination of FPCON levels accomplished in accordance with appendix B and documented in the AT plan?

(8) Do subordinate commanders obtain their higher commander's written concurrence prior to lowering the higher-level commander's FPCON level?

(9) Is a review mechanism established to lower the FPCON level as soon as the threat environment permits?

(10) Are site-specific FPCON measures for stationary and in-transit units developed and implemented to supplement the FPCON measures and actions enumerated for each FPCON level in appendix B?

(11) Does the development of site-specific FPCON measures permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement and the Standing Rules of Force?

(12) Are organic intelligence, CI, and law enforcement resources, institutional knowledge of the area of AT responsibility, and comprehensive understanding of organic capabilities utilized in developing and implementing site-specific FPCON measures for stationary and in-transit units?

(13) Are procedures in place to notify all organic, tenant, and supported units, to include RC units of FPCON transition procedures and measures?

(14) Does the capability exist to implement all FPCON measures, either through on-hand assets or availability of local assets?

(15) Are AT plans and orders with complete lists of site-specific AT measures, linked to a FPCON, classified "CONFIDENTIAL?"

(16) When separated from the AT plan, are specific AT measures linked to FPCON and site-specific FPCON levels downgraded to "FOR OFFICIAL USE ONLY" if appropriate?

(17) Are FPCON reporting requirements accomplished in accordance with appendix C?

w. Standard 23. AT Training and Exercises.

(1) Is AT training 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?

(2) Is AT training included in mission rehearsals and pre-deployment training for all units (platoon level or above) prior to deployment?

(3) Are multi-echelon individual training using vignettes and AT scenarios incorporated as required?

(4) Do units, which are deploying to or moving through HIGH threat areas, conduct pre-deployment training that includes SROE/SRUF, AOR-specific threat orientation, defensive TTPs/exercises, and the operation and use of security equipment?

(5) Is a comprehensive AT plan exercise conducted annually?

(6) Does it encompass all aspects of the AT plan including the following areas: implementation of AT measures through FPCON DELTA at parts of the command, installation, unit, or SAF; terrorist use of WMD; initial response and consequence management capabilities; terrorist attacks on Army information systems; use and evaluation of attack warning systems; medical mass casualty scenarios; and MOA, MOU, MAA or similarly structured protocols with local and HN response agencies.

(7) Is AT exercise documentation maintained for no less than 2 years to ensure incorporation of lessons learned in the AT plan?

(8) Is AT individual and collective training incorporated into annual training and exercise plans to prepare for the annual exercise?

x. Standard 24. Formal AT Training.

(1) Does the AT Training Program incorporate the training elements specified in AR 525–13? Do these elements include Level I through Level IV training (see Standards 25, 26, 27 and 28), AOR-specific training, and HRP AT training (see Standard 16 for HRP training requirements)?

(2) Do all assigned personnel complete appropriate formal training and education?

(3) Are individual records updated to reflect completion of the AT training prescribed by this regulation?

(4) Are newly assigned individuals, who are not properly trained, provided the required AT training as soon as practicable following the arrival of such individuals? Concurrently, is this deficiency reported through the chain of command to the losing unit's chain of command?

y. Standard 25. Level I AT Awareness training.

(1) Is post-accession Level I AT Awareness training provided annually to all personnel (every Soldier, DA employee, and local national or third country citizen in a direct-hire status by the DA, regardless of grade or position)?

(2) Does all face-to-face Level l AT Awareness training include training on active shooter response and detection, social media, and insider threat?

(3) Is AT information provided to Defense contractors as required in the DFARS, Section 252.225–7043?

(4) Do dependent family members ages 14 and older (or younger at the discretion of the sponsor) traveling outside CONUS on official business (that is, on an accompanied permanent change of station move) complete Level I AT Awareness training as a part of their pre-departure requirements?

(5) Are dependent family members encouraged to complete Level I AT Awareness training before any travel OCONUS (for example, leave) or to any locale where the Terrorism Threat Level is MODERATE or higher?

(6) Is Level I AT Awareness training documented for assigned personnel in the unit's individual training records in accordance with AR 350–1, paragraph 4–4?

(7) Is AT Awareness training incorporated in the Command Information Program?

z. Standard 26. Level II ATO Training.

(1) Has the ATO received formal certifying training at the TRADOC-designated (USAMPS) course within 180 days of assumption of these duties?

