

Military Operations
Antiterrorism Program

History. This is the first printing of this regulation.

Summary. This regulation prescribes policy and procedures and assigns proponenty for any Fort Hood antiterrorism program. This directive implements planning guidance of Army Regulation (AR) 525-13 and Department of Defense Instruction DODI 2000-12.H to develop and maintain a directive antiterrorism program.

Applicability. This regulation is intended for implementation in conjunction with III Corps and Fort Hood Regulation 525-7 (Terrorist Threat/Incident Response) and applies to agencies

and units stationed at Fort Hood or transiting the installation, as well as deployed Fort Hood units.

Supplementation. Local supplementation of this regulation is prohibited except upon approval of Directorate of Human Resources (DHR).

Suggested Improvements. The proponent of this regulation is the Directorate of Plans, Training, Mobilization, and Security (DPTMS), Force Protection Branch. Users are invited to send comments and suggested improvements on DA Form 2028 to Director, DPTMS, ATTN: IMSW-HOD-POL, (Antiterrorism), Fort Hood, Texas 76544-5056.

FOR THE COMMANDER:

JOHN M. MURRAY
Colonel, GS
Chief of Staff

Official:



CHARLES E GREEN, SR.
Directorate of Human
Resources

DISTRIBUTION:
IAW FH Form 1853, S

Contents

Overview, 1, *page 3*
Purpose, 1a, *page 3*
References, 1b, *page 3*
Abbreviations and terms, 1c, *page 3*
Antiterrorism program, 1d, *page 3*

Responsibilities, 2, *page 4*
Installation commander, 2a, *page 4*
Antiterrorism officer, 2b, *page 4*

Public affairs officer, 2c, *page 6*

Major subordinate command commanders/Directorates, 2d, *page 7*

Antiterrorism plan measures, 3, *page 7*

Antiterrorism program phases, 3a, *page 7*

Antiterrorism key elements, 3b, *page 9*

Antiterrorism training, 3c, *page 12*

Force protection condition, 3d, *page 13*

Random antiterrorism measure program, 3e, *page 14*

Antiterrorism assessments, 3f, *page 15*

Local vulnerability assessment, 3g, *page 15*

Assessment areas, 3h, *page 16*

Army antiterrorism standards and implementing guidance, 4, *page 17*

Antiterrorism critical tasks, 4a, *page 17*

Critical task 1: Establish an antiterrorism program, 4b, *page 17*

Critical task 2: Collection, analysis, and dissemination of threat information, 4c, *page 19*

Critical task 3: Assess and reduce critical vulnerabilities (conduct antiterrorism assessments), 4d, *page 20*

Critical task 4: Increase antiterrorism awareness in every soldier, civilian, and family member, 4e, *page 21*

Critical task 5: Maintain installation defenses in accordance with force protection conditions, 4f, *page 23*

Critical task 6: Establish civil/military partnership for weapons of mass destruction crisis, 4g, *page 24*

Critical task 7: Terrorist threat/incident response training, 4h, *page 25*

Critical task 8: Conduct exercises and evaluate/assess antiterrorism plans, 4i, *page 26*

Appendix A. References, *page 27*

Glossary and terms, *page 28*

OVERVIEW

1

Purpose

This regulation outlines policies, guidance, and procedures for implementation of the Fort Hood antiterrorism program.

1a

References

Appendix A lists required and related references.

1b

Abbreviations and terms

The glossary explains abbreviations and terms used in this regulation.

1c

Antiterrorism (AT) program

The antiterrorism (AT) program is both a Department of Defense (DOD) and Department of the Army (DA) program whose goal is to maximize readiness and combat efficiency.

- The AT program is a collective effort that seeks to reduce the likelihood that DOD affiliated personnel, their families, facilities, and materiel shall be subject to a terrorist attack and to prepare to respond to the consequences of such attacks should they occur.
- Standard 14 of DOD 2000-16 describes a commander's major requirements and responsibilities for implementing an AT program.
- The AT program incorporates all defensive measures used to reduce the vulnerability of individuals and property to terrorist acts to include limited response and containment by local forces.
- It is essential to stress from the beginning that the effectiveness of any program is directly impacted by a commander's emphasis of the importance of his or her program, regardless of the level of command.

1d

RESPONSIBILITIES

2**Installation
commander**

The installation commander will:

- Incorporate AT into their overall force protection (FP) program.
- Appoint an AT officer (minimum grade of O-3 or equivalent civilian grade) within operations or a location best suited to execute the program.
- Publish guidance for the execution of AT standards within the overarching FP security program.
- Designate a focal point to coordinate requirements to receive and disseminate time-sensitive threat information received from federal, state, local, and United States (US) intelligence agencies.
- Ensure all tenants and supported reserve component (RC) units/activities are participants in the AT planning process and are included in AT plans, providing guidance and assistance as required.
- Implement and execute Army AT standards in accordance with implementing guidance identified in chapter 4.

2a**Antiterrorism
officer (ATO)**

The antiterrorism officer (ATO) will:

- Have a basic understanding of existing policy and standards and where to access information for reference.
- Organize structure for AT highlights how units are structured to execute AT responsibilities. For example, a discussion of FP working groups, threat working groups, intelligence fusion cells, and their roles in bringing together the various functional representatives may be appropriate.

