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
11 September 2008

SUMMARY of CHANGE

AR 525–13
Antiterrorism

This major revision, dated 11 September 2008--

- Clarifies the responsibilities for the management, execution, and oversight of Army installation antiterrorism programs, to include revising responsibilities to reflect Army realignment and the unique responsibilities of U.S. Army North (paras 2-17, 2-26, 2-27, and 2-28).

- Requires Army Command, Army Service Component Command, and Direct Reporting Unit antiterrorism strategic plans (para 2-25).

- Converts antiterrorism critical tasks into a framework of eight antiterrorism tasks (chap 4).

- Establishes Army antiterrorism standards in alignment with DOD antiterrorism standards (chap 5).

- Mandates the establishment of a Threat Working Group and an Antiterrorism Executive Committee at Army Commands, Army Service Component Commands, Direct Reporting Units, installations, and stand-alone facilities (paras 5-12 and 5-13).

- Requires commanders to use the Core Vulnerability Assessment Management Program to track all reported vulnerabilities of their subordinate organizations and/or installations to resolution/closure (para 5-36).

- Revises Army force protection condition measures to reflect current Army installation access control procedures (for vehicles and personnel) and recent DOD force protection condition measure changes (app B).

- Modifies terrorist threat/incident and force protection condition reporting requirements (app C).

Headquarters
Department of the Army
Washington, DC
11 September 2008

*Army Regulation 525–13

Effective 11 October 2008

Military Operations

Antiterrorism

By Order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the Secretary of the Army

History. This publication is a major revision.

Summary. This regulation prescribes policy and procedures and assigns responsibilities for the Army Antiterrorism Program. This program implements DODD 2000.12 and DODI 2000.16 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 Active 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 and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Army management control process. This regulation contains management control provisions in accordance with AR 11–2, but it does not identify key management controls that must be evaluated (see appendix B).

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–OPS–AT), 2800 Army Pentagon, Washington, DC 20310–2800 or e-mail AOCATBranch@conus.army.mil.

Committee Continuance Approval. The Department of the Army committee management official concurs in the establishment and/or continuance of the committee(s) outlined herein, in accordance with AR 15–1. Army Regulation 15–1 requires the proponent to justify establishing/continuing committee(s), coordinate draft publications, and coordinate changes in committee status with the Department of the Army Committee Management Office (AARP-ZA), 2511 Jefferson Davis Highway, Taylor Building, 13th Floor, Arlington, VA 22202–3926. Further, if it is determined that an established "group" identified within this regulation, later takes on the characteristics of a committee, 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 command levels B, C, D, and E for the Active 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 Office of the Provost Marshal General (DAPM–MPO–AT), 2800 Army Pentagon, Washington, DC 20310–2800 or e-mail to AOCATBranch@conus.army.mil.

*This regulation supersedes AR 525–13, dated 4 January 2002.

Contents (Listed by paragraph and page number)

Contents—Continued

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
Required and related publications and prescribed and referenced forms are listed in appendix A.

1–3. Explanation of abbreviations and terms
Abbreviations and special terms used in this regulation are explained in the glossary.

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

1–5. 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 (Financial Management and Comptroller)
The Deputy Assistant Secretary of the Army for Budget will maintain a uniform tracking system to display the expenditure and programming of funds to satisfy AT requirements in accordance with annual guidance from the Undersecretary of Defense (Comptroller).

2–2. Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
The Office of the Assistant Secretary of the Army (Acquisition, Logistics, and Technology) will 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. The AT measures to be incorporated into the contracting process are specified in paragraph 5–19 (Standard 18).

2–3. Office of the Chief of Staff, Army, General Officer Management Office
The Office of the Chief of Staff, Army, 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.

2–4. The Inspector General
The Inspector General (IG) will—

a. Integrate AT as an area of special interest for DA, Army Commands (ACOMs), Army Service Component Commands (ASCCs), and Direct Reporting Units (DRUs) and installation level IG inspections.

b. Assess whether AT policies and programs are present and current, receive command emphasis, and are integrated into all operational planning and execution.

c. Report AT-related results revealed during special inspections.

2–5. Chief, Public Affairs
The Chief, Public Affairs (CPA) will provide guidance to ACOMs, ASCCs, and DRUs for the development and execution of command information and public information programs in support of AT efforts.

2–6. Assistant Chief of Staff for Installation Management

a. The Assistant Chief of Staff for Installation Management (ACSIM) will—

b. Mandate compliance with the Unified Facilities Criteria (UFC) 4–010–01, DOD Minimum AT Standards for Buildings and UFC 4–010–02, DOD Minimum AT Standoff Distances for Buildings 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.

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.

2–7. Deputy Chief of Staff, G–1

The Deputy Chief of Staff (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) 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 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.

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

2–8. Deputy Chief of Staff, G–3/5/7

The Deputy Chief of Staff, G–3/5/7 (DCS, G–3/5/7) is responsible for the security of the Army and provides overall policy guidance and staff supervision and coordination for the Army Force Protection (FP) and AT programs. In discharging overall general staff responsibility for the Army FP and AT programs, the DCS, G–3/5/7, through the Director, Readiness and Mobilization Directorate (DAMO–OD), will—

a. Serve as the proponent for all FP related programs and policies to include AT and remain in close coordination with the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS), the other Services, combatant commanders, Defense agencies and field activities, ACOMs, ASCCs, and DRUs.

b. Establish a FP Executive Committee in accordance with paragraph 5–13. The FP Executive Committee will be chaired by the Deputy Director, DAMO–OD and will serve as the horizontal integrator for Army AT and other FP initiatives. This board will be composed of key functional staff elements and commands responsible for oversight of the Army AT program and other FP efforts. Additionally, the FP Executive Committee will develop and allocate tasks based on threat assessments, intelligence, and JCS guidance.

c. Assess the posture of the Army AT program at ACOM, ASCC, and DRU level.

d. Conduct FP Assessment Team (FPAT)/higher headquarters AT program reviews of organizations and operational forces related to Title 10 requirements.

2–9. Deputy Chief of Staff, G–2

The Deputy Chief of Staff, G–2 (DCS, G–2) will—

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

b. In coordination with the U.S. Army Intelligence and Security Command (INSCOM) and DCS, G–3/5/7 provides intelligence personnel to support operation of the Antiterrorism Operations Intelligence Center (ATOIC).

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

d. Provide policy, programming, and resources for the detailing of Army CI personnel to FBI Joint Terrorism Task Forces (JTTF) in CONUS to leverage opportunities to identify international terrorist information which may pose a threat to Army.

e. Provide policy, programming, and resources for Army CI assignment to DOD Force Protection Detachments (FPD) OCONUS for the purpose of detecting and warning of threats to DOD personnel in transit at overseas locations.

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

g. Implement policy for Subversion and Espionage Directed Against the Army (SAEDA) reporting under the provisions of AR 381–12 and local threat reporting by CI personnel to the Army Counterintelligence Center (ACIC) and the FBI GUARDIAN System.

h. Provide personnel to the DCS, G–3/5/7, as appropriate to support FPATs.

2–10. Deputy Chief of Staff, G–4

The Deputy Chief of Staff, G–4 (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.

2–11. The Surgeon General

The Surgeon General (TSG) will—

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

b. Provide technical support and guidance for food and water vulnerability assessments and food defense at the Installation level as well as in geographical areas of responsibility for subsistence.

c. Support installation AT working groups with support and technical assistance on animal medicine issues.

2–12. The Provost Marshal General

The Provost Marshal General (PMG) in direct support to the HQDA, DCS, G–3/5/7 in the management and execution of the Army AT mission will provide—

a. An AT branch that will—

(1) Serve as the functional proponent for AT and establish Army AT policy and objectives; coordinate and evaluate policies and procedures consistent with DOD Directives; and provide resources.

(2) Establish 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.

(3) Integrate and synchronize 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.

(4) Evaluate the Army posture and the effectiveness of Army AT programs annually, and provide guidance and assistance, as required.

(5) Validate and prioritize all requirements for staffing and administering Army AT program functions. Track resource execution.

(6) Establish policy that governs the development of AT doctrine and training.

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

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

(9) Monitor and report worldwide force protection conditions (FPCON).

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

2–13. Director, Army National Guard

The Director, Army National Guard (ARNG) 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 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 all ARNG Soldiers receive required AT awareness training prior to deployment outside continental United States (OCONUS).

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

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

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

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. Ensure State Adjutants General publish 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 threat working groups 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 ATO.

m. Additionally, the responsibilities listed in paragraph 2–25 will apply to Director, ARNG.

2–14. Chief, Army Reserve

The Chief, Army Reserve (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. Publish guidance concerning USAR implementation of the AT program, including all mandated Army AT standards.

h. Ensure all Army Reserve Soldiers receive required AT awareness training prior to deployment OCONUS.

i. Provide review and construction oversight of all AT design measures related to Military Construction, Army Reserve (MCAR) projects and ensure compliance with the Unified Facilities Criteria (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.

2–15. Commander, U.S. Army Training and Doctrine Command

The Commander, U.S. Army Training and Doctrine Command 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 non-commissioned officer (NCO) professional military education and appropriate civilian management professional development courses to ensure the long-term development of knowledge and skills.

(2) Providing Level I 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 E.

(3) Specialized training for personnel assigned to operations, military intelligence (MI), criminal investigation, and provost marshal (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 weapons of mass destruction (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 E.

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 Training and Doctrine Command (TRADOC) and HQDA.

e. Assist 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.