(2) Are ATO positions identified that require formal or refresher AT training prior to assumption of duties?

(3) Are requirements forwarded through the chain of command to HQDA DCS, G–1 to ensure assignment orders for such incoming personnel clearly delineate special instructions for Level II ATO training prior to assignment to the gaining theater/command?

(4) Is the ATO certified and has the ATO completed the USAMPS Level II AT officer refresher training course every 3 years?

(5) If the ATO has not attended formal training at the USAMPS, has the first O–6, or equivalent, in the chain of command certified the ATO based upon the individual having received formal training in AT (for example, other DOD Level II ATO courses) or by virtue of previous assignments and experience and having extensive knowledge in AT?

aa. Standard 27 Level III Pre-Command AT Training.

(1) Have all O–5 and O–6 commanders or civilian equivalent director position received Level III Pre-Command AT Training?

(2) Did all O–5 and O–6 commanders or civilian equivalent director positions receive Level III Pre-Command AT Training at the Army pre-command (PCC) training courses conducted at branch, component, and functional schools?

bb. Standard 28. Level IV Executive Seminar.

(1) Is Level IV AT Executive Training made available to all O–6 through O–8 commanders and civilian equivalent/senior executive service?

(2) Is Level IV AT training requested through the individual's higher headquarters to HQDA AT Branch?

(3) Does the commander understand the GCC/ASCC expectations for commanders in the AOR?

cc. Standard 29. AOR-Specific Training for DA Personnel and In-transit Forces.

(1) Do all DA personnel associated with their command receive an AOR update prior to traveling OCONUS or within 3 months of an OCONUS permanent change of station?

(2) Are all Defense contractors associated with their command offered an AOR update prior to traveling OCONUS?

(3) Do units maintain a memorandum for record documenting an individual's AOR-specific training?

(4) Do family members, age 14 years or older, receive similar training prior to traveling outside the 50 United States, its territories, and possessions when on official Government orders?

dd. Standard 30. AT Resource Requirements.

(1) Are prioritized AT requirements submitted through the chain of command to HQDA in accordance with DA Program Objective Memorandum Resource Formulation Guide and timelines using Schedule 75?

(2) Are funding requirements supporting the AT Program prioritized based on the threat, documented vulnerabilities, regulatory requirements, and/or command directives?

(3) Are funds supporting the AT Program tracked and accounted for in accordance with applicable regulations and directives?

(4) Are emergent or emergency AT requirements submitted through the chain of command to the Combatant commander pursuant to the requirements specified in JP 1–06, "CCIF?"

ee. Standard 31. Comprehensive Program Review.

(1) Are comprehensive AT Program reviews conducted to evaluate the effectiveness and adequacy of AT Program implementation?

(2) Does the commander conduct a self-assessment of their AT Programs within 60 days of assumption of command and annually thereafter or whenever there are significant changes in threat, vulnerabilities, or asset criticality?

(3) Is this assessment conducted using either the Internal Control Evaluation Checklist at appendix H higher headquarters approved (ACOM, ASCC, or DRU) checklist?

(4) Are assessments from a higher headquarters or DTRA JMAA used to meet the annual assessment requirement?

(5) ACOM, ASCC, and DRU commanders: Is a comprehensive AT Program review conducted a minimum of once every 3 years of subordinate commands?

(6) ACOM, ASCC, and DRU commanders: Does the program review focus on the essential AT Program elements (see Army standard 1) and as a minimum, assess the following functional areas: physical security, engineering, plans, operations, training, and exercises, resource management, MI, CI, information operations, law enforcement, threat options, OPSEC, medical, and executive protection/high risk personnel?

(7) For deploying unit commanders—

(a) Is a comprehensive AT Program review conducted in conjunction with pre-deployment vulnerability assessments (see Standard 6)?

(b) Does this self-assessment examine if deploying units have viable AT Programs and executable AT plans for transit to, from, and during operations or training exercises in the deployed AOR?

(8) ACOMs, ASCCs, DRUs, and ARNG: Is every subordinate garrison and SAF AT Program (populated daily by 300 or more personnel) assessed by a higher headquarters for compliance with this regulation at a minimum of once every 3 years?

ff. Standard 32. Program Review Teams.

(1) ACOM, ASCC, and DRU commanders: Are AT Program Review Assessment Teams established to execute the AT Program review requirements established in paragraph 5–32?