(continued on next page)

**Antiterrorism
officer (ATO)
(continued)**

- Fully comprehend the threat assessment process, to include actions taken to perform an assessment, the individuals responsible for those actions, and the application/usefulness of the assessment final product. ATOs should understand that the local threat assessment, as addressed in an AT program, is a different product than a country threat assessment produced by higher echelon intelligence organizations. This area of instruction should also include discussion of the following:
 - Integration of intelligence, counterintelligence, and law enforcement functions via a threat working group-like cell.
 - Importance of threat information flow throughout the chain of command.
 - Weapons of mass destruction (WMD) threat.
 - Need to conduct local threat assessments annually.
 - Elements of a risk assessment.
- The ATO is responsible for establishing and maintaining a formal documentation methodology documenting AT resource requirements about threat, asset criticality, vulnerabilities, current program effectiveness, and commander's risk. Requirements must be continuously documented and ready for funding data calls for information.
- Once the requirements are documented, the information needs to be articulated and justified to the installation AT working groups, budget personnel, installation councils, and commander.
- Work continuously with the programming, resourcing, and budgeting personnel to justify requirements and assist in determining the best source of funding and the associated data call timeline. Continuously forward AT requirements through the chain of command regardless of funding availability and always follow-up and track requirements status.

2b

**Public
affairs
officer
(PAO)**

The public affairs officer (PAO) will:

- Maintain the flow of authoritative information between the authorities and the media.
- Keep the public informed.
- Protect the interests of hostages or DOD personnel participating in incident resolution.
- The PAO has specific functions to perform, including screening information provided to the media to ensure operational security, preserving the privacy of hostages, victims, and their families and advising the DOD and other US government or foreign government officials managing the crisis on public affairs matters.
- Public affairs responsibilities for dissemination of information following terrorist incidents mirror jurisdiction and authority. Public affairs responsibilities belong principally to the installation activity where the terrorist incident has occurred, with guidance and support coming from the chain of command.
- Installation PAO have a special prominent role to play in the AT program. Installations, facilities, organizations, and commands should have an ongoing program intended to reduce its risk and vulnerability to terrorist attack. A PAO annex should be developed in support of an installation AT plan.
- PAO plays a major role in the AT program. They are educators, making audiences, within the installation, aware of the threat of terrorism.
- PAO exercises constant vigilance and sensitivity to the needs of their audiences. They also remember that the terrorists themselves are a part of that audience. PAO constantly coordinates with other members of the installation, activity, organization, or command staff.

(continued on next page)

**Public
affairs
officer
(PAO)
(continued)**

- PAO is a member in the force protection working group. During a terrorist incident, the PAO provides information to local authorities as well as the media, thereby allowing the commander and ATO to focus on the incident at hand.
- PAO should establish an Incident Information Center in the event of a terrorist incident. The purpose of the center is to provide a single location where news media can meet with the PAO to attain information about the incident. It should be located where media access can be controlled, for example, in close proximity to an access control point. The Incident Information Center should not be collocated with the Installation Operation Center (IOC).
- AT PAO uses the various mass notification means available to educate personnel; including newspapers, newsletters, flyers, and closed circuit television.

2c

**Major
subordinate
command
(MSC)
Commanders/
Directorates**

The major subordinate command (MSC) Commanders/Directorates will:

- Participate in the host installation AT planning process. During this planning process, any tenant unit/activity personnel support requirements will be identified that are required for the implementation of host installation force protection condition (FPCON) levels.
- Comply with host installation AT requirements.
- Provide personnel support as specified in host installation AT plans.

2d

ANTITERRORISM PLAN MEASURES

3

**Antiterrorism
program
phases**

The AT plan contains all the specific measures taken to establish and maintain an AT program. AT program elements include the risk management process, planning, training and exercises, resource generation, and a program review.

(continued on next page)

**Antiterrorism
program
phases
(continued)**

- The AT program has two phases: proactive and reactive (crisis management).
- The proactive phase encompasses the planning; resourcing, preventive measures, awareness, education, training, and exercising that take place prior to a terrorist incident. Commanders and directors must consider the installation infrastructure critical to mission accomplishment; integration of physical assets; funding requirements; security forces to detect, assess, delay, and respond to at threat; awareness education, and training (specialized skills proficiency training and exercising plans). Proactive phase begins with a deliberate application of the AT risk management process. AT risk management process:
 - Threat - threat assessment (TA). The TA should identify the terrorist threat. For each group that may be a threat, the assessment provides information on the group's intent, capability, history as well as any specific targeting information that may be available.
 - Criticality - criticality assessment. This is done to determine which assets need to be protected. The criticality assessment determines the importance of each asset, the effect of a terrorist attack on the assets, and the recoverability of the asset from attack.
 - Vulnerability Assessment (VA). The VA evaluates and determines the vulnerability to a terrorist attack of an installation, unit, exercise, port, ship, residence, facility, or other site. It assesses each asset and identifies shortfalls or weaknesses that make the asset vulnerable, determines if existing countermeasures are effective, and prioritizes these vulnerabilities.
 - Risk Assessment. Risk assessment combines the criticality, threat, and vulnerability rating given to each asset and unwanted event. It uses the theory that in order for there to be risk, each one of the elements (criticality, threat, and vulnerability) must be present; therefore, risk = criticality x

(continued on next page)

**Antiterrorism
program
phases
(continued)**

threat x vulnerability. Risk is based on the value of the asset in relation to the threats and vulnerabilities associated with it.