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 Center for Army Lessons Learned (CALL).

h. Ensure all personnel attending resident schooling receive required antiterrorism awareness training in accordance with paragraph 5–26 (AT Standard 25) and appendix E 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 (PCC) training courses conducted at branch, component, and functional schools.

2–16. Commander, U.S. Army Materiel Command

The Commander, U.S. Army Materiel Command (USAMC) 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.

2–17. Commander, U.S. Army North

The Commander, U.S. Army North (USARNORTH) will—

a. Serve as the Army point of contact (POC) to USNORTHCOM in the USNORTHCOM area of responsibility (AOR) for AT.

b. Execute TACON (for FP) authority over all Army components executing responsibilities for installations and facilities in the AOR, also referred to as FP Reporting Commands. This includes tactical control (TACON) (for FP) authority over Senior Mission Commanders and Installation Commanders when executing FP responsibilities for installations and facilities in the AOR.

c. Coordinate support with ACOM, ASCC, and DRU executing their responsibility for operational forces not assigned to USARNORTH, also referred to as FP Supporting Commands.

d. Share responsibility with HQDA for immediately identifying and clarifying and or addressing issues with USNORTHCOM AT standards/directives that impact mission execution for operational Army forces or execution of Army Title 10 responsibilities.

e. Coordinate and disseminate the flow of AT-related information to Army organizations/commands located in the USNORTHCOM AOR, except in Alaska and those Army elements under a Chief of Mission.

f. Conduct higher headquarters AT program reviews of ACOM, ASCC and DRU in the USNORTHCOM AOR. Implementation of DOD, USNORTHCOM, and Army policy for AT and FP is a requirement for all Army ACOM, ASCC, and DRU in the USNORTHCOM AOR. As the single Army POC to USNORTHCOM for FP, USARNORTH is responsible to USNORTHCOM for ensuring Army FP programs in the AOR meet DOD, USNORTHCOM, and Army standards.

(1) Coordinate ACOM, ASCC, and DRU AT program reviews with HQDA, G–3/5/7 to ensure minimum disruption of operations.

(2) Assess AT programs for FP Reporting Commands. USARNORTH will coordinate with HQDA to augment the USARNORTH assessment teams with HQDA subject matter experts to ensure all functional areas assessed under the HQDA Force Protection Assessment Team concept are also part of the FP Reporting Command assessments (for example, Information Assurance, Physical Security, Military working Dogs, and so forth). USARNORTH and HQDA will share all final assessment reports.

(3) Coordinate with HQDA to augment HQDA teams assessing AT programs for FP Supporting Commands FP Supporting Commands with USARNORTH SME(s) to ensure consistency in standards between FP Supporting and FP Reporting Commands. HQDA and USARNORTH will share all final assessment reports.

2–18. Commander, U.S. Army Corps of Engineers

The Commander, U.S. Army Corps of Engineers (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 CG, INSCOM and the U.S. Army Criminal Investigations Command and support ACOMs, ACSSs, 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, ACSSs, 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 (MCA) projects in compliance with Army MILCON policy.

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

2–19. Commander, U.S. Army Special Operations Command

The Commander, U.S. Army Special Operations Command (USASOC) will—

a. Develop doctrine and training supporting execution of AT operations unique to ARSOF.

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

2–20. Commander, U.S. Army Criminal Investigation Command

The Commander, U.S. Army Criminal Investigation Command (USACIDC) will—

a. Collect, analyze, and disseminate to affected commands criminal intelligence pertaining to threat activities, within the provisions of applicable statutes and regulations.

b. Maintain a capability to analyze and disseminate collected, time-sensitive information concerning the criminal threat against Army interests.

c. Provide appropriate threat-related criminal intelligence to HQDA (ATOIC), INSCOM, and the Army Counterintelligence Center (ACIC).

d. Investigate threat incidents of Army interest. Monitor the conduct of such investigations when conducted by civilian, HN, military or other police agencies. Provide applicable results of terrorist-related investigations to HQDA (ATOIC), ACIC, and CALL.

e. Provide trained hostage negotiators to support Army AT operations worldwide.

f. Plan and coordinate the protection of high-risk personnel for DOD, DA, and foreign officials as directed by HQDA.

g. Serve as the Army's primary liaison representative to Federal, state, and local law enforcement agencies and host country agencies to exchange criminal intelligence.

h. Establish 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.

i. Immediately notify the affected installation PM/SO, the installation's higher headquarters, and HQDA (in accordance with appendix C) upon receipt of time-sensitive threat information.

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

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

l. Investigate all incidents of suspected 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.

m. Provide appropriate terrorism analysis and threat assessments to the ATOIC in support of Army requirements and the AT program.

n. Ensure 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.

2–21. Commander, INSCOM

The Commander, INSCOM will—

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

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

c. Provide supported Army commanders with information concerning the foreign threat against their personnel,

facilities, and operations consistent with the provisions and limitations of AR 381–10 and other applicable regulations and directives.

d. Coordinate with ACOMs, ASCCs, and DRUs to ensure CI support for those DA organizations without organic CI capability within the provisions of DOD Directive (DODD) 5240.10 and AR 381–20.

e. Include foreign terrorist threat information in briefings on subversion and espionage directed against the Army (SAEDA) in accordance with AR 381–12.

f. Unless provided by theater ASCC assets, 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 Army Service Component Commander and other U.S. agencies.

g. Establish procedures to ensure appropriate liaison at all levels between INSCOM, USACIDC, and PM/SO elements operating in support of the AT program.

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

2–22. Commander, 1st Information Operations Command (Land)

The Commander, 1st Information Operations Command (Land) will—

a. In coordination with USACIDC and USANETCOM, assess specific or general Army command and control vulnerabilities open to terrorist exploitation and attack.

b. Perform computer and network vulnerability assessments in coordination with USACIDC and USANETCOM based on Army commanders' operational requirements, applicable policies, and AT plan.

c. Recommend courses of action to reduce or avoid terrorist threat to Army or Army-associated computer and network information infrastructures.

d. Provide Information Operations-related mission-specific assistance in contingency operations, planning, training, test, demonstration, experimentation, and exercise support.

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

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

2–23. State Adjutants General

State Adjutants General, based upon DARNG guidance, will—

a. Publish 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.

b. Appoint a state command AT officer and establish a state AT working group, AT executive committee, and threat working group in accordance with paragraphs 5–10 (Standard 9), 5–11 (Standard 10), 5–12 (Standard 11), and 5–13 (Standard 12).

c. Comply with all FPCON reporting and implementation procedures. OCONUS Adjutants General will report changes in their FPCON to the ASCC responsible for the geographic area.

d. Resource requirements for staffing and administering the AT program.

e. Evaluate state AT posture and the effectiveness of AT programs in accordance with Army AT standards and provide guidance and assistance, as required.

f. Ensure all state ARNG Soldiers receive required AT awareness training prior to deployment OCONUS and require individual/unit records be maintained documenting training.

g. Ensure all state ARNG units (battalion level and above) called to active duty have a Level II trained/certified ATO assigned in accordance with paragraph 5–10 (Standard 9).

h. Consider and include AT design measures, as appropriate, in state ARNG construction projects.

i. Disseminate threat information to state ARNG units, facilities, and activities.

j. Submit required reports in accordance with appendix C.

2–24. Director, Army Counterintelligence Center

The Director, Army Counterintelligence Center (ACIC) will—

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

b. Conduct liaison with national level intelligence analytical organizations to exchange foreign threat information.

c. Analyze information on all aspects of international terrorism and the threat it poses to U.S. Army personnel and critical resources.

d. Provide international terrorism analysis and threat assessments to the ATOIC in support of Army requirements and the AT program.

e. Serve as the Army's analytical representative for international terrorism intelligence and analysis.

f. Coordinate with the USACE Protective Design Center to ensure that threat assessments are sufficiently detailed to serve as the basis for military construction design. These assessments should be applicable over the long-term and include terrorist capabilities (tactics, weapons, tools, and explosives).

2–25. Army Command, Army Service Component Command, and Direct Reporting Unit (includes the Director, ARNG)

ACOM, ASCC, and DRU Commanders (includes the Director, ARNG) will—

a. Incorporate AT into their plans and operations.

b. 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.

c. 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.

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

e. Ensure subordinate elements designate a focal point to coordinate requirements for, and receive and disseminate time-sensitive threat information received from Federal, state, local, host nation (HN), USACIDC, and U.S. intelligence agencies.

f. 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.

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

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

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

j. Submit AT mission requirements and distribute funding.

k. 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).

l. Additionally, ACOM and DRU Commanders that execute responsibilities for installations and facilities will—

(1) Provide operational oversight/technical guidance and assessments for their command-managed installation 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 MDEP VTER, QLPR, QPSM, and 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.

m. ASCC Commanders will receive, validate, prioritize and submit Combating Terrorism Readiness Initiatives Fund (CbT–RIF) submissions to the respective geographic Combatant Commander (GCC) for Joint Staff consideration.

2–26. Senior mission commanders

As specified in AR 600–20, SMCs of Army installations are those general officer commanders designated by senior Army leadership. Their responsibilities include the following:

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.

b. Execute both SMC responsibilities and the responsibilities of the installation commander (IC) listed below when designated as the SMC and the IC.

2–27. Installation commanders

As specified in AR 600–20, ICs are usually the senior commander residing on the installation or in the surrounding community. They are designated by senior Army leadership. They oversee the implementation of the installation AT program in support of the senior mission commander. Their oversight responsibilities include the following—

a. Validate and prioritize the installation AT requirements.

b. Recommend approval of the installation AT plan to the SMC.

c. Conduct an annual program review of the installation AT program.