(2) ACOM, ASCC, and DRU commanders: Are AT Program Review Assessment Teams comprised of individuals with sufficient functional expertise to satisfactorily assess and evaluate the effectiveness and adequacy of AT Program implementation at the level (headquarters, unit, command, garrison, SAF, and so forth) for which the program review is being conducted?

(3) ACOM, ASCC, and DRU commanders: Are the AT Program Review Assessment Team guidelines established and do they include, at a minimum, compliance with the requirements prescribed in this regulation, accepted TTP, and best AT practices?

gg. Standard 33. Incorporation of AT into the Command Information Program.

(1) Is AT incorporated into the command information program?

(2) Does the PAO at each level of command serve as the primary spokesperson to the news media in the event of an AT incident?

(3) Is an awareness program developed to ensure the visibility of the AT Program and enhance the awareness of all personnel?

(4) Is the PAO authorized to release information to the news media about activities, programs, and operations on an installation or within a command, provided such releases are prepared in accordance with guidance in appendix D of this regulation?

(5) Does the PAO remain the primary spokesperson for the command until responsibility is transferred to another Federal agency (for example, the FBI or DHS)?

hh. Standard 34. Terrorist Threat/Incident Reporting.

(1) Is a TTWR transmitted when a command receives credible information concerning an imminent, planned terrorist attack against Army personnel (Soldiers, Civilian employees, or their Family members), facilities, or other assets?

(2) Is a TIR submitted when a terrorist incident or suspected terrorist incident occurs, involving Army personnel (Soldiers, Civilian employees, or their Family members), facilities, or other assets?

(3) Are after action reports, containing comprehensive discussion of lessons learned, forwarded by ASCCs to HQDA (DAMO–ODF) and CALL?

(4) Are TTWRs, TIRs, and after action reports prepared and submitted in accordance with appendix C?

H–5. Supersession
This evaluation supersedes the evaluation previously published in AR 525–13.

H–6. Comments
Submit comments for improvement of this management controls tool to the Provost Marshal General (DAPM–MPO–AT), 2800 Army Pentagon, Washington, DC 20310–2800.

Glossary

Section I

Abbreviations

AAR
after action report

ACIC
Army Counterintelligence Center

ACOM
Army command

AMC
Army Materiel Command

AOC
Army operations center

AOR
area of responsibility

APP
Army Protection Program

AR
Army regulation

ARCYBER
U.S. Army Cyber Command

ARIMS
Army Records Information Management System

ARNG
Army National Guard

ARTIC
Army Threat Integration Center

ASA (ALT)
Assistant Secretary of the Army (Acquisition, Logistics, and Technology)

ASA (IE&E)
Assistant Secretary of the Army (Installation, Energy and Environment)

ASA (M&RA)
Assistant Secretary of the Army (Manpower and Reserve Affairs)

ASCC
Army service component command

AT
antiterrorism

ATC
antiterrorism coordinator

ATEC
antiterrorism executive committee

ATEP
Antiterrorism Enterprise Portal

ATO
antiterrorism officer

ATWG
Army Threat Working Group

BASOPS
base operations

C4
command, control, communications, and computers

CALL
Center for Army Lessons Learned

CAR
Chief, Army Reserve

CBRNE
chemical, biological, radiological, nuclear and high yield explosive materials

CCIF
Combatant Commander Initiative Fund

CCIR
commander's critical information requirements

CG
commanding general

CI
counterintelligence

CIO/G–6
Chief Information Officer/G–6

CJCS
Chairman of the Joint Chiefs of Staff

CJCSI
Chairman of the Joint Chiefs of Staff instruction

CJCSM
Chairman of the Joint Chiefs of Staff manual

CNGB
Chief, National Guard Bureau

COM
chief of mission

CONUS
continental United States

CoS
chief of staff

CPA
Chief of Public Affairs

CT
counterterrorism

CTL
composite threat list

DA
Department of the Army

DA Pam
Department of the Army pamphlet

DCS
Deputy Chief of Staff

DCSOPS
Deputy Chief of Staff for Operations and Plans

DFARS
Defense Federal Acquisition Regulation Supplement

DHS
Department of Homeland Security

DIA
Defense Intelligence Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DOS
Department of State