- The reactive phase includes implementation of crisis response plans, limited response, and initiation of the appropriate response to a terrorist incident (military police and security forces, fire, hazardous material chemical, biological, radiological, nuclear and high yield explosive (CBRNE), mass casualty). The AT risk management process generally follows multi-service tactics, techniques, and procedures for tactical level risk management in the planning and execution of operations. The process has two levels of application: deliberate and crisis action. Available time to complete the process is the basic factor that shall determine the level of application. Deliberate AT risk management allows the application of the complete process when time is not critical. Crisis AT risk management is conducted immediately before or after a terrorist attack by doing a mental or verbal review of the situation using the basic AT risk management process.
- Antiterrorism working group (ATWG). The ATWG meets at the action officer level to develop and recommend policy; prepare planning documents; and conduct criticality, vulnerability, and risk assessments.
- The threat working group (TWG) consists of the ATO, counterintelligence representative, law enforcement representative, information operations representative, and CBRNE representative. Installation threat fusion member must obtain local terrorist threat information by querying the Federal Bureau of Investigation (FBI) through the installation's law enforcement liaison, local law enforcement, and other federal agencies.

3a

**Antiterrorism
key elements**

The AT key elements are the:

- Terrorism threat assessment. Commanders shall prepare a terrorism threat assessment for those personnel and assets for which they have AT responsibilities. The threat assessment shall be prepared at least annually and should identify the full range of

(continued on next page)

**Antiterrorism
key elements
(continued)**

known or estimated terrorist capabilities for use in conducting vulnerability assessments and planning countermeasures. Threat analysis is required to adequately support risk management decisions of both stationed forces within, and those in-transit through, higher-threat areas including ports, airfields, and inland movement routes. Terrorism threat assessments shall be the basis and justification for recommendations on AT enhancements, program/budget requests, and the establishment of FPCON.

- Risk assessment. Risk assessments provide the commanders with a method that assists them in making resource allocation decisions designed to protect their people and assets from possible terrorist threats in a resource-constrained environment. Commanders shall conduct risk assessments to integrate threat and vulnerability assessment 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. Risk assessment allows the commander to obtain a clear picture of the current AT posture and identify those areas that need improvement. During the risk assessment, important information is also collected that can be used when writing the overall AT plan.
- AT physical security measures. AT physical security measures shall be considered, must support, and must be referenced within the AT plan to ensure an integrated approach to terrorist threats. Where there are multiple commanders at an installation, the Installation Commander is responsible for coordinating and integrating individual unit physical security plans and measures into the AT plan. The AT physical security measures shall integrate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide maximum AT protection to personnel and assets. Well designed AT physical security measures include detection, assessment, delay, denial, and notification.
- Terrorist incident response measures. Limiting the effects and the number of casualties resulting from an attack will undermine the terrorists' overall objectives. An effective incident response strategy and capability can contribute to deterring terrorist attacks if our adversaries recognize the US ability to limit the effects of their attacks. Installation Commander shall prepare installation-wide terrorist incident response measures. These measures shall

(continued on next page)

**Antiterrorism
key elements
(continued)**

include procedures for determining the nature and scope of incidence response; procedures for coordinating security, fire, and medical first responders; and steps to reconstitute the installation's ability to perform AT measures. The terrorist incident response measures should address the full scope of the installation's response to a terrorist incident. The nature of the response will depend on many factors. The character of operations underway at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

- Terrorist consequence management. Commanders shall include terrorist consequence management preparedness and response measures as an adjunct to the installation AT plan. The terrorist consequence management measures should include emergency response and disaster planning and/or preparedness to respond to a terrorist attack for installation and/or base engineering, logistics, medical, mass casualty response, transportation, personnel administration, and local and/or host nation support.
- Training and exercises. Commanders (battalion-level and above) shall conduct field and staff training to exercise AT plans, to include AT physical security measures, terrorist incident response measures, and terrorist consequence management measures, at least annually. AT training and exercises shall be provided the same emphasis afforded combat task training and executed with the intent to identify shortfalls affecting the protection of personnel and assets against terrorist assault and subsequent consequence management efforts. AT training, particularly pre-deployment training, shall be supported by measurable standards and include credible deterrence/response, tactics, techniques and procedures. AT training shall also be incorporated into unit-level training plans and pre-deployment exercises. To realize incorporation of lessons learned, commanders should maintain exercise documentation for no less than one year.
- Comprehensive AT Review. Commanders at all levels shall review their own AT program and plans at least annually to facilitate AT program enhancement. Commanders at all levels shall likewise review the AT program and plan of their immediate subordinate in the chain of command at least annually. While such reviews do not constitute a vulnerability assessment, they are intended to ensure compliance with the standards contained in this regulation. To

(continued on next page)

**Antiterrorism
key elements
(continued)**

ensure the design and implementation of physical security measures coincident with the AT program are consistent with the local terrorist threat level, AT programs shall also be reviewed when the terrorism threat level changes.