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

2–28. Garrison commanders

As specified in AR 600–20, garrison commanders are military officers in the rank of lieutenant colonel or colonel and are selected by the DA. Garrison commanders will—

a. Execute the installation AT program in support of the SMC.

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 PPBE, and forward them to their respective SMCs 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.

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 F).

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

2–29. 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 F).

2–30. Commanders/directors of U.S. Army tenant units/activities on U.S. Army, DOD, 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 SMC 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 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 paragraph 2–30*d* and *e*, paragraph 2–25 (ACOM, ASCC, DRU) or paragraph 2–29 (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.

2–31. Commanders/Directors of stand-alone activities/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 installations/facilities. 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 and administrative facilities, and ARNG armories. Commanders/directors will—

a. Forward a request to the next higher headquarters or supporting garrison for support if they not able to comply with regulatory requirements.

b. Apply FPCON measures as appropriate. Site-specific deviations requests will be submitted and approved in accordance with Army AT Standard 22.

c. Implement and execute Army AT tasks and all the Army AT standards with the exception of Standards 12, 19, and 32 in accordance with implementing guidance identified in chapter 4 and 5 (see app F).

d. Army organizations specified in this standard that are populated by less than 10 DOD personnel daily are not required to develop/maintain their own AT program. Commanders/directors of such organizations 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.

Chapter 3
The Army Antiterrorism Program

3–1. Overview

a. Antiterrorism is the Army's defensive program to protect against terrorism. The combination of AT, CT, 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. CONUS 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 that 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, weapons of mass destruction (WMD), and instances of Web site tampering to further their cause. Not all of these have been attempted against the Army but the potential still 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. As terrorists cannot challenge us in conventional warfare, they have resorted to asymmetrical attacks to further their objectives. Asymmetrical 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. The Department of State (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 (DOJ) 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 Federal Bureau of Investigation (FBI) will be the primary agency for investigating and apprehending terrorists in such incidents.

c. The Department of Homeland Security (DHS) has the 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), which is charged with preventing terrorist attacks and protecting the US 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 (FEMA), which 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), which 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 50 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 50 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 Department of Defense. 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 50 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 Chief of Mission (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, DA civilians, and DA dependent Family members will comply with theater, country, and special clearance requirements (DODD 4500.54 and DOD 4500.54–G) before overseas travel.

e. Commanders do not have the same legal responsibility to provide AT training for Defense contractors as that provided for military forces or direct-hire employees. Contractors remain private U.S. citizens. The DOD will assist the DOS, where militarily feasible, in supporting efforts to protect U.S. citizens abroad. Contractors are required to contact the combatant command to obtain, and comply with, the specific AT guidance for that particular area. Commanders are required to offer AT training to contractors under the terms specified in the contract. Contractors working within a U.S. military facility or in close proximity of U.S. Forces will receive incidentally the benefits of 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 (MSC), 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. 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 AT 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. AT Task 1. Establish an AT 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. AT officer.
e. Standard 10. AT working group.
f. Standard 12. AT executive committee.
g. Standard 30. AT resource requirements.
h. Standard 34. Terrorist threat/incident reporting

4–3. AT 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. AT Task 3. Assess and reduce critical vulnerabilities (conduct AT 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. Vulnerability assessment.
d. Standard 31. Comprehensive program review.
e. Standard 32. Comprehensive program review teams.
f. Standard 35. Core Vulnerability Assessment Management Program

4–5. AT Task 4. Increase AT 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. AT Task 5. Maintain defenses in accordance with FPCON

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. AT 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. AT 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. AT Task 8. Conduct exercises and evaluate/assess AT plans

Commanders will institute an exercise program that develops, refines, and tests the command's AT response procedures to terrorist threats/incidents and ensure antiterrorism 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 AT 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 2000.16.

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. AT 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 AT 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 priority intelligence requirements (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 countersurveillance, 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 CRIMINT 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, ATOIC, FBI, ACIC, USACIDC, provost marshal, local law enforcement, Intelink-S, and Intelink).

(11) Ensure the command uses the DOD Intelligence Production Program to validate and receive intelligence community 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. AT 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 FM 3–100.12 , FM 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 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 JSIVA satisfies this requirement.

5–5. Standard 4. Terrorism 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) ACOM, ASCC, and DRU commanders and Director, ARNG will incorporate terrorist threat information into an annual terrorism threat assessment based on the annual comprehensive DA threat statement to subordinate units/organizations/installations in preparing their specific threat statements. A copy of the annual terrorism threat statement will be forwarded to their subordinate elements and HQDA (DAPM–OPS–AT and DAPM–OPS–ATOIC) within 90 days of receipt of the DA annual threat statement via the Automated Message Handling System (AMHS). The results of threat assessments will be disseminated to all affected activities (for example, organic, tenant, and supported Reserve Component (RC) units).

(2) 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 Intelligence Community (IC) activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a continuous analysis of threat information to support the Threat Warning process.

(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 (i.e., 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, DCSOPS/G–3/DPTMS/and so forth).

5–6. Standard 5. Criticality Assessment

a. Army standard 5. Commanders will conduct a criticality assessment to identify, classify, and prioritize mission-essential assets, facilities, resources, and personnel. Additionally, commanders will conduct a criticality assessment 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 to warrant protective measures to ensure continued efficient operation; protection from disruption, degradation, or destruction; and timely restoration.

b. Implementing guidance.

(1) Criticality assessments will be updated annually to produce a prioritized AT Critical Facilities List based on the following factors:

(a) Relative importance.

(b) Effect of loss.

(c) Recoverability.

(d) Mission functionality.

(e) Substitutability.

(f) Reparability.

(2) Criticality assessments will 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.

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. Terrorism vulnerability assessments will be conducted at a minimum for, but not limited to—

(a) Any Army installation, facility, or activity populated daily by 300 or more 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 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 or other activity involving a gathering of 300 or more DOD personnel (that is, battle assemblies, drill assemblies, Independence Day and Armed Forces Day Celebrations). 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) Joint Service Integrated Vulnerability Assessment (JSIVA) Security Classification Guide.

(3) Terrorism vulnerability assessments will be conducted consistent with the principles outlined in DOD O–2000.12–H, "DOD Antiterrorism Handbook," chapter 7.

(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) Results from assessments identified in paragraph 5–7*b*(1)(a)–(e) will be populated into CVAMP within 120 days from the completion of the assessment.

(7) Results from higher headquarters assessments (for example, JSIVA) will be populated into the CVAMP within 120 days from the completion of the assessment.

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

(9) 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. AT 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 Director, ARNG 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, stand-alone activity, 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). AT requirements will be included in the deployment order as an annex or as apart 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 construction and building considerations.

(f) AT measures for logistics and other contracting

(g) AT measures for Critical Asset Security.

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

(i) Terrorism incident response measures.

(j) 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).

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

5–9. Standard 8. AT 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 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 AT plans 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.

(2) Commanders OCONUS will—

(a) Comply with applicable Status-of-Forces Agreement (SOFA) 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 Antiterrorism Officer (ATO).

b. Implementing guidance.

(1) ACOM, ASCC, and DRU Commanders and Director, ARNG 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) A stand-alone activity having 300 or more individuals assigned, occupied, or under the operational control of a designated commander or director will have a Level II-certified ATO (minimum grade of E–6 or higher or equivalent civilian grade).

(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).

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; Headquarters (HQ), ARNG; Army Garrisons; and stand-alone activities (populated daily by 300 or more personnel).

(2) Formal ATWGs 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). Units will participate in the host installation/garrison ATWG.

(3) ATWG membership will include the following:

(a) Commander or designated representative (that is, Deputy Commander, 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; HQ, ARNG; Army Garrisons; and stand-alone activities (populated daily by 300 or more personnel).

(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) TWG membership will include the following:

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

(b) ATO.

(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 Intelligence Community.

5–13. Standard 12. AT Executive Committee

a. Army standard 12. Commanders will establish an AT executive-level committee or similarly structured corporate body that meets at least semi-annually to develop and refine AT program guidance, policy, and standards; to act upon the recommendations of the ATWG and TWG; and to assist in determining resource allocation priorities to mitigate or eliminate terrorism-related vulnerabilities.

b. Implementing guidance. ATECs will be established at all ACOMs; ASCCs; DRUs; HQ, ARNG; and Army Garrisons. Membership should include the commander, his staff principals, and the ATO.

5–14. Standard 13. AT 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) At a minimum, 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. AT Measures for Off-Installation Facilities, Housing, and Activities

a. Army standard 15. All AT programs will 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.

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.

5–17. Standard 16. AT 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 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 non-tactical armored vehicles in support of HRP security operations.

5–18. Standard 17. AT Construction and Building Considerations

a. Army standard 17. The construction and building standards prescribed in DOD 5200.8–R, U FC 4–010–01, DOD Minimum AT Standards for Buildings, 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 DOD O–2000.12–H.

(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.

5–19. Standard 18. AT 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 Army contracting officer, establish a mechanism to ensure the following measures are incorporated into contracting actions—

(1) 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.

(2) 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.

(3) 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.

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

(5) Ensure contracts incorporate AT Level I requirements (para 5–26*b*(2)(b) and app E).

5–20. Standard 19. AT Measures for Critical Asset Security

a. Army standard 19. Risk mitigation 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 Unified Facilities Criteria, and include distributive information and computer-based systems and networks. In addition to those items prioritized on the AT Critical Facilities List, Defense Critical Assets must identified per DODD 3020.40.

b. Implementing guidance. Commanders will—

(1) Develop and implement AT risk mitigation measures for critical assets, resources, and personnel in accordance with DOD O–2000.12–H and AR 525–26.