DPTMS
Directorate of Plans, Training, Mobilization and Security

DRU
direct reporting unit

DTM
Directive-Type Memorandum

DTRA
Defense Threat Reduction Agency

FBI
Federal Bureau of Investigation

FP
force protection

FPCON
force protection condition

GCC
geographical combatant commander

GOMO
General Officer Management Office

HN
host nation

HQ
headquarters

HQDA
Headquarters, Department of the Army

HRB
high-risk billet

HRP
high-risk personnel

HRT
high-risk target

IC
intelligence community

IFVA
installation food vulnerability assessment

INSCOM
U.S. Army Intelligence and Security Command

JMAA
joint mission assurance assessment

MA
mission assurance

MAA
mutual assistance agreement

MARMS
Mission Assurance Risk Management System

MDEP
Management Decision Execution Program

MEVA
mission essential vulnerable area

MI
military intelligence

MILCON
military construction

MOA
memorandum of agreement

MOU
memorandum of understanding

OCONUS
outside continental United States

OPMG
Office of the Provost Marshal General

OPORD
operations order

OPREP
operational reporting

OPSEC
operations security

PAO
public affairs officer

PCC
pre-command course

PCS
permanent change of station

PIR
priority intelligence requirements

PM
provost marshal

PM/SO
provost marshal/security officer

PMG
Provost Marshal General

RAM
random antiterrorism measures

RC
Reserve Component

SAF
stand-alone facility

SOP
standing operating procedures

SROE
standing rules of engagement

SRUF
standing rules for the use of force

TAA

TACON
tactical control

TARP
Threat Awareness and Reporting Program

TDY
temporary duty

TIC
toxic industrial chemical

TIG
The Inspector General

TIH
toxic industrial hazard

TIM
Toxic industrial material

TIR
terrorist incident report

TRADOC
Training and Doctrine Command

TSA
Transportation Security Administration

TSG
The Surgeon General

TTP
tactics, techniques, and procedures

TTWR
terrorist threat warning report

TWG
threat working group

UFC
unified facilities code

USACE
U.S. Army Corps of Engineers

USACIDC
U.S. Army Criminal Investigation Command

USAMPS
U.S. Army Military Police School

USAR
U.S. Army Reserve

USARNORTH
U.S. Army North

USASOC
U.S. Army Special Operations Command

USC
United States Code

USCG
U.S. Coast Guard

USDR
U.S. Defense representative

USNORTHCOM
U.S. Northern Command

WMD
weapons of mass destruction

Section II

Terms

Agreements
Agreements are other non-procurement instruments, used as needed, to implement statutes, executive orders, or other Federal Government-wide rules that apply to non-procurement instruments, as well as to grants and cooperative agreements. Cooperative agreements, technology investment agreements, and other assistance agreements, are legal instruments used to reflect assistance relationships between the United States Government and recipients.

Antiterrorism
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Antiterrorism awareness
Fundamental knowledge of the terrorist threat and measures to reduce vulnerability to terrorism.

Antiterrorism 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 for continuing essential military operations are important adjuncts to an effective AT Program.

Assistance agreement
An assistance agreement is the transfer of a thing of value to a recipient to carry out a public purpose of support or stimulation authorized by a law of the United States (see 31 USC 6101(3)). Grants, cooperative agreements, and technology investment agreements are examples of legal instruments used to provide assistance.

Combating terrorism
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Cooperative agreement
A cooperative agreement is a legal instrument which, (see 31 USC 6305), used to enter into the same kind of relationship as a grant (see definition "grant"), except that substantial involvement is expected between the DOD and the recipient when carrying out the activity contemplated by the cooperative agreement. The term does not include "cooperative research and development agreements" (see 15 USC 3710a).

Counterterrorism
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Credible threat
A threat that is evaluated as serious enough to warrant a FPCON change or implementation of additional security measures.

Criminal intelligence
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.

Criticality assessment
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

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 DOD to fulfill its mission.

Department of Defense Components
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Department of Defense Contractor
Any individual, firm, corporation, partnership, association or other legal non-Federal entity that enters into a contract directly with DOD 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 that are engaged in selling to the DOD or a DOD component, or foreign corporations wholly owned by foreign governments.

Department of Defense System of Record
A system of record is a data management term for an information storage system (commonly implemented on a computer system running a database management system) that is the authoritative data source for a given data element or piece of information. The need to identify systems of record can become acute in organizations where management information systems have been built by taking output data from multiple source systems, re-processing this data, and then re-presenting the result for analysis.

Deterrence
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

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

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.