3b

**Antiterrorism
training**

These standards address personnel responsible for managing AT programs and training requirements for individuals, commanders, senior executive officers, high-risk personnel and those assigned to high-risk billets, and units preparing to deploy.

- Level I awareness training. Individual security awareness and antiterrorism training are essential elements of an overall AT program. Each individual must share in this responsibility by ensuring the proper degree of alertness and employment of personal protection measures. AT awareness training begins immediately upon entry into service with the DOD and continues throughout the career of all DOD personnel.
- The Level I awareness training requirement should not be confused with area of responsibility (AOR) specific training. Awareness training is conducted annually. For individuals traveling outside the continental of United States (OCONUS), in addition to completing the annual awareness training, they must also receive an AOR specific update within three months of travel.
- Individuals administering Level I training must be qualified to do so by attending a formal service approved Level II ATO training course. Commanders may qualify subject matter experts who have not attended a service approved ATO course to administer Level I training. In the latter case, subject matter experts may be exempt from attending Level II training provided they receive AT and individual protection training that reviews current AT publications and identifies methods to obtain AOR specific updates.
- Level II antiterrorism officer training (ATO). Each installation and/or deploying unit (e.g., battalion, squadron) must have at least one assigned ATO. Units down to battalion level will have a Level II trained AT officer, sergeant first class or higher, who serves as the commander's planner/advisor on AT matters and serves as the

(continued on next page)

**Antiterrorism
training
(continued)**

instructor for Level I unit training. Personnel identified as unit ATOs are responsible for managing the AT program, advising the commander on AT issues, and providing Level I awareness training.

- Level III pre-command AT training. Level III training for commanders shall be conducted at the Lieutenant Colonel (O-5) and Colonel (O-6) level by the services in conjunction with pre-command training. The focus of this training shall be on the responsibilities discussed in the pertinent DOD 2000 series publications, service publications, and associated joint doctrine.
- Chair Joint Chiefs of Staff Level IV antiterrorism executive seminar. Executive level seminars conducted by the Joint Staff and tailored for an O-6 to Major General (O-8) audience. The focus of this training is to provide current updates, briefings, and discussion topics pertinent to an AT program. The training shall include, but not be limited to, AT simulations and war games. Level IV seminars are held three times a year. The combatant commanders, services, and DOD agencies are responsible for nominating attendees.

3c

**Force
protection
condition
(FPCON)**

There are five FPCONs. Supporting measures for each condition are listed below. The circumstances that apply and the purposes of each protective posture are as follows:

- FPCON Normal: Applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.
- FPCON Alpha: Applies when there is an increased general threat of possible terrorist activity against personnel or facilities and the nature and extent are unpredictable. Alpha measures must be capable of being maintained indefinitely. Refer to III Corps and Fort Hood Regulation 525-7, Terrorist Threat/Incident Response, Chapter 3 for measures.
- 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 relations with local authorities. In addition to the measures required by

 (continued on next page)

**Force
protection
condition
(FPCON)
(continued)**

FPCON Alpha, refer to III Corps and Fort Hood Regulation 525-7, Terrorist Threat/Incident Response, Chapter 3 for measures.

- 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. Refer to III Corps and Fort Hood Regulation 525-7, Terrorist Threat/Incident Response, Chapter 3 for measures.
- 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. Normally, this FPCON is declared as a localized condition. FPCON Delta measures are not intended to be sustained for substantial periods. Refer to III Corps and Fort Hood Regulation 525-7, Terrorist Threat/Incident Response, Chapter 3 for measures.

3d

**Random
antiterrorism
measure
program
(RAMP)**

Commanders and directors should randomly change their AT tactics, techniques, and procedures so that they ensure a robust security posture from which terrorists cannot easily discern patterns or routines that are vulnerable to attack. An effective random antiterrorism measure program (RAMP) shall enable security to appear not only formidable but also unpredictable and ambiguous to instill uncertainty in terrorist planning.

- The basic approach for RAMP is to select security measures from higher FPCONs, as well as other measures not normally associated with FPCONs (command developed measures or locally developed site-specific measures) that can be employed in a random manner to supplement the basic FPCON measures already in place. Using a variety of additional security measures in a normal security posture prevents overuse of security forces, as would be the case if a higher FPCON were to be maintained for an extended period. Selected random antiterrorism measures (RAMs) offer an alternative to full implementation of a higher FPCON level. This is particularly important when terrorist threat estimates suggest that lower FPCONs may not, for the moment, be adequate in view of the risk, vulnerability, and criticality of DOD assets at the installation or facility.

(continued on next page)

Random antiterrorism measure program (RAMP) (continued)

- Executing a comprehensive RAMP. Executing a comprehensive RAMP enables commanders/directors to maintain/sustain lower FPCON without compromising security effectiveness. In addition, it maximizes scarce security resources and minimizes security force burnout and degradation in command AT awareness.
- RAMP responsibility. The installation ATO is in charge of the RAMP, not the Directorate of Emergency Services (DES) or security officer if a separate entity/individual. However, the ATO should coordinate with the DES/security officer regarding RAM that require utilization of security personnel. The ATO should monitor, track, and analyze RAMP implementation efforts.