(2) Develop and implement risk mitigation measures for those assets designated as Defense Critical Assets per DODD 3020.40.

(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 Assets and overall capability of the Army to execute National Military Strategy.

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.

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) At garrison level, commanders will identify high risk targets (HRTs), mission essential vulnerable areas (MEVAs) and 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.

(3) Commanders will develop procedures to ensure periodic review, update, and coordination of response plans with appropriate responders.

(4) Commanders will ensure CBRNE, medical, fire, and police response procedures are integrated into consequence management/AT plans.

(5) Plans will include procedures for an attack warning system using a set of recognizable alarms and reactions for potential emergencies, as determined by the terrorist threat, criticality, and vulnerability assessments. Commanders will exercise the attack warning system and ensure personnel are trained and proficient in recognition. In conjunction with the alarm warning system, commanders will conduct drills on emergency evacuations/ movements to safe havens/ shelters-in-place.

(6) CONUS commanders 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.

(7) 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 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.

(8) USACIDC will investigate threat incidents in accordance with paragraph 2–20*d*.

(9) AT plans, orders, SOPs, 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. Clear command, control, and communication lines will be established between local, state, Federal, and HN emergency assistance agencies to detail support relationships and responsibilities. Response to WMD use by terrorists will be synchronized with other crisis management plans that deal with large-scale incident response and consequence management. Separate plans devoted only to terrorist use of WMD need not be published if existing crisis management plans covering similar events (such as accidental chemical spills) are sufficiently comprehensive.

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 2000.18); mass notification system standards (UFC 4–021–01); establishment of medical surveillance systems (DODD 6490.2); deployment of CBRNE sensors and detectors; providing collective protection; and providing individual protective equipment in the following priority:

(1) Emergency responders and first responders. Personnel who work closest to known or suspected CBRNE hazards (for example, emergency responders) should be given the best protection (for example, Responders should use maximum possible protection until determined otherwise by competent authority.

(2) 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.

(3) 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 (i.e., escape, survive, and restore essential operations).

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

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 DODD 6200.3 and DODD 3020.40.

5–23. Standard 22. FPCON Measures

a. Army standard 22. Commanders will develop a process based on threat information and or guidance from higher headquarters to raise or lower FPCON measures. FPCON transition procedures and measures will be disseminated to and implemented by all subordinate and tenant commanders.

b. Implementing guidance.

(1) The GCCs have TACON (for FP) authority and responsibility for all DOD elements and personnel within their respective AOR. The GCC is responsible for establishing the baseline FPCON for the AOR and procedures to ensure that FPCON measures are uniformly disseminated and implemented.

(2) If it is determined that certain FPCON measures or other AT procedural requirements are inappropriate for current operations, or proper threat mitigation, commanders may request a waiver. Waiver requests will be submitted in writing to the first general officer in requesting commander's chain of command for final approval. Information copies of the waiver requests will be sent to the ASCC operations center for forwarding to the GCC's joint operations center, and the AOC. Approved waivers, to include mitigating measures or actions, must be forwarded to the ASCC operations center for forwarding 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 five working days after approval.

(3) Determination of FPCON levels will be in accordance with appendix B and will be documented in the AT plan. Subordinate commanders may raise a higher-level commander's FPCON for those personnel and assets for which they have AT responsibilitiy. Subordinate commander's will not lower a higher-level commander's FPCON level without the higher-level commander's written concurrence.

(4) Additionally, commanders will—

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

(b) Develop and implement site-specific FPCON measures for stationary and in-transit units to supplement the FPCON measures and actions enumerated for each FPCON level in appendix B. The development of site-specific FPCON measures must permit sufficient time and space to determine hostile intent, while fully considering constraints imposed by the Standing Rules of Engagement (SROE) and the Standing Rules of Force (SROF) in CJCSI 3121.01B. Organic intelligence, CI, and law enforcement resources, institutional knowledge of the area of AT responsibility, and comprehensive understanding of organic capabilities will be utilized in developing and implementing site-specific FPCON measures for stationary and in-transit units.

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

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

(5) In AT plans and orders, site-specific AT measures, linked to a FPCON, will be classified "CONFIDENTIAL." When separated from the AT plan or order, specific AT measures linked to FPCON and site specific FPCON levels may be downgraded to "OFFICIAL USE ONLY," if appropriate.

(6) Ensure required FPCON reports are submitted in accordance with appendix C.

5–24. Standard 23. AT 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/SROF, AOR-specific threat orientation, deterrence-specific TTPs/exercises, lessons learned, and the operation and use of security equipment.

(3) Conduct a comprehensive AT plan exercise annually.

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

1. Implementation of AT measures through FPCON DELTA at parts of the command, installation, unit, or stand-alone activity.

2. Terrorist use of WMD and CBRNE weapons to include TIH.

3. Initial response and consequence management capabilities.

4. Threat attacks on Army information systems.

5. Use and evaluation of attack warning systems.

6. Medical mass casualty (MASCAL) scenarios.

7. Memorandums of Agreement (MOA), Memorandums of Understanding (MOU), MAA, and similarly structured protocols with local and HN response agencies.

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

(c) 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.

5–25. Standard 24. Formal AT Training

a. Army standard 24. The Army's formal AT Training Program will incorporate the training elements specified in DODI 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 E.

5–26. Standard 25. Level I AT 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 Chief of Mission requirements.

(3) Commanders will—

(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) 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.

(c) 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.

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

(e) Incorporate AT awareness training in their Command Information Program.

5–27. Standard 26. Level II ATO 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/standalone activity 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 three 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.

5–28. Standard 27. Level III Pre-Command AT 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 AT 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 JCS providing focused updates, detailed briefings, guest speakers, and panel discussions. Seminar will include a tabletop AT war-game focusing on power projection, WMD, antiterrorism, 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. AOR–Specific Training for DOD 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 three 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. AT Resource Requirements

a. Army standard 30. Commanders will identify AT resource requirements using the Planning, Programming, Budgeting, and Execution (PPBE) 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 CJCSI 5261.01E, "CbT–RIF."

5–32. Standard 31. Comprehensive AT 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 Management Control Evaluation Checklist at appendix G or a 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 stand-alone activity. 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 JSIVA 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 three 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) Operations Security (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 stand-alone activity AT Program (populated daily by 300 or more personnel) will be assessed by their higher headquarters for compliance with this regulation at a minimum of once every three 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 three years. .

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

5–33. Standard 32. AT Program Review Teams

a. Army standard 32. ACOM, ASCC, and DRU Commanders and Director, ARNG 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, stand-alone activity, 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 AT into Command Information Programs

a. Army standard 33. Commanders will incorporate AT into their command information programs. The public affairs officer (PAO) at each level of command will serve as the primary spokesperson to the news media in the event of an AT incident.

b. Implementing guidance.

(1) Commanders will develop an awareness program to ensure the visibility of the AT Program and enhance the awareness of all personnel.

(2) The PAO is 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 at appendix D in this regulation.

(3) The PAO remains the primary spokesperson for the command until responsibility is transferred to another Federal agency (for example, the FBI or DHS). When responsibility is transferred to another Federal agency, the Army PAO will assist in the transfer. The Army PAO also will continue to serve as the release authority for information concerning Army involvement in the incident.

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 (AAR). Terrorist Threat/Incident AARs, containing comprehensive discussion of lessons learned, will be forwarded to HQDA (DCS, G–3/5/7 (DAMO–ODF) and OPMG (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 (as specified in HQDA Execution Order: U.S. Army North FY 2007 FP and AT Responsibilities, 5 Dec 06) 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. CVAMP

a. Army standard 35. Commanders will use the CVAMP to track all reported vulnerabilities of their subordinate organizations and/or installations to resolution/closure.

b. Implementing guidance. Commanders will—

(1) Ensure that personnel designated to input information and data into the CVAMP complete the designated Joint Staff managed web-based training tutorial prior to operating the system.

(2) Identify and place into their CVAMP hierarchy trees all subordinate commands, installations, units, facilities, or activities for which they conduct a higher headquarters assessment or comprehensive AT program review.

(3) Populate the results from Terrorist Vulnerability Assessments identified in paragraph 5–7*b*(1)(a)-(f) and the assessments and comprehensive AT program reviews identified in paragraph 5–32*b*(1)–(6) into CVAMP in accordance with the reporting timeframes established paragraph 5–7*b*(6) and (7) and paragraph 5–32*b*(7).

Appendix A
References

Section I
Required Publications

AR 380–13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations (Cited in para 5–3*b*(2)(h).)

AR 381–10
U.S. Army Intelligence Activities (Cited in paras 2–21*c*, 2–24*a*, 5–3*b*(9), and 5–5*b*(2)(g).)

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA) (Cited in paras 2–9, 2–21*d*, and 5–3*b*(g).)

AR 381–20
The Army Counterintelligence Program (Cited in paras 2–21*d*, 2–25*h*.)

