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 (DAMO–ODL), Office of the Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington, DC 20310–0400.

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

Headquarters
Department of the Army
Washington, DC
4 January 2002

UNCLASSIFIED

SUMMARY of CHANGE

AR 525–13
Antiterrorism

Specifically, this revision--

- Changes the name of AR 525-13 from “Antiterrorism Force Protection: Security of Personnel, Information, and Critical Resources” to “Antiterrorism.”

- Separates the terms Antiterrorism/Force Protection for the purpose of eliminating confusion between the two programs.

- Establishes minimum military and civilian grades for major Army command, installation, and unit antiterrorism officers (paras 2-24, 2-25, and 4-2*b*(8)).

- Establishes the Army Antiterrorism Program (chap 3).

- Refines mandatory Army antiterrorism standards to integrate and synchronize antiterrorism elements into the broader security program called Force Protection (chap 4).

- Provides a framework for standards identified as critical tasks that support the Department of Defense’s Force Protection Objectives as outlined in DOD Directive 2000.12 and DOD Instruction 2000.16 (chap 4).

- Implements revised DOD antiterrorism standards resulting from the findings and recommendations of the U.S.S. Cole Commission Report (chap 4).

- Establishes the Antiterrorism Operational Assessment Program (para 4-9*b*(2)).

- Provides a Management Control Evaluation Checklist to assist commanders in evaluating their AT Program (app C).

- Provides training requirements for all military, Department of the Army civilians, Department of Defense contractors, and family members (app F).

Headquarters
Department of the Army
Washington, DC
4 January 2002

*Army Regulation 525–13

Effective 4 February 2002

Military Operations

Antiterrorism

By Order of the Secretary of the Army:

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army

History. This printing publishes a revision of this publication. Because the publication has been extensively revised, the changed portions have not been highlighted.

Summary. This regulation prescribes policy and procedures and assigns responsibilities for the Army Antiterrorism (AT) Program. This program implements DOD Directive 2000.12 and DOD Instruction 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 of the United States (ARNGUS), and the U.S. Army Reserve (USAR) as well as Army owned and managed installations, facilities, and civil works projects. This regulation applies during partial and full mobilization.

Proponent and exception authority. The proponent of this regulation is the Deputy Chief of Staff for Operations and Plans (DCSOPS, DAMO–ODL). The DCSOPS has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. The DCSOPS may delegate this approval authority, in writing, to a division chief within the proponent agency in the grade of colonel or the civilian equivalent.

Army management control process. This regulation contains management control provisions in accordance with AR 11–2 and identifies key management controls that must be evaluated.

Supplementation. Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from Headquarters, Department of the Army (HQDA) (DAMO–ODL), Office of the Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington, DC 20310–0400.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to HQDA (DAMO–ODL), Office of the Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington, DC 20310–0400 or e-mail to ATO@hqda-aoc.army.pentagon.mil.

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 of the United States (ARNG), and the U.S. Army Reserve (USAR). 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 (DAMO-ODL), Office of the Deputy Chief of Staff for Operations and Plans, 400 Army Pentagon, Washington, DC 20310–0400 or e-mail to ATO@hqda-aoc.army.pentagon.mil.

*This regulation supersedes AR 525–13, dated 10 September 1998.

Contents (Listed by paragraph and page number)

Contents—Continued

Appendixes

Glossary

Index

Chapter 1
Introduction and Policies

1–1. Purpose
This regulation establishes the Army Antiterrorism (AT) Program to protect personnel (soldiers, Department of the Army (DA) civilian employees, Department of Defense (DOD) contractors and family members of DOD employees), information, materiel, and facilities in all locations and situations against terrorism. It provides—

a. Department of the Army AT standards.

b. Implementing guidance for the execution of the AT standards.

c. 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 10 U.S.C. 3013.