3e

Antiterrorism assessments

Combatant commander/service is mandated to develop an AT VA capability. VA helps determine the vulnerability of a facility to a terrorist attack and identifies areas of improvement to withstand, mitigate, or deter the attack. Three types of assessments are:

- Joint Staff integrated vulnerability assessments (JSIVAs).
- Combatant commander/service integrated vulnerability assessments (IVAs).
- Local vulnerability assessments (LVAs).
- Combatant commanders and/or Directorates shall ensure lower level AT programs receives a higher headquarters vulnerability assessment at least once every 3 years to ensure unity of AT efforts throughout the AORs or subordinate commands.

3f

Local vulnerability assessment (LVA)

Local vulnerability assessments (LVAs):

- Commanders shall conduct a local vulnerability assessment for facilities, installations, and operating areas within their area of responsibility. The local vulnerability assessment shall address the broad range of physical threats to the security of personnel and assets and shall be conducted at least annually.

(continued on next page)

**Local
vulnerability
assessment
(LVA)
(continued)**

- The Defense Threat Reduction Agency (DTRA) AT/FP vulnerability assessment team guidelines is an excellent tool available to help conducting vulnerability

3g**Assessment
areas**

Assessment areas:

- AT plans and programs. The assessment shall examine the installation AT program and its ability to accomplish appropriate standards contained in those established by the appropriate combatant command, service, or DOD agency.
- Counterintelligence, law enforcement liaison, and intelligence support. The assessment shall focus on the installation's ability to receive threat information and warnings from higher headquarters and local resources, actively collect information on the threat (when permitted and in accordance with applicable law and regulations), process that information to include local fusion and analysis, and develop a reasonably postulated threat statement of the activity. Further, the assessment shall examine the ability to disseminate threat information to subordinate commands, tenant organizations, assigned to or visiting DOD personnel (including military members, civilians and contractor employees, and dependents), and how that process supports the implementation of appropriate force protection measures to protect military personnel, DOD civilians and family members.
- AT physical security measures. The assessment shall determine the installation's ability to protect personnel by detecting or deterring terrorists, and failing that, to protect by delaying or defending against acts of terrorism. Physical security techniques include procedural measures such as perimeter security, security force training, security surveys, medical surveillance for unnatural disease outbreaks, and armed response to warning or detection as well as physical security measures such as fences, lights, intrusion detection devices, access control systems, closed circuit television cameras, personnel and vehicle barriers, biological, chemical, and radiological agent detectors and filters, and other security systems.

3h

ARMY ANTITERRORISM STANDARDS AND IMPLEMENTING GUIDANCE

4

Antiterrorism critical tasks This section provides a critical task list framework that defines eight AT critical tasks commanders must implement to obtain DODs AT objectives to deter incidents, employ counter measures, mitigate effects, and conduct incident recovery. Commanders will execute Army standards that ensure compliance with all DOD mandatory standards as outlined in applicable regulations and directives (DODI 2000.16).

- All of the AT critical tasks are discussed below. The discussion of each contains a statement of the standard and implementing instructions.
- Commanders should develop more specific standards and supplemental guidance as appropriate to the local situation.

4a

Critical task 1: Establish an antiterrorism program Army Standard 1: 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 attacks.

- Implementing guidance.
 - All commanders are responsible for developing a full working knowledge of AT policies.
 - Commanders will ensure that their AT program is proactive and include the tenets of counter surveillance, counterintelligence, and other specialized skills as a matter of routine. Commanders will incorporate proactive assets to detect and deter terrorists.
 - Commanders will establish clear operational responsibility for AT for all units and individuals whether permanently or temporarily assigned. When responsibilities for AT overlap and are not otherwise governed by law or specific DOD/service policy, the affected parties will resolve this conflict through the preparation of a memorandum of agreement clearly outlining AT responsibilities. Additionally, commanders will verify that

 (continued on next page)

**Critical task 1:
Establish an
antiterrorism
program
(continued)**

procedures are in place to ensure each individual and unit is aware of who is operationally responsible for AT and that those personnel operationally responsible for AT are notified upon the arrival and departure of individuals and units.

- Installation commander will:
 - Establish an AT committee and working group that focuses on planning, coordinating, and executing the installation's AT program.
 - Establish proactive AT plans, orders, or other implementing guidance that addresses procedures to collect and analyze threat information and threat capability; assess vulnerability to threat attacks; and implement procedures to deter, detect, and defend; and recover from terrorist threats to include WMD.
 - AT programs will be based on assessments of both threats and identified vulnerabilities. Antiterrorism proactive operational planning will identify, coordinate, allocate, and employ resources to ensure AT measures are developed that provide the appropriate level of protection for all applicable threats.
 - Commanders will coordinate AT plans and orders with the local supporting FBI office and state and local law enforcement agencies in addition to all appropriate Army law enforcement and security organizations.
 - Units down to battalion level will have a Level II trained AT officer, sergeant first class or higher, who serves as the commander's planner/advisor on AT matters and serves as the instructor for Level I unit AT training.
 - All units will incorporate AT planning into all aspects of their deployments from home station. Special emphasis will be given to the planning and execution of AT protective measures and terrorist threat/incident response when moving over public highways and transiting through commercial/public transportation centers that present high risk targets to terrorists (that is, rail stations/yards, bus terminals, airports, seaports, and harbors). Unit AT plans will be approved by the next higher commander (minimum battalion commander).