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 Proponent System

AR 25–2
Army Information Assurance

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 190–16
Physical Security

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
The Physical Security

AR 195–2
Criminal Investigation Activities

AR 350–1
Army Training and Leader Development

AR 380–5
Department of the Army Information Security Program

AR 380–53
Information Systems Security Monitoring

AR 415–15
Army Military Construction Program Development and Execution

AR 525–26
Infrastructure Risk Management

AR 530–1
Operations Security (OPSEC)

AR 600–20
Army Command Policy

DA Pam 190–51
Risk Analysis for Army Property

DODD 2000.12
DOD Antiterrorism Program

DODD 3020.3
Defense Critical Infrastructure Program (DCIP)

DODD C–4500.51
DOD Non-Tactical Armored Vehicle Policy

DODD 4500.54
Official Temporary Duty Travel Aboard

DODD 5200.27
Acquisition of Information Concerning Persons and Organizations not Affiliated with DOD

DODD 5240.10
DOD Counterintelligence

DODD 6200.03
Emergency Health Powers in Military Installations

DODD 6490.02
Mental Health Evaluations of Members of the Armed Forces

DOD 5200.08–R
Physical Security Program

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

DOD O–2000.12–H
Protection of DOD Personnel and Activities against Acts of Terrorism and Political Turbulence

DODI 2000.16
DOD Antiterrorism Standards

DODI 2000.22
Designation and Physical Protection of DOD High Risk Personnel

UFC 4–010–01
DOD Minimum AT Standards for Buildings

UFC 4–010–02
DOD Minimum AT Standoff Distances for Buildings

UFC 4–021–01
Design and O&M: Mass Notification Systems

FM 3–025
Army Special Operations Forces

FM 3–13
Information Operations

FM 3–19.1
Military Police Operations

FM 3–19.13
Law Enforcement Investigations

FM 3–19.30
Physical Security

FM 3–100.12
Risk Management

FM 5–19
Composite Risk Management

FM 19–10
Military Police Law and Order Operations

FM 34–60
Counterintelligence

CJSCM 3150.03B
Joint Reporting Structure Events and Incident Reports

JFTR, volume I
Joint Federal Travel Regulations-Uniformed Service Members, volume I (www.dtic.mil/perdiem/)

Section III
Prescribed Forms

This section contains no entries.

Section IV
Referenced Forms

DA Form 11–2–R
Management Control Evaluation Certification Statement

Appendix B
Force Protection Conditions and Threat Levels

B–1. The Force Protection Conditions System

The Force Protection Conditions (FPCON) System discussed here is mandated in DODD 2000.12 and DODI 2000.16. They describe progressive levels of security measures for implementation in response to threats to U.S. Army personnel, information, and critical resources. The FPCON system is the foundation of all AT plans and orders. AT plans and orders must be constructed to address the threat assessment and implement the measures described in this appendix. The measures listed below are based on the DOD measures located in DOD I 2000.16, with additional Army-common implementing guidance. When producing plans, local commanders must further refine this guidance into more specific instructions in order to meet the unique requirements of the specific location. 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 civilian exercising equivalent authority. Still, Army commanders of such tenant elements should execute the FPCON measures that do not involve installation-level actions, at least to limited degree.

a. There are five FPCONs:

(1) *FPCON NORMAL.* Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture. As a minimum, access control will be conducted at all DOD installations and facilities. The minimum FPCON for U.S. Army commands is NORMAL.

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

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

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

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

b. It may be necessary to implement certain measures from higher FPCONs levels resulting from intelligence received or as a deterrent. At FPCON ALPHA through CHARLIE, commanders will implement selected measures from higher FPCONs as a part of RAM. At any FPCON, commanders may implement any measures they deem appropriate from any higher FPCON.

c. An AT plan, with a complete listing of site specific AT security measures linked to a FPCON, will be classified at a minimum as CONFIDENTIAL. When separated from the AT plan, site-specific AT security measures and FPCONs should be handled as For Official Use Only (FOUO).

B–2. FPCON NORMAL

The following measures will be implemented—

a. Measure NORMAL 1. Assess all vehicles for authorized access to Army installations (for example, vehicle registered in accordance with AR 190–5 and installation policy).

b. Measure NORMAL 2. Verify the identity of all personnel entering Army installations in accordance with AR 190–16. Security personnel will inspect identification cards, security badges, or other forms of personal identification approved by the commander.

c. Measure NORMAL 3. Secure buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities and areas at installation, directorate, or activity level.

d. Measure NORMAL 4. Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

e. Measure NORMAL 5. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

f. Measure NORMAL 6. Identify defense critical assets and high-occupancy buildings

B–3. FPCON ALPHA

The following measures will be implemented—

a. Measure ALPHA 1. Continue, or introduce, all measures of the previous FPCON level.

b. Measure ALPHA 2. At regular intervals, inform all personnel, including Family members, of the general situation. Ensure personnel arriving for duty are briefed on the threat. Additionally, remind all personnel, including Family members, to report the following to appropriate law enforcement or security agencies—

(1) Suspicious personnel, particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about military operations or security measures.

(2) Unidentified vehicles parked or operated in a suspicious manner on, or in the vicinity of U.S. installations, units, or facilities.

(3) Abandoned parcels or suitcases.

(4) Any possible surveillance attempts or other activity considered suspicious.

c. Measure ALPHA 3. The duty officer or personnel with access to building plans as well as the plans for area evacuations must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on-call and readily available. Ensure that law enforcement and security agencies have immediate access to building floor plans and emergency evacuation plans for high-risk targets (HRTs).

d. Measure ALPHA 4. Increase unannounced security spot checks (inspection of the contents of vehicles, suitcases, briefcases and other containers) at access control points for U.S. installations and facilities.

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

f. Measure ALPHA 6. Test mass notification procedures.

g. Measure ALPHA 7. Review all operations plans and orders and SOPs, identify resource requirements and be prepared to implement measures of the next higher FPCON.

h. Measure ALPHA 8. Review security measures for HRP and implement additional measures warranted by the threat and existing vulnerabilities (for example, HRP should alter established patterns of behavior and wear inconspicuous body armor when traveling in public areas).

i. Measure ALPHA 9. Increase liaison with local police and intelligence and security agencies to monitor the threat to Army personnel, installations, and facilities. Notify local police agencies concerning FPCON BRAVO measures that, if implemented, could impact on their operations in the local community.

j. Measure ALPHA 10. Review intelligence, CI, and operations dissemination procedures.

k. Measure ALPHA 11. Review barrier plans.

l. Measure ALPHA 12. Review all higher FPCON measures.

B–4. FPCON BRAVO

The following measures will be implemented—

a. Measure BRAVO 1. Continue, or introduce, all measures of the lower FPCON levels.

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

c. Measure BRAVO 3. Keep cars and objects (for example, crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings. Consider applying to all inhabited structures to the greatest extent possible. Standoff distance should be determined by the following factors: asset criticality; the protection level provided by structure; IED/Vehicle Borne IED threat; and available security measures. Consider centralized parking and implementation of barrier plans. If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures in accordance with local plans (frequent inspection by explosive detector dog (EDD) teams, centralized parking, controlled access to parking areas, and so forth).

d. Measure BRAVO 4. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

e. Measure BRAVO 5. At the beginning and end of each workday and at random intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, or for signs of tampering, or indications of unauthorized entry.

f. Measure BRAVO 6. Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices, or other dangerous material. If available, use trained EDD teams for inspection of suspicious items and to conduct periodic screening of mail. Encourage Soldiers, civilian employees, and Family members to inspect their personal mail, report suspicious items to local law enforcement agencies, and refrain from handling such items until cleared by the appropriate authority.

g. Measure BRAVO 7. Randomly inspect commercial deliveries to identify explosive and incendiary devices. Use trained EDD teams for some inspections, when available. Encourage Family members to check home deliveries, report suspicious packages to local law enforcement agencies, and refrain from handling them until cleared by appropriate authority.

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

i. Measure BRAVO 9. Increase both overt and covert security force patrols and surveillance of Army housing areas,

schools, messes, commissaries, exchanges, guesthouses, clubs, libraries, chapels, and high-occupancy targets to improve deterrence and defense, and to build confidence among staff and Family members.

j. Measure BRAVO 10. Implement plans to enhance off-installation security for Army facilities in conjunction with local and state law enforcement agencies or HN law enforcement agencies. In areas with Threat Levels of MODERATE or higher, coverage includes facilities (for example, DOD schools and daycare centers) and transportation services and routes (for example, bus routes) used by DOD employees and Family members. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.

k. Measure BRAVO 11. Inform local security committees of actions being taken.

l. Measure BRAVO 12. Verify the identity of all personnel entering HRTs and other sensitive activities specified in local plans (inspect identification cards or grant access based on visual recognition). Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers entering the installation, HRTs, and other sensitive activities specified in local plans. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, and so forth) and randomly inspect suitcases, parcels, briefcases, and other containers carried by visitors.

m. Measure BRAVO 13. Increase the frequency of random building and identity checks (inspection of identification cards, security badges, and vehicle registration documents) conducted by security force patrols on the installation.

n. Measure BRAVO 14. Implement additional security measures for HRP, such as conduct of countersurveillance operations, in accordance with existing plans. Consider providing 24-hour protective services protection for Level I HRP, if not already provided.

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

p. Measure BRAVO 16. Brief all law enforcement personnel, guards, and security augmentation force personnel concerning the threat and policies governing use of force/rules of engagement. Repeat this briefing on a periodic basis.

q. Measure BRAVO 17. As deemed appropriate, verify the identity of personnel entering buildings.

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

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

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

u. Measure BRAVO 21. Review all higher FPCONs. Increase liaison with local police, intelligence and security agencies to monitor the threat to Army personnel, installations, and facilities. Notify local police agencies concerning FPCONS CHARLIE and DELTA measures that, if implemented, could impact their operations in the local community.

B–5. FPCON CHARLIE

The following measures will be implemented—

a. Measure CHARLIE 1. Fully implement all measures of lower FPCONs.

b. Measure CHARLIE 2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of the current rule for the use of force, rules of engagement and any applicable Status of Forces Agreements or HN agreements. Review types of weapons and ammunition issued to augmentation security personnel; heightened threats may require employment of different weapon capabilities.

c. Measure CHARLIE 3. Be prepared to react to requests for assistance from local authorities and other installations, facilities, or units in the area.

d. Measure CHARLIE 4. Limit installation and HRT access points to the absolute minimum necessary for continued operation. Randomly search vehicles.