Chapter 2
Responsibilities

2–1. Administrative Assistant to the Secretary of the Army
The Administrative Assistant to the Secretary of the Army (SAAA) will designate high-risk personnel (HRP) within Headquarters, Department of the Army (HQDA) in accordance with AR 190–58.

2–2. Special Assistant for Military Support, Office of the Secretary of the Army
The Special Assistant for Military Support, Office of the Secretary of the Army will provide oversight of AT policy.

2–3. 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 AT funds in accordance with annual guidance from the Undersecretary of Defense (Comptroller).

2–4. Director of Information Systems for Command, Control, Communications, and Computers.
The Director of Information Systems for Command, Control, Communications, and Computers (DISC4) will—

a. Serve as the Army focal point for the management of the Army Information System Security (ISS) Program and relevant components of the Army Command and Control (C2) Protect Program.

b. Implement measures, both procedural and material, to protect the Army's C2 systems.

c. Consolidate relevant C2 Protect AT inputs and provide to the ODCSOPS in support of Information Operations (IO) policy.

d. Develop and publish C2 Protect ISS standards.

e. Provide C2 Protect direction, procedures, and guidance to all Army support organizations.

2–5. The Inspector General
The Inspector General (IG) will—

a. Ensure AT is integrated as an area of special interest for major Army command (MACOM) and installation level inspection.

b. Ensure that AT policies and programs are present and current, receive emphasis, and are integrated into overall force protection (FP) planning and execution.

2–6. Chief, Public Affairs
The Chief, Public Affairs (CPA) will provide guidance to MACOMs for the development and execution of command information and public information programs in support of AT efforts.

2–7. Assistant Chief of Staff for Installation Management

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

a. Develop construction policies for incorporating physical security design measures into military construction (MILCON) projects and modifications to existing facilities in support of the Army's AT Program.

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

2–8. Deputy Chief of Staff for Personnel

The Deputy Chief of Staff for Personnel (DCSPER) 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 AT awareness training.

b. Establish procedures to ensure Army personnel who will be designated as HRP in accordance with AR 190–58 are programmed to attend the Individual Terrorism Awareness Course (INTAC) prior to reporting to such positions.

c. Establish procedures to identify those key positions at the MACOM and installation level that require formal or refresher AT training (including risk management) prior to assumption of duties and ensure assignment orders delineate special instructions for training in accordance with DODI 2000.16 prior to assignment to the gaining command.

2–9. Deputy Chief of Staff for Operations and Plans

The Deputy Chief of Staff for Operations and Plans (DCSOPS) is responsible for the security of the Army and provides overall policy guidance and staff supervision and coordination for the Army AT Program. In discharging overall general staff responsibility for the Army AT Program, the DCSOPS will—

a. Ensure that the Chief, Security, Force Protection, and Law Enforcement Division (DAMO–ODL) will—

(1) Serve as the functional proponent for AT and remain in close coordination with the Office of the Secretary of Defense (OSD), the Joint Chiefs of Staff (JCS), the other Services, Defense agencies, MACOMs, and vulnerability assessment visits conducted by higher headquarters.

(2) Establish Army AT policy and objectives, coordinate and evaluate policies and procedures consistent with Department of Defense (DOD) Directives, and provide resources.

(3) Integrate and synchronize all AT elements and enablers with the assistance of proponent HQDA staff sections, functional MACOMs, and other intelligence, security and law enforcement agencies, as appropriate.

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

(5) Validate resource requirements for staffing and administering Army AT Program functions.

(6) Establish policy governing 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 to ensure allocation of school quotas supports AT operational requirements.

(9) Publish DA AT travel advisories, as required, to inform commanders of DOD-designated high physical threat and potential security threat countries, high crime rate cities, and DOS travel advisories.

(10) Maintain a master file of all personnel designated HRP Level I and II by the SAAA and commanders of MACOMs and provides changes to Commander, U.S. Army Criminal Investigation Command as they occur.