4b

Critical task 2: Army standard 2: Commanders will develop a system to collect, analyze, and disseminate terrorist threat information and apply the appropriate FPCON.

Collection, analysis, and dissemination of threat information

- Implementing guidance.
 - Commanders will ensure AT intelligence information is developed, collected, analyzed, and disseminated in a timely manner. Current intelligence will be integrated into the AT training program.
 - Commanders at installation level and above will have a fully integrated foreign, domestic, and criminal intelligence AT intelligence program focused and based on priority intelligence requirements priority incident report (PIR) that provide the appropriate threat information to protect personnel, family members, facilities, material, and information in all locations and situations. The commander will ensure production and analysis requirements are focused and based on PIR. PIR must be reviewed for currency, revalidated at least annually, and updated whenever appropriate to meet changing threats and/or requirements.
- Commanders will:
 - Develop a process based on threat information and/or guidance from higher headquarters to raise or lower FPCONs. FPCON transition procedures and measures will be disseminated and implemented by all subordinate and tenant commanders. All commanders can set a local FPCON; subordinate commanders can raise but not lower a higher-level commander's FPCON.
 - Ensure FPCON procedures contain provisions to notify all organic, tenant, and supported units, to include supported RC units.

4c

-
- Critical task 3: Assess and reduce critical vulnerabilities (conduct antiterrorism assessments)** Army standard 3: Commanders will continuously conduct assessments of their antiterrorism efforts, to include overall program review, assessment of individual physical, and procedural security measures to identify vulnerabilities and unit pre-deployments assessments.
- Implementing guidance.
 - The focus of vulnerability assessments is to determine the unit's 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 standards.
 - Installation commander will conduct a self-assessment of their AT programs within 60 days of assumption of command and annually thereafter. The incorporation of additional tasks are authorized. An assessment from the Headquarters, Department of the Army (HQDA), Forces Command (FORSCOM), Installation Management Agency (IMA) can be used to meet the self-assessment annual requirement.
 - Installation commander is required to conduct a comprehensive assessment a minimum of once every three years. This comprehensive self-assessment is in addition to all the other assessment requirements. Assessment team expertise and composition must, at a minimum, support assessment of the following functional areas:
 - Physical security.
 - Engineering.
 - Operations, training, and exercises.
 - Military intelligence.
 - Criminal intelligence.
 - Command and Control (C2) Protect.
 - Law enforcement.
 - Threat options.
 - Operation Security (OPSEC).
 - Medical.
 - Executive protection/high risk personnel.

(continued on next page)

**Critical task 3:
Assess and
reduce critical
vulnerabilities
(conduct
antiterrorism
assessments)**

- Vulnerability assessments will serve as a basis and justification for AT plans, enhancements, program/budget requests, and establishment of FPCONs.
- Vulnerability assessments will be part of the leader's reconnaissance in conjunction with deployments. Follow-on vulnerability assessments will be conducted for all deployments as determined by the commander or directed by higher headquarters.
- Pre-deployment vulnerability assessments will be conducted for units deploying OCONUS, whether the deployment is for an exercise or operational mission/support. Pre-deployment assessments will include threat assessment and vulnerability assessment of area port of embarkation (APOEs), port of embarkation (POEs), base camps, support structures (contract and host nation), and local operating communities.
- 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.

4d

**Critical task 4:
Increase
antiterrorism
awareness in
every soldier,
civilian, and
family
member**

Army standard 4: 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.

- Implementing guidance.
- Within this standard are seven subordinate tasks as follows:
 - Ensure AT training is an integral part of unit training plans, major training exercises/events, and a special interest item at training management reviews.
 - Enhance the general awareness of terrorism issues (command information program, PAO effort, etc.).
 - Conduct annual AT awareness training.

(continued on next page)

**Critical task 4:
Increase
antiterrorism
awareness in
every soldier,
civilian, and
family
member
member
(continued)**

- Ensure unit level AT officers are formally trained and certified.
 - Provide senior level leadership with AT knowledge (level IV AT training).
 - In significant and high threat areas, ensure personnel receive training concerning hostage survival.
 - Assign AT officers at battalion and above level units to provide training to unit members and advise the commander on AT matters. Ensure unit level AT officers are formally trained and certified.
-
- Commanders will incorporate AT into their command information programs. The PAO at each level of command will serve as the primary spokesperson to the news media in the event of an AT incident. Commanders also will develop an awareness program to ensure visibility of the AT program and enhance awareness of all personnel.
 - Commanders will ensure all military and DA civilians associated with their command receive annual antiterrorism awareness and receive an AOR update prior to deploying to an area of a higher threat level or within two months of traveling OCONUS. Commanders will offer all DOD employed contractors, associated with their command, annual antiterrorism awareness training and will offer an AOR update prior to traveling OCONUS. Units will maintain a memorandum for record documenting an individual's training. Training awareness status will be reported quarterly to higher headquarters.
 - Battalion and brigade level commanders will receive AT training in the Army pre-command course (PCC) training courses at Fort Leavenworth, Kansas. Instruction, using the training doctrine (TRADOC)-developed PCC training support package, will provide commanders with knowledge, skills, and abilities necessary to implement the Army AT.