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

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

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

h. Measure CHARLIE 8. Increase patrolling of the installation/facility/unit including waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions and persons outside the perimeter. For airfields, patrol or provide observation of approach and departure flight corridors as appropriate to the threat.

Coordinate with Transportation Security Administration, Marine Patrol, U.S. Coast Guard, and local law enforcement as required to cover off-facility approach and departure flight corridors.

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

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

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

l. Measure CHARLIE 12. Review personnel policy procedures to determine appropriate courses of action for dependent Family members.

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

n. Measure CHARLIE 14. Consider escorting children to and from DOD schools (among options to consider are escorting school buses, recommending parents escort children to/from school, and so forth).

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

p. Measure CHARLIE 16. Review all FPCON DELTA measures.

B–6. FPCON DELTA

The following measures will be implemented—

a. Measure DELTA 1. Fully implement all measures of lower FPCON levels.

b. Measure DELTA 2. Augment guard forces to ensure absolute control over access to the installation and HRTs.

c. Measure DELTA 3. Identify the owners of all vehicles already on the installation and, OCONUS, in the vicinity of soft targets off installations. In those cases where the presence of a vehicle can not be explained (owner is not present and has no obvious military affiliation), inspect the vehicle for explosive or incendiary devices, or other dangerous items, and remove the vehicle from the vicinity of HRTs as soon as possible. OCONUS commanders take unilateral action off-post only in circumstances where there is a reasonable basis to believe that death, grievous bodily harm, or significant property damage will otherwise occur. If unilateral action is taken, notify the HN as-soon-as-possible.

d. Measure DELTA 4. Inspect all vehicles entering the installation, facility, or activity. Inspections should include cargo storage areas, undercarriage, glove boxes, and other areas where explosive or incendiary devices or other dangerous items could be concealed. Briefcases, suit cases, boxes, and other containers in vehicles should also be inspected. Selected, pre-screened and constantly secured vehicles used to transport HRP may be exempted.

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

f. Measure DELTA 6. Search all personally carried items (that is, suitcases, briefcases, packages, backpacks) brought on the installation for presence of explosive or incendiary devices, or other dangerous items.

g. Measure DELTA 7. Close DOD schools.

h. Measure DELTA 8. Implement frequent inspections of the exterior of buildings (to include roof and subterranean areas) and parking areas. Security force personnel should conduct inspections at HRTs.

i. Measure DELTA 9. Restrict all non-essential movement.

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

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

l. Measure DELTA 12. Request that local authorities close those public roads and facilities in the vicinity of military installations, facilities, and activities that might facilitate execution of a terrorist attack.

m. Measure DELTA 13. Begin continuous monitoring for chemical, biological, and radiological contamination.

B–7. Threat levels

a. The decision to implement a particular FPCON is a command decision which should be 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 JCS.

(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. Anti-U.S. 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 Chief of Mission (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, etc. 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). 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 U.S. Defense Representative (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 commander 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 [RCS exempt: AR 335–15, para 5–2e(2)]

a. Terrorist Threat Warning Report (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, TTWR will be provided immediately by the ASCC via telephone to the AOC (phone DSN 227–0218 or commercial (703) 697–0218). 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 thereto.

c. A follow-up report will be transmitted within six hours of receiving the information by e–mail message to the

AOC at AOCARMYWATCH@conus.army.mil (unclassified) or AOCARMYWATCH@hqda.army.smil.mil (classified). Simultaneously, courtesy copies of the followup report will be provided to:

(1) ATOIC at AOCATOIC@conus.army.mil (unclassified) or AOCATOIC@hqda.army.smil.mil (classified).

(2) AT Branch, OPMG at AOCATBRANCH@conus.army.mil (unclassified) or AOCATBRANCH@hqda.army.smil.mil (classified).

(3) Headquarters, USACIDC at CIOPIN@conus.army.mil (unclassified) or CIDINTELDIV@sbelvoir.army.mil.smil (classified).

(4) U.S. Army Counterintelligence - Law Enforcement Center (USACILEC) at ARMYCILEC@mi.army.mil (unclassified) or ARMYCILEC@mail.north-inscom.army.smil.mil (classified).

(5) ACOMs and DRUs who have units/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 e–mail message directly from ASCC receiving the information to the addressees in paragraph D–1. *c* . 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 Chief, Joint Chiefs of Staff Manual (CJCSM) 3150.03B) or similar format (i.e., 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 [RCS exempt: AR 335–15, para 5–2e(2)]

a. Terrorist Incident Report (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 227–0218 or commercial (703) 697–0218). 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 six hours of an actual or suspected terrorist incident involving U.S. Army personnel or facilities, an updated TIR will be submitted by e–mail message to the AOC at AOCARMYWATCH@conus.army.mil (unclassified) or AOCARMYWATCH@hqda.army.smil.mil (classified). Simultaneously, courtesy copies of the follow-up report will be provided to:

(1) ATOIC at AOCATOIC@conus.army.mil (unclassified) or AOCATOIC@hqda.army.smil.mil (classified);

(2) AT Branch, OPMG at AOCATBRANCH@conus.army.mil (unclassified) or AOCATBRANCH@hqda.army.smil.mil (classified);

(3) Headquarters, USACIDC at CIOPIN@conus.army.mil (unclassified) or CIDINTELDIV@sbelvoir.army.mil.smil (classified); and

(4) USACILEC at ARMYCILEC@mi.army.mil (unclassified) or ARMYCILEC@mail.north-inscom.army.smil.mil (classified).

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

d. 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.

e. All TIR will use an OPREP–3 (see CJCSM 3150.03B) or similar format (i.e., the sending command's report format). The following information will be included in the report:

f. A complete description of the terrorist incident, including the following:

(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 AAR [RCS 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 OPMG (DAPM–MPO)) and the CALL within 45 days of a reported terrorist threat or terrorist incident.

C–4. FPCON Report [RCS 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. Within the USNORTHCOM AOR, Army reporting and supporting commands (as specified in HQDA Execution Order: U.S. Army North FY 2007 FP and AT Responsibilities, 5 DEC 06) will be included in the ASCC FPCON reporting system.

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, initial report will be provided telephonically to the AOC within six hours (phone DSN 227–0218 or commercial (703) 697–0218). 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 at AOCARMYWATCH @conus.army.mil (unclassified) or AOCARMYWATCH @hqda.army.smil.mil (classified).

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

(a) ATOIC at AOCATOIC @conus.army.mil (unclassified) or AOCATOIC@hqda.army.smil.mil (classified)

(b) OPMG AT Branch at AOCATBRANCH@conus.army.mil (unclassified) or AOCATBRANCH@hqda.army.smil.mil (classified).

(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 (e.g., FPCON ALPHA with B3, B5–7, and C4). 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 D–4*d* (1).

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

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

(a) Monthly reports will be provided via e–mail message to the AOC at AOCARMYWATCH @conus.army.mil (unclassified) or AOCARMYWATCH @hqda.army.smil.mil (classified) by 1200Z on the second duty day of each month, with an as of date/time of 1200Z on the first duty day of the month.

(b) Simultaneously provide courtesy copies to—

1. ATOIC at AOCATOIC@conus.army.mil (unclassified) or AOCATOIC@hqda.army.smil.mil (classified).

2. AT Branch, OPMG at AOCATBRANCH@conus.army.mil (unclassified) or AOCATBRANCH@hqda.army.smil.mil (classified).

(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
Public Affairs Officer Guidance

D–1. Public affairs planning and execution procedures in support of AT efforts

a. The media may interview Army officials, commanders, senior leaders, and knowledgeable individuals about AT matters pertaining to those areas for which they are responsible. AT measures and procedures should be discussed in a general manner without providing specific details.

b. In response to queries seeking information concerning specific defensive measures for AT Programs, the following replies are appropriate:

(1) In the United States. "Army policy prohibits discussing specific defensive measures in our AT Program. Such disclosure could adversely affect the success of the program."

(2) Outside the United States. "U.S. military authorities are working closely with HN security forces to ensure maximum coordination for appropriate protective measures." (In those rare instances where the U.S. and HN do not have close relations, use the response appropriate for use in the United States.)

c. The Office of the Assistant Secretary of Defense for Public Affairs (OASD(PA)) must approve all media requests to film, videotape, or photograph AT training. PAOs receiving such media requests will submit them through ACOMS/ASCC/DRU public affairs channels to HQDA (SAPA–MR), Washington, DC 20310. HQDA (SAPA–MR) will coordinate requests with OASD (PA) and ODCS, G–3/5/7 and HQDA.

d. Prior to releasing Army-produced AT training photos, videotapes, films, or slides to the media, PAOs must obtain OASD (PA) and HQDA, ODCS, G–3/5/7 approval by submitting a copy of the visual image requested through channels described in the previous paragraph.

e. In response to media queries regarding a possible or actual terrorist threat at a particular installation or activity, the PAO may acknowledge, if appropriate, that increased security measures have been (or will be) taken without going into specific details. PAOs may acknowledge specific details concerning physical security measures taken if such information is obvious to the public-for example, increased guards at gates or additional patrols.

f. The installation PAO is the initial release authority for an incident or disturbance occurring on an installation until the incident is determined to be a terrorist act. Until the act is confirmed as a terrorist incident, the PAO will treat the disturbance as a regular criminal incident.

g. Once the incident has been determined to be an act of terrorism, and until another Federal agency assumes overall responsibility, PAOs will act in accordance with this regulation and AR 360–1, chapter 5. If the terrorist act creates a chemical or nuclear accident or incident, AR 360–1, chapter 12, will govern PA actions.

h. PAOs will immediately report all terrorist incidents through channels to HQDA (SAPA–PP), Washington, DC 20310. HQDA (SAPA–PP) in turn will notify OASD (PA).

i. Except for cases involving public safety, no public release of information regarding a terrorist incident may be made without OASD (PA) approval and HQDA, ODCS, G–3/5/7.