(11) Assess the terrorist and other criminal threats to U.S. Army forces and publish an annual comprehensive DA threat statement and daily DA force protection memorandum, to disseminate potential and future threats, thereby enhancing threat awareness at all levels.

b. Operate an Antiterrorism Operations Intelligence Cell (ATOIC) in close coordination with the Office of the Deputy Chief of Staff for Intelligence (ODCSINT) and the U.S. Army Criminal Investigation Command (USACIDC) in the Army Operations Center (AOC). The ATOIC will monitor and report worldwide force protection conditions (FPCONs) and coordinate the analysis and reporting of terrorist-related intelligence with the appropriate intelligence and law enforcement agencies in order to provide warning and maintain visibility of threats to MACOMs, the senior Army leadership, and threatened installations, activities, facilities, and personnel. The ATOIC will fuse foreign terrorist intelligence and domestic threat information to form a single threat picture for commands assigned to the continental United States.

c. Establish an AT Steering Committee Board of Directors in accordance with paragraph 4–2.

d. Assess the posture of the Army AT Program at MACOM and installation level.

e. Identify and code all MACOM and installation antiterrorism officer (ATO) positions to require formal or refresher AT training (including risk management) prior to assumption of duties and ensure assignment orders delineate special instructions for training in accordance with DODI 2000.16 prior to assignment to the gaining command.

2–10. Deputy Chief of Staff for Intelligence

The Deputy Chief of Staff for Intelligence (DCSINT) will—

a. Develop policy and procedures, and ensure resourcing, for collecting, reporting, disseminating, and producing intelligence concerning international terrorism and only that information on U.S. persons authorized by military intelligence jurisdiction.

b. In coordination with the U.S. Army Intelligence and Security Command (INSCOM) and ODCSOPS provide intelligence personnel to support operation of the ATOIC.

c. Provide Army intelligence requirements related to international terrorism to the National Foreign Intelligence Board.

d. Represent the Army in matters related to international terrorism in the intelligence community.

e. In coordination with INSCOM, provide technical personnel support to the Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS) designated assessment teams, as required.

2–11. The Surgeon General

The Surgeon General (TSG) will consider the use of weapons of mass destruction by terrorists when establishing policy and procedures for casualty treatment and preventive medicine procedures.

2–12. 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 called to active duty 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 condition 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 D.

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 establishment of state AT committees and AT working groups and appointment of state command AT officers, in accordance with paragraph 4–2.

2–13. 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 all USAR soldiers called to active duty receive required AT awareness training prior to deployment OCONUS.

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

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

f. Ensure procedures are established for reporting FPCON changes implemented by USAR units, facilities, and activities to the ATOIC.

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

h. Ensure procedures are established for submission of required reports in accordance with appendix D.

2–14. Commanding General, U.S. Army Training and Doctrine Command

The Commanding General, U.S. Army Training and Doctrine Command (CG, TRADOC) will—

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

(1) An orientation for cadets, officer candidates, and 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.

(2) Integration of AT and risk management training into all officer and NCO professional military education to ensure the long-term development of knowledge and skills. Training will include educating leaders on physical security technology.

(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 threat attacks.

(4) Develop AT training requirements in accordance with paragraph 4–5 and appendix F.

(5) Develop collective training to integrate U.S. Army forces AT operations with host nation (HN)/joint elements.

b. Staff and resource the Army specified proponent for AT doctrine and training in accordance with AR 5–22 to coordinate programs within TRADOC and with the U.S Army Special Operations Command (USASOC) and HQDA.

c. Assist USASOC in the development of doctrine and training supporting execution of AT operations unique to Army Special Operations Forces (ARSOF).

d. Develop AT doctrine, tactics, techniques, and procedures.

e. 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).

f. Ensure all personnel attending resident schooling receive required antiterrorism awareness training in accordance with paragraph 4–5 and appendix F prior to departure to gaining command.

2–15. CG, U.S. Army Corps of Engineers

The CG, 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 and recommend security-engineering techniques to deter or reduce the impact of threat attacks on both permanent facilities and deployed forces.