Family member
"Dependent "as defined by 10 USC 1072(2): spouse; unmarried widow; unmarried widower; unmarried legitimate child, including adopted child or stepchild (under 21, incapable of self-support or under 23 and enrolled in a full-time institution). Also, the Family members of DOD Civilian employees, particularly as it pertains to those assigned overseas.

Force protection
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Force protection condition
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Grant
A legal instrument which, (see 31 USC 6304), used to enter into a relationship—
a. Of which the principal purpose is to transfer a thing of value to the recipient to carry out a public purpose of support or stimulation authorized by a law of the United States, rather than to acquire property or services for the DOD's direct benefit or use; and
b. In which substantial involvement is not expected between the DOD and the recipient when carrying out the activity contemplated by the grant.

Higher Headquarters Assessment
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.

High–risk billet
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 targets.

High–risk personnel
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

High–risk target
Resources/facilities/events considered being at risk as potential terrorist targets because of mission sensitivity, ease of access, isolation, symbolic value, and/or potential for mass casualty.

Hostage
Any person held against their will as security for the performance or nonperformance of specific acts.

Improvised explosive device
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Intelink
An intelligence community network, operating in the high security mode. It facilitates collaboration among intelligence community agencies and provides users with tailored intelligence support.

Intelink–S
A secret level network that supports intelligence, policy decisions, foreign affairs, and military operations at all echelons.

Intelligence
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

International (or transnational) terrorism
Terrorism in which planning and execution of the terrorist act transcends national boundaries.

Military Service
A branch of the Armed Forces of the United States, established by an act of Congress, in which persons are appointed, enlisted, or inducted for military service, and which operates and is administered within a military or executive department. The military Services are the United States Army, United States Navy, United States Air Force, United States Marine Corps, and the United States Coast Guard.

Mission essential vulnerable areas
MEVAs are facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful accomplishment of the installation's, State National Guard, or major U.S. Army Reserve command mission. This includes areas nonessential to the installation's/facility's operational mission but which, by the nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

Non–State supported terrorism
Terrorist groups that operate autonomously, receiving no significant support from any government.

Operations security
Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: identify those actions that can be observed by adversary intelligence systems; determine indicators foreign intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Physical security
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Sabotage
An act or acts with intent to injure, interfere with, or obstruct the national defense of a country by willfully injuring or destroying, or attempting to injure or destroy, any national defense or war material, premises or utilities, to include human and natural resources.

Security
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Security procedural measures
Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Special Event
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Stand–alone facilities
Army units or organizations not located on an Army installation, DOD installation, DOD owned/leased facilities, or other Government installations.

State–directed terrorism
Terrorist groups that operate as agents of a government, receiving substantial intelligence, logistical, and operational support from the sponsoring government.

State–supported terrorism
Terrorist groups that generally operate independently, but receive support from one or more governments.

Status of forces agreement
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

System of Record
A system of record is a data management term for an information storage system (commonly implemented on a computer system running a database management system) that is the authoritative data source for a given data element or piece of information. The need to identify systems of record can become acute in organizations where management information systems have been built by taking output data from multiple source systems, re-processing this data, and then re-presenting the result for analysis.

Tactical control (for force protection)
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Technology investment agreements
A special class of assistance instruments used to increase involvement of commercial firms in defense research programs and for other purposes related to integrating the commercial and defense sectors of the nation's technology and industrial base. Technology investment agreements include one kind of cooperative agreement with provisions tailored for involving commercial firms, as well as one kind of other assistance transaction (see Part 37, Title 32, Code of Federal Regulations (32 CFR Part 37)).

Terrorism
The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

Terrorism consequence management
DOD preparedness and response for mitigating the consequences of a terrorist incident including the terrorist use of WMD. DOD consequence management activities are designed to support the lead Federal agency (domestically, DHS; overseas, DOS) 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.

Terrorism threat assessment
a. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat.
b. The product of a threat analysis for a particular unit, installation, or activity.

Terrorism vulnerability assessment
a. 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.
b. 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.
c. A systematic examination of the characteristics of an installation, system, asset, application, or its dependencies to identify vulnerabilities.

Terrorist
An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Terrorist groups
Any number of terrorist who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives.

Threat analysis
In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment.

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

Vulnerability
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).

Weapons of mass destruction
Defined in The DOD Dictionary of Military and Associated Terms (DOD Dictionary).