(1) PAOs, after coordinating proposed releases with their local crisis management team, will forward the proposal through the appropriate ACOM/ASCC/DRU to HQDA (SAPA–PP). HQDA (SAPA–PP) will coordinate release with OASD (PA) and HQDA, ODCS, G–3/5/7.

(2) In cases where the PAO releases information to the media prior to obtaining OASD (PA) approval, the information should be provided by the most expeditious means to HQDA (SAPA–MR). The intent is to ensure information released to the public by all Army levels is consistent. HQDA (SAPA–MR) will provide copies of such materials to HQDA, ODCS, G–3/5/7. The use of periodic, scheduled news briefings is one method to ensure essential, factual, and cleared information is provided the press during the course of an incident.

j. When commands declare a FPCON above NORMAL, command information programs should be used to keep internal audiences informed about actions being taken and the reasons for those actions. Information programs also should reinforce the requirement to maintain OPSEC.

k. During the course of an incident, Army personnel are not authorized to comment on, or speculate about, possible U.S. response to the terrorist act.

D–2. Policy governing counterterrorism forces

a. In responding to queries about national CT forces, PAOs at all levels may only state the following: "The U.S. Government has trained and equipped forces from all four Services to cope with terrorist incidents. We also have said command and control elements for these forces exist and have been exercised. These elements report to the Joint Chiefs of Staff, as do other command and control elements for military operations. We do not comment on any details concerning the circumstances under which these forces may be deployed, their identity, or tactics."

b. Requests to interview, film, photograph, or record CT personnel or their training will not be approved.

c. Questions beyond the scope of this guidance on CT forces should be referred to HQDA (SAPA–PP).

d. All public media requests to interview or film ARSOF personnel and training must be coordinated with the Commander, USASOC (AOPA), Fort Bragg, NC 28307. Requests dealing with CT issues will be forwarded by USASOC through USSOCOM to OASD (PA) for approval. HQDA (SAPS–MR) will be an information addressee on all such requests.

Appendix E
Antiterrorism Training Requirements

E–1. Level I, AT 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 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 (IED) attacks.

(7) Kidnapping and hostage survival.

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

c. All DOD personnel should be provided and retain personal copies of Chairman of the Joint Chiefs of Staff Guide 5260, "Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism," (October 14, 2005) and Chairman of the Joint Chiefs of Staff (CJCS) Pocket Card 5260 "Antiterrorism Individual Protective Measures" (October 1, 2001). Local reproduction of both CJCS issuances is authorized.

E–2. Level II, ATO 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 upon the development of 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 reference sources to include the AT Enterprise Portal (ATEP) on the secure internet protocol router network (SIPRNET) at https://www.atep.smil.mil or non-secure internet protocol router network (NIPRNET) at https://atep.dtic.mil/portal/site/atep.

(d) (I/U) Understand online Core Vulnerability Assessment Management Programs (CVAMP).

(e) (I) Understand necessary coordination with HN, Combatant Commands, Department of State, 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 (consider using the Joint Antiterrorism (JAT) Guide program).
(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 (consider using the JAT Guide).
(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 CVAMP.
(b) (I/U) CbT–RIF.
(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.
c. Review of the following Army, DOD and Joint Staff publications:
(1) (I/U) AR 525–13.

(2) (I) DODD 2000.12.
(3) (I/U) DODI 2000.16.
(4) (I/U) DODI 2000.18.
(5) (I/U) DOD O–2000.12–H.
(6) (I/U) CJCS Guide 5260.
(7) (I/U) Unified Facilities Criteria (UFC) 4–010–01, 4–010–02, and 4–021–01.
(8) (I/U) DOD 4500.54–G.

E–3. Level III, Pre-Command AT Training

a. The training described below applies to O5/O6 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 application.
(h) Comprehensive AT program review.
(2) Ensuring preparation of AT plans.
(a) Baseline FPCON posture.
(b) Mitigating CBRNE (including TIH)/WMD attack/risks.
(c) MOUs, MOAs, and MAAs.
(d) JAT Guide capabilities.
(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 force protection information.
(b) Fusion of intelligence, counterintelligence, and law enforcement information.
(c) Terrorism threat levels.
(6) Building a sustainable AT Program (CVAMP capabilities).
(7) Executing resource responsibilities.
(a) AT resourcing program.
(b) Role of CVAMP in resource process.
(c) Construction standards.
(8) Understanding use of force and rules of engagement (terrorist scenarios and hostile intent decisionmaking).

c. Review of the following Army, DOD and Joint Staff publications:

(1) (I/U) AR 525–13.
(2) (I) DODD 2000.12.
(3) (I/U) DODI 2000.16.
(4) (I/U) DODI 2000.18.
(5) (I/U) DOD O–2000.12–H.
(6) (I/U) CJCS Guide 5260.
(7) (I/U) Unified Facilities Criteria (UFC) 4–010–01, 4–010–02, and 4–021–01.
(8) DOD 4500.54–G.

E–4. Level IV, AT 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 F
AT Standards/Command-level Matrix

The following matrix portrays which AT standards must be implemented by higher headquarters (ACOM, ASCC, and DRU), installation/garrison, unit, tenant, and stand-alone activity commanders as specified in chapter 2, paragraphs 2–25 through 2–31.

Table F–1
AT Standards/Command-level Matrix

AT Standard	ACOM, ASCC, DRU	Installation and Garrison	Unit	Tenant	Stand-alone Activity
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, Antiterrorism Officer	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 Antiterrorism Officer Training	X	X	X	X	X
Standard 27, Level III Pre-Command AT Training	X	X	X	X	X

Table F–1
AT Standards/Command-level Matrix—Continued

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
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
Standard 35, CVAMP	X	X	X	X	X

Appendix G
Management Control Evaluation Checklist

G–1. Function
The function covered by this checklist is the management of Army AT Programs.

G–2. Purpose
The purpose of this checklist is to assist assessable commanders in evaluating the key management controls outlined below. It is not intended to cover all controls. Questions raised in this appendix are for checklist purposes only and should not be construed as an independent basis for authority to act in response to any particular question. Any such response must conform and comply with applicable statue and regulation.

G–3. Instructions
Answers must be based on the actual testing of key management 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 management 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-R (Management Control Evaluation Certification Statement).

G–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 priority intelligence requirements (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) 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 CRIMINT 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, ATOIC, 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 intelligence community 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 s 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 FM 3-100.12, FM 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, paragraph 3-9?

(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 Intelligence Community (IC) activities; other local community officials and individuals; the applicable U.S. country team; port authority officials and husbanding contractors, as appropriate, to provide for a continuous analysis of threat information to support the Threat Warning process?

(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 CRIMINT 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 300 or more 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 (i.e., 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 JSIVA Security Classification Guide?

(6) Are terrorism vulnerability assessments conducted consistent with the principles outlined in DOD O-2000.12–H, "DOD Antiterrorism Handbook," chapter 7?

(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 CVAMP within 120 days from the completion of the assessment?

(10) Are higher headquarters assessment (HHA) results populated into the CVAMP 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, stand-alone activity, 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. Antiterrorism Officer (ATO).

(1) For ACOM, ASCC, and DRU Commanders and Director, ARNG: 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 a stand-alone activity having 300 or more individuals assigned, occupied, or under the operational control of a designated commander or director: Is a Level II-certified ATO appointed (minimum grade of E-6 or higher or equivalent civilian grade)?

(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. AT Working Group (ATWG).

(1) For commanders of ACOMs; ASCCs; DRUs; HQ, ARNG; Army Garrisons; and stand-alone activities (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. Threat Working Group (TWG).

(1) For commanders of ACOMs; ASCCs; DRUs; HQ, ARNG; Army Garrisons; and stand-alone activities (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 Intelligence Community?

(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 stand-alone activities (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 High-Risk Personnel (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 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, "Physical Security Program," UFC 4–010–01 "DOD Minimum Standards for Buildings" and 4–010–02, "DOD Minimum AT Standoff Distances for Buildings," 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 DOD O–2000.12–H?

(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)

(f) Contract review procedures are developed and implemented to ensure contracts comply with AT provisions of the Defense Federal Acquisition Regulation Supplement.

(g) AT Level I training requirements are incorporated into contracts.

g. Standard 19. AT Measures for Critical Asset Security.

(1) Are AT risk mitigation measures developed and implemented for critical assets, resources, and personnel IAW DOD O-20002-H and AR 525-26?

(2) Are risk mitigation measures developed and implemented for those assets designated as Defense Critical Assets per DODD 3020.40?

(3) (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 Assets 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 mission essential vulnerable areas (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) (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 2000.18); mass notification system standards (UFC 4-021-01); establishment of medical surveillance systems (DODD 6490.2); 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 DODD 6200.3, "Emergency Health Powers on Military Installations," 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 IAW 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 stand-alone activity; 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 (MASCAL) 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 two 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) Is AT information provided to Defense contractors as required in the Defense Federal Acquisition Regulation Supplement (DFARS), Section 252.225-7043?

(3) 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?

(4) 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?

(5) 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?