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

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

e. Assist, as requested, MACOM and installation commanders in conducting vulnerability assessments.

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

g. Ensure USACE engineers have incorporated AT measures for all new construction and modifications to existing structures and facilities, in coordination with appropriate Staff/Commander In Chief (CINC), considering local threat and vulnerability assessments.

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

i. In coordination with CG, TRADOC, recommend training of engineer assets for responding to threat incidents requiring engineering assets in rescue efforts.

j. Provide technical personnel support to ODCSOPS designated assessment teams.

2–16. CG, U.S. Army Special Operations Command

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

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

b. Conduct resident Individual Terrorism Awareness Course (INTAC) for DOD personnel designated as HRP.

c. Conduct resident AT Instructor Qualification Course (AIQC) to prepare officers, noncommissioned officers and equivalent grade civilian employees to train individuals and units in individual terrorism awareness.

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

e. Serve as the training proponent for antiterrorism individual protective measures and hostage survival.

2–17. CG, U.S. Army Criminal Investigation Command

The CG, 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, host nation (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 agencies and host country agencies to exchange criminal intelligence.

h. Ensure that those personal security vulnerability assessments (PSVAs) conducted in support of HRP security programs consider potential attacks by terrorists.

i. 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.

j. Immediately notify the affected installation PM/SO and HQDA (in accordance with appendix D) upon receipt of time-sensitive threat information.

k. Conduct domestic criminal intelligence collection efforts and disseminate information on domestic criminal threats against the Army.

l. Implement criminal investigative measures, crime prevention efforts and criminal investigations to protect the Army's C2 systems, and to respond to criminal attacks and intrusions.

m. Consolidate relevant C2 Protect AT inputs and provide to the ODCSOPS in support of information operations (IO) policy.

n. In coordination with the Land Information Warfare Activity (LIWA), assess specific and general Army C2 vulnerabilities open to criminal activity, and recommend corrective actions to eliminate or mitigate them.

o. Perform criminal threat and vulnerability assessments for Army personnel, installations, systems, operations, and other interests as directed by HQDA and/or based on Army commanders' operational requirements.

p. Provide technical personnel support to ODCSOPS designated assessment teams, as required.

q. Investigate all incidents of suspected terrorism as criminal acts, to include the safeguarding of evidence, collection of testimony, 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.

r. In coordination with the ACERT and INSCOM, react to and assess Army computer security incidents (that is, unauthorized root use or access, denial of service, etc.) to determine if criminal acts were perpetrated, and investigate those related crimes as appropriate.

s. In conjunction with DISC4 and LIWA, conduct computer crime and information assurance vulnerability assessment, examining for early warnings and indications of terrorist and/or criminal activities involving Army or DOD information systems.

t. Provide liaison to the Joint Task Force-Computer Network Defense (JTF–CND) for law enforcement and criminal investigative matters involving attacks on Army information systems.

u. Provide domestic terrorism analysis and threat assessments to the ATOIC in support of Army requirements and the AT Program.

v. 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.

2–18. CG, U.S. Army Intelligence and Security Command

The CG, U.S. Army Intelligence and Security Command (INSCOM) will—

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

b. Maintain a capability to report and disseminate INSCOM-collected, time-sensitive information concerning the foreign 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. Include foreign threat information in briefings on subversion and espionage directed against the Army (SAEDA) in accordance with AR 381–12.

e. Unless provided by theater MACOM 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 threat information. Host country coordination should be in accordance with agreements between the Army Service Component Commander, or numbered Army Commander, and other U.S. agencies.

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

g. Immediately notify the affected installation PM/SO and HQDA (in accordance with appendix D) upon receipt of time-sensitive threat information.

2–19. CG, U.S. Army Military District of Washington

The CG, U.S. Army Military District of Washington (MDW) will coordinate AT issues and act as the focal point for the coordination and dissemination of AT information and FPCON coordination within the National Capital Region, in accordance with existing inter-Service agreements and memorandums of agreement with local civilian support agencies.