4e

-
- Critical task 5: Maintain installation defenses in accordance with force protection conditions (FPCON)** Army standard 5: Commanders will ensure that AT specific security procedural and physical measures are employed to protect personnel, information, and material resources from terrorist threats.
- Implementing guidance.
 - Installation commander will formally identify all installation high-risk targets (HRT) and use HRT as the focus for developing AT plans and implementing counter terrorism (CT) security measures. HRT should include areas of high personnel concentrations (that is, troop billets, headquarters above brigade level, movie theaters, schools, and office buildings).
 - Installation commander will ensure that installation vehicle access procedures are implemented in accordance with AR 190–16.
 - Commanders will ensure personnel who are at a greater risk than the general population, by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat are identified and assessed. Personnel requiring additional security to reduce or eliminate risks will be formally designated as high-risk personnel (HRP) to make them eligible for special control/security measures. HRP will be identified and protected in accordance with AR 190–58.
 - Installation commander and commanders of units in-transit will develop site specific measures or actions for each FPCON, which supplement those measures/actions enumerated for each FPCON .
 - Installation commander will have a formally documented RAMP under the supervision of the AT officer.
 - Commanders will ensure that RAMP is conducted as an integral part of all AT programs. RAMP is particularly important for our installations due to the static nature of our forces and missions often result in the establishment of identifiable routines.
 - RAMP will test implementation of all FPCON measures on at least an annual basis.

(continued on next page)

**Critical task 5:
Maintain
installation
defenses in
accordance
(FPCON)
protection
conditions
with force
(continued)**

- All commanders will utilize the concept of RAMP in providing AT for their unit. Below installation level; however, the program requires no formal documentation.
- AT officers will coordinate with a physical security specialist to ensure the AT threat is considered in the application of overall physical security measures.
- Commanders will develop a prioritized list of AT factors for site selection teams. These criteria will be used to determine if facilities under consideration for occupancy can adequately protect occupants against threat attack. Commander will develop lists targeted to address the appropriate level threat and vulnerability assessment and based on guidance contained in DOD 0-2000.12-H.

4f

**Critical task 6:
Establish civil/
military
partnership
for weapons
of mass
destruction
(WMD) crisis**

- Army standard 6: Commanders will coordinate with local civilian communities to establish working relationships to formulate partnerships to combat and defend against terrorism.
- Implementing guidance.
 - Commanders will ensure AT plans are coordinated with local community officials to ensure a complete understanding of how and what military or civilian support will be rendered in the event of a WMD crisis.
 - In the event of a terrorist incident involving WMD, commanders and civilian authorities will discover that the effects of these events test and in many cases, overwhelm internal assets immediately. It is imperative that commanders attempt to establish memoranda of understandings and/or memoranda of agreements with the local authorities to foster relationships that facilitate the shared use of critical resources.
 - Commanders will ensure that any support provided to civilian law enforcement agencies complies with AR 500–51.

4g

Critical task 7: Terrorist threat/incident response training Army standard 7: Commanders and Directorates will develop reactive plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents.

- Implementing guidance.
 - Reactive 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.
 - Installation commander will identify HRT 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.
 - In significant and high terrorist threat level areas, plans to respond to terrorist incidents will contain current residential location information for all DA personnel and their dependents.
 - Commanders will develop procedures to ensure periodic review, update, and coordination of reactive plans with appropriate responders.
 - Commanders will ensure medical, fire, and police response procedures are integrated into consequence management/AT plans.
 - Plans will develop an attack warning system using a set of recognizable alarms and reactions for potential emergencies, as determined by the threat and vulnerability assessment. 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.

4h

-
- Critical task 8: Conduct exercises and evaluate/assess antiterrorism plans**
- Army standard 8: 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.
- Implementing guidance.
 - Installation commander will conduct an AT exercise at least annually and maintain a written record until no longer needed. The purpose of the exercise program is to validate the AT plan, identify weaknesses, synchronize the AT plan with other related crisis action/consequence management plans, and develop corrective actions. At installation level, the exercise will contain and test areas such as the following:
 - Implementation of FPCON levels.
 - Implementation of individual FPCON measures.
 - Terrorist use of WMD.
 - Initial response and consequence management capabilities.
 - Threat attacks on Army information systems.
 - Use and evaluation of attack warning systems.
 - Medical mass casualty scenarios.

Appendix A
References

Section I. Required Publications

This section not used.

Section II. Related Publications

AR 190-16

Physical Security

AR 190-58

Personal Security

AR 500-51

Individual Augmentation Management

AR 525-13

Antiterrorism

DOD 2000.12-H

DOD Antiterrorism Handbook

DOD Instruction 2006.16

DOD Antiterrorism Standards

Section III. Prescribed Forms

This section not used.