(6) 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 three 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 Antiterrorism 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 three 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 CJCS 5261.01E, "CbT-RIF?"

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 Management Control Evaluation Checklist at appendix G or a higher headquarters approved (ACOM, ASCC, or DRU) checklist?

(4) Are assessments from a higher headquarters or DTRA JSIVA 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 three 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, military intelligence, CI, IO, 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 stand-alone activity 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 three 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, stand-alone activity, 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 public affairs officer (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 Terrorist Threat Warning Report (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 Terrorist Incident Report (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?

ii. Standard 35. CVAMP.

(1) Is CVAMP used to track all reported vulnerabilities of subordinate organizations and/or installations to resolution/closure?

(2) Are personnel designated to input information and data into the CVAMP?

(3) Have personnel designated to input information and data into the CVAMP completed the designated Joint Staff managed web-based training tutorial prior to operating the system?

(4) ACOM, ASCC, and DRU Commanders: Are all subordinate commands, installations, units, facilities, or activities (for which a higher headquarters assessment or comprehensive AT program review is conducted) identified and placed into their CVAMP hierarchy trees?

(5) Are the results from Terrorist Vulnerability Assessments identified in paragraph 5–7*b*(1)(a)–(f) and the assessments and comprehensive AT program reviews identified in paragraph 5–32*b*(1)–(6) populated into CVAMP in accordance with the reporting timeframes established paragraph 5–7*b*(6) and (7) and paragraph 5–32b.(7)?

5. Supersession

This checklist supersedes the checklist published AR 525–13, 4 January 2002.

6. Comments

Submit comments for improvement of this management controls tool to: HQDA (DAPM-MPO-AT), 2800 Army Pentagon, Washington, DC 20310-2800.

Glossary

Section I
Abbreviations

AAR
after action report

ACOM
Army command

ACIC
Army Counterintelligence Center

ACSIM
Assistant Chief of Staff for Installation Management

AMHS
Automated Message Handling System

AOC
Army operations center

AOR
area of responsibility

AR
Army regulation

ARNG
Army National Guard

ARNGUS
Army National Guard of the United States

ARSOF
Army Special Operations Forces

ASA(FM&C)
Assistant Secretary of the Army (Financial Management and Comptroller)

ASCC
Army service component command

AT
Antiterrorism

ATEC
Antiterrorism executive committee

ATEP
Antiterrorism enterprise portal

ATO
antiterrorism officer

ATOIC
antiterrorism operations and intelligence cell

ATTN
attention

ATWG
antiterrorism working group

BASOPS
base operations

BOD
board of directors

C4
command, control, communications, and computers

CALL
Center for Army Lessons Learned

CAR
Chief of the Army Reserve

CATA
criminal activity threat assessment

CBR
chemical, biological, and radiological

CBRNE
chemical, biological, radiological, nuclear and high yield explosive materials

Cbt-RIF
Combating Terrorism Readiness Initiatives Fund

Cbt-T
combating terrorism

CDR
commander

CCIR
commander's critical information requirements

CG
commanding general

CI
counterintelligence

CJCS
Chairman of the Joint Chiefs of Staff

CJCSM
Chairman of the Joint Chiefs of Staff Manual

COM
chief of mission

CONUS
continental United States

CoS
chief of staff

CPA
Chief of Public Affairs

CRIMINT
criminal intelligence

CT
counterterrorism

CTL
composite threat list

CVAMP
Core Vulnerability Assessment Management Program

DA
Department of Army

DARNG
Director, Army National Guard

DCIP
Defense Critical Infrastructure Program

DCS
Deputy Chief of Staff

DCSOPS
Deputy Chief of Staff for Operations and Plans

DFARS
Defense 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

DOJ
Department of Justice

DOS
Department of State

DPTM
Director of plans, training, and mobilization

DRU
direct reporting unit

DTRA
Defense Threat Reduction Agency

EDD
explosive detector dog

FBI
Federal Bureau of Investigation

FEMA
Federal Emergency Management Agency

FM
field manual

FOUO
for official use only

FP
force protection

FPAT
force protection assessment team

FPCON
force protection condition

GCC
geographical combatant commander

GOMO
General Officer Management Office

HHA
higher headquarters assessment

HN
host nation

HRB
high-risk billet

HRP
high-risk personnel

HRT
high-risk target

HQ
headquarters

HQDA
Headquarters, Department of the Army

HUMINT
human intelligence

IC
intelligence community

IED
improvised explosive device

IG
Inspector General

IMCOM
Installation Management Command

INSCOM
United States Army Intelligence and Security Command

IO
information operations

JAT
joint antiterrorism

JCS
Joint Chiefs of Staff

JFTR
joint federal travel regulations

JSIVA
joint staff integrated vulnerability assessment

JTTF
joint terrorism task force

LFA
lead federal agency

MAA
mutual assistance agreement

MASCAL
mass casualties

MCA
military construction, Army

MCAR
Military construction, Army Reserve

MDEP
Management Decision Execution Program

MDW
Military District of Washington

MEVA
mission essential or vulnerable area

MI
military intelligence

MILCON
military construction

MP
military police

MOA
memorandum of agreement

MOU
memorandum of understanding

MSC
major subordinate command

NBC
nuclear, biological, and chemical

NCIC
National Crime Information Center

NIPRNET
non-secure internet protocol router network

OASD (PA)
Office of the Assistance Secretary of Defense (Public Affairs)

OCONUS
outside continental United States

OPORD
operation order

OPREP
operational reporting

OPSEC
operations security

OSD
Office of the Secretary of Defense

PA
public affairs

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

POC
point of contact

POM
program objective memorandum

PPBE
planning, programming, budgeting, and execution

PSVA
personal security vulnerability assessment

RAM
random antiterrorism measures

RC
reserve component

RCS
requirement control symbol

ROTC
Reserve Officer Training Corps

SAEDA
subversion and espionage directed against the U.S. Army

SCI
sensitive compartmented information

SIPRNET
secure internet protocol router network

SITREP
situation report

SJA
staff judge advocate

SMC
senior mission commander

SO
security officer

SOFA
status of forces agreement

SOP
standing operating procedures

SROE
standing rules of engagement

SROF
standing rules of force

TACON
tactical control

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, training, 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

USAMC
U.S. Army Materiel Command

USAMPS
U.S. Army Military Police School

USANETCOM
U.S. Army Network Enterprise Technology Command

USARNORTH
U.S. Army North

USASOC
U.S. Army Special Operations Command

USAR
U.S. Army Reserve

USCG
U.S. Coast Guard

USDR
U.S. Defense representative

USMEP
U.S. Military Processing Stations

USSOCOM
U.S. Special Operations Command

WMD
weapons of mass destruction

Section II
Terms

Antiterrorism
Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

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.

Combating terrorism
Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum.

Counterterrorism
Operations that include offensive measures taken to prevent, deter, preempt, and respond to terrorism.

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
A criticality assessment addresses the effect of temporary or permanent loss of key assets or infrastructures on the

installation or a unit's ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability, and infrastructure support.

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.

Deterrence
The prevention of an action by fear of the consequence. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction.

DOD Components
The Office of the Secretary of Defense (OSD); the Military Departments, including the Coast Guard when operating as a service of the Navy; the Chairman, Joint Chiefs of Staff and the Joint Staff; the combatant commands; the Inspector General of the Department of Defense (IG, DOD); and the Defense agencies.

DOD 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.

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 U.S.C 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
Actions taken to prevent or mitigate hostile actions against DOD personnel (to include Family members), resources, facilities, and critical information. Force protection does not include actions to defeat the enemy or protect against accidents, weather, or disease.

Force protection condition
A DOD-approved system standardizing DOD's identification of and recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates coordination among DOD Components and support for antiterrorism activities.

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
Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.

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.

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.

Hostage
Any person held against their will as security for the performance or nonperformance of specific acts.

Improvised explosive device
A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate military stores, but is normally devised from nonmilitary components.

Intelligence
1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

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.

International (or transnational) terrorism
Terrorism in which planning and execution of the terrorist act transcends national boundaries.

Mission essential vulnerable areas
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.

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.

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
That part of the security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

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
1. Measures taken by a military unit, activity or installation to protect itself against all acts designed to, or that may, impair its effectiveness. 2. A condition that results from the establishment and maintaining protective measures that ensures a state of inviolability from hostile acts or influences.

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

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.

Stand-alone activities
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
An agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state. Agreements delineating the status of visiting military forces may be bilateral or multilateral. Provisions pertaining to the status of visiting forces may be set forth in a separate agreement, or they may form a part of a more comprehensive agreement. These provisions describe how the authorities of a visiting force may control members of that force and the amenability of the force or its members to local law or to the authority of local officials. To the extent the agreements delineate matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements.

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

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 LFA (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 vulnerability assessment
1. An assessment to determine the vulnerability to a terrorist attack against an installation, unit, exercise, port, ship, residence, facility, or other site. It identifies areas of improvement to withstand, mitigate, or deter acts of violence or terrorism. 2. The process the commander uses to determine the susceptibility to attack from the full range of threats to the security of personnel, Family members, and facilities, which provide a basis for determining AT measures that can protect personnel and assets from terrorist attacks. 3. 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.

Terrorism threat assessment
1. The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. 2. The product of a threat analysis for a particular unit, installation, or activity.

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

Vulnerability
1. In AT, a situation or circumstance, which if left unchanged, may result in the loss of life or damage to mission essential resources. 2. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or will to fight diminished. 3. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. 4. The characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard.

Weapons of mass destruction
Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and dividable part of the weapon.

Section III
Special Abbreviations and Terms
This section contains no entries.

PIN 063256–000