2–20. 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. Establish a state AT committee and AT working group and appoint a state command AT officer, in accordance with paragraph 4–2.

c. Comply with all FPCON reporting and implementation procedures. OCONUS Adjutants General will report changes in their FPCON to the MACOM 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 called to active duty receive required AT awareness training prior to deployment OCONUS and require individual/unit records be maintained documenting training.

g. Program/budget funds and identify state ARNG personnel for specialized AT training.

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

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

j. Submit required reports in accordance with appendix D.

k. Designate HRP in accordance with AR 190–58 and the following guidelines—

(1) State Adjutants General are authorized to designate personnel as Level I HRP. The Commander, Forces Command (FORSCOM), or the Commander, U.S. Army Pacific (USARPAC), as appropriate, will be provided written notice of such designations.

(2) The authority to designate Level II HRP rests with Adjutants General and cannot be further delegated.

l. Report personnel designated as HRP Levels I and II to HQDA in accordance with AR 190–58.

2–21. CG, U.S. Army Soldier and Biological Chemical Command

The CG, U.S. Army Soldier and Biological Chemical Command (SBCCOM) will—

a. Provide staff and over-watch support to the deployment and activities of the Technical Escort Unit.

b. Maintain an emergency response capability to respond to chemical/biological accidents/incidents worldwide, as required, to support DOD, Federal, state, and local agencies in accordance with applicable regulations and directives.

c. Monitor research, development, and technology programs of the Chemical Biological Rapid Response Team, Edgewood Chemical Biological Center, in support of emergency response forces and ensure complete integration of technology and responders.

d. Provide chemical/biological analysis and assessments in response to Army Staff and MACOM requirements.

e. Provide technical personnel support to ODCSOPS designated assessment teams, as required.

2–22. Director, Army Counterintelligence Center

The Director, Army Counterintelligence Center (ACIC) will—

a. Provide supported Army commanders with information concerning the 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 CG, USACE 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).

g. Publish a Monthly International Terrorism Summary (MITS), at the lowest classification level possible, which outlines the terrorist threat in DOD designated high and medium potential physical security threat countries.

2–23. Director, Land Information Warfare Activity

The Director, Land Information Warfare Activity (LIWA) will—

a. In coordination with USACIDC, assess specific or general Army C2 vulnerabilities open to adversary exploitation and attack.

b. Perform C2 risk management assessments based on Army commanders' operational requirements, in accordance with applicable policy.

c. Recommend courses of action to reduce or avoid adversary threat to Army or Army-associated information infrastructures.

d. Provide task-organized worldwide Army AT and other IO-related mission-specific assistance in contingency operations, planning, training, test, demonstration, experimentation, and exercise support.

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

f. Provide technical personnel support to ODCSOPS designated assessment teams, as required.

2–24. MACOM Commanders

a. For purposes of this regulation, MACOM requirements also apply to the U.S. Army Reserve Command, Numbered Army, and Army Service Component Commanders.

b. MACOM Commanders will—

(1) Incorporate AT into their overall Force Protection (FP) Program.

(2) Appoint an AT officer (minimum grade of O-4 or equivalent civilian grade) within operations or a staff organization that is best suited to execute the program (DCSOPS/G-3/etc.).

(3) Publish guidance to installations for execution of AT standards within the overarching FP security program.

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

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

(6) Coordinate with geographic MACOMs, as appropriate, to ensure subordinate units receive requisite support and oversight for those regulatory requirements the parent MACOM cannot execute.

(7) Implement and execute the Army AT standards in accordance with implementing guidance identified in chapter 4.

(8) Validate intelligence production and threat assessment support requests submitted by subordinate organizations.

(9) Establish a process to track movements through high threat areas for units of 30 personnel or more.