Section IV. Referenced Forms

DA Form 2028

Recommended Changes to Publications and Blank Forms

FH Form 1853

Distribution Scheme

Glossary

Section I. Abbreviations

AOR

Area of Responsibility

APOE

Area Port of Embarkation

AR

Army Regulation

AT

Antiterrorism

ATO

Antiterrorism Officer

ATWG

Antiterrorism Working Group

C2

Command and Control

CBRNE

Chemical, Biological, Radiological, Nuclear, or High Yield Explosives

CT

Counter Terrorism

DA

Department of the Army

DES

Directorate of Emergency Services

DHR

Directorate of Human Resources

DOD

Department of Defense

DODI

Department of Defense Instruction

DPTMS

Directorate of Plans, Training, Mobilization, and Security

DTRA

Defense Threat Reduction Agency

FBI

Federal Bureau of Investigation

FH

Fort Hood

FORSCOM

Forces Command

FP

Force Protection

FPCON

Force Protection Conditions

HQDA

Headquarters, Department of the Army

HRP

High-Risk Personnel

HRT

High-Risk Target

IAW

In Accordance With

IMA

Installation Management Agency

IOC

Installation Operation Center

IVA

Integrated Vulnerability Assessment

JSIVA

Joint Service Integrated Vulnerability Assessment

LVA

Local Vulnerability Assessment

MSC

Major Subordinate Command

O-5

Lieutenant Colonel

O-6

Colonel

O-8

Major General

OCONUS

Outside the Continental United States

OPSEC

Operations Security

PAO

Public Affairs Officer

PCC

Pre-Command Course

PIR

Priority Incident Report

POE

Port of Embarkation

RAMP

Random Antiterrorism Measures Program

RC

Reserve Component

TA

Threat Assessment

TRADOC

Training Doctrine

TWG

Threat Working Group

US

United States

VA

Vulnerability Assessment

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 forces. The AT program is one of several security-related programs that fall under the overarching force protection and combating terrorism programs. An AT program is a collective effort that seeks to reduce the likelihood that Department of Defense affiliated personnel, their families, facilities, and materiel will be subject to a terrorist attack and to prepare to respond to the consequences of such attacks should they occur.

Antiterrorism awareness

Fundamental knowledge of the threat and measures to reduce vulnerability to threat attacks.

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 or unacceptable counteraction.

DOD components

The office of the Secretary of Defense; 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; and the defense agencies.

Family member

“Dependent” as defined 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).

First responders

The first units, usually military police, fire, and/or emergency medical personnel, to arrive on the scene of a threat incident.

Force protection

Security program to protect soldiers, civilian employees, family members, information, equipment, and facilities in all locations and situations. This is accomplished through the planned integration of combating terrorism, physical security, information operations, high-risk personnel security, and law enforcement operations; all supported by foreign intelligence, counterintelligence, and other security programs.

Force protection condition

Terrorist FPCON is a DOD approved system standardizing the military services' identification of and recommended preventive actions and responses to terrorist threats against US personnel and facilities. This system is the principle means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-service coordination and support for antiterrorism activities.

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 considered being at risk as potential terrorist targets because of mission sensitivity, ease of access, isolation, symbolic value, and/or potential for mass casualty.

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.

Installation

A grouping of facilities, located in the same vicinity, that support particular functions.

Installation commander

The senior commander on the installation, camp, post, or other places formally identified as a location where one unit works or leaves.

Intelligence

The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Community agencies and provides users with tailored intelligence support.

Major Subordinate Command

Division unit assigned to a major command.

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.

Operations security

Operations security is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- a. Identify those actions that can be observed by adversary intelligence systems.
- b. 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.
- c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Physical protective measures

Physical security measures used to counter risk factors that usually do not change over a period of time such as mission impact, cost, volume, and criticality of resources and vulnerabilities. The measures are usually permanent and involve the expenditure of funds.

Physical security

That part of the Army security system employing physical and procedural security measures to detect, deter, and defend personnel, property, equipment, facilities, material, and information against espionage, terrorism, sabotage, damage, misuse, theft, and other criminal acts.

Random Antiterrorism Measures Program

A security program that involves implementing multiple security measures in a random fashion to change the appearance of an installations/activities security program.

Security

Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. A condition that results from the establishment and maintenance of protective measures that ensures a state of inviolability from hostile acts or influences. With respect to classified matter, the condition prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.

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. Those acts are usually planned to attract widespread

publicity and are designed to focus attention on the existence, cause, or demands of the terrorists.

Terrorist

An individual who uses violence, terror, and intimidation to achieve a result.

Terrorist groups

Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its 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 the presence of a terrorist group, operational capability, activity, intentions, and operating environment.

Threat assessment

The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat. Also, it is the product of a threat analysis for a particular unit, installation, or activity.

Threat Assessment Plan

The process used to conduct a threat analysis and develop a threat assessment.

Threat statement

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

Vulnerability

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. 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.

Vulnerability assessment

The process through which the commander determines the susceptibility to attack and the board range of physical threats to the security of personnel and facilities, which provides a basis for determining antiterrorism measures that can protect personnel and assets from terrorist attacks.

Weapons of mass destruction

Any weapons or devices that are intended or have the capability of a high order of destruction and/or being used in such a manner as to destroy large numbers of people. It can be CBRNE weapons, but excludes the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon. In AT,

27 APRIL 2006

III CORPS & FH REG 525-6

this includes the use of very large improvised explosive devices and environmental sabotage, which is capable of destruction at the same magnitude.