2–25. Installation commanders

a. For purposes of this regulation, installation commanders' requirements also apply to the U.S. Military Academy, the National Guard, and the U.S. Army Reserve facilities.

b. Installation commanders will—

(1) Incorporate AT into their overall FP program.

(2) Appoint an AT officer (minimum grade of O-3 or equivalent civilian grade) within operations or a location best suited to execute the program (DCSOPS/G—3/DPTMS/etc.).

(3) Publish guidance for the execution of AT standards within the overarching FP security program.

(4) Designate a focal point to coordinate requirements for, receive, and disseminate time-sensitive threat information received from Federal, state, local, HN, USACIDC, and U.S. intelligence agencies.

(5) Ensure all tenant 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.

(6) Implement and execute Army AT standards in accordance with implementing guidance identified in chapter 4.

2–26. Commanders of units, battalion-level and above

Commanders of units, battalion-level and above will—

a. Implement and execute Army AT standards in accordance with implementing guidance identified in chapter 4.

b. Ensure AT training is identified as a unit combat task and is an integral part of unit training plans, major training exercises/events, and a special interest item at training management reviews.

c. Corps, Division, and Brigade commanders will ensure that AT training is embedded throughout subordinate units' training plans and is performance oriented and measurable.

2–27. Commanders/Directors of U.S. Army tenant units/activities of U.S. Army installations

Commanders/Directors will—

a. 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 FPCON levels.

b. Comply with host installation AT requirements.

c. Provide personnel support as specified in host installation AT plans.

2–28. Commanders/Directors of stand-alone activities/facilities

a. For purposes of this regulation, these requirements also apply to Army organizations that are tenants of other Services, HQDA Staff sections, and U.S. Army Cadet Command, U.S. Army Recruiting Command, and U.S. Army Military Entrance Processing Command sites.

b. Commanders/Directors will—

(1) Forward a request to the next higher headquarters or supporting installation for support for Government-owned contractor operated facilities not able to support regulatory requirements.

(2) Implement and execute Army AT standards in accordance with implementing guidance identified in chapter 4.

Chapter 3
The Army AT Program

3–1. Overview

Antiterrorism is the Army's defensive program to protect against terrorism. The combination of AT, counterterrorism (CT), consequence management, and intelligence support constitute the overall Combating Terrorism (Cbt–T) Program. The AT Program centers on planning, training, exercising, awareness efforts, and the conduct of the Random Antiterrorist Measures Program (RAMP). AT planning coordinates specific AT security requirements into the efforts of supporting FP security programs (HRP, LE, PS, and IO).

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 a threat'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 weapons of mass destruction (WMD), composed primarily of chemical and biological 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 for dealing with 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 Lead Federal Agency (LFA) 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 LFA for investigating and apprehending terrorists in such incidents.

c. The Federal Aviation Administration (FAA) 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 FAA is responsible for communicating terrorist threat information to commercial air carriers and their passengers. DA will provide the FAA threat information within its operational area of interest, consistent with appropriate DOD and DA policies.

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

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

3–5. U.S. Army Antiterrorism Policy

In support of U.S. Government policy on terrorism, DA will implement the following policy:

a. Prevent threat incidents through implementation of appropriate protective and preventive measures. To meet this objective, DA will allocate resources necessary to—

(1) Sustain an intelligence capability to monitor and report on the activities, intentions, and capabilities of threat groups in accordance with applicable regulations and directives.

(2) Maintain comprehensive AT operations plans/orders and standing operating procedures (SOPs) which detail protective and preventive measures appropriate at each FPCON level (Normal-Delta).

(3) Ensure all personnel are trained to perform their AT responsibilities.

(4) Ensure all personnel are informed of the threat and of all appropriate security precautions designed to reduce their vulnerability to threat attacks prior to traveling outside the 50 United States, its territories, and possessions.

(5) Implement structural and procedural security measures, as required, to protect against the threat.

b. Respond quickly and effectively when a threat attack is detected. To that end, DA will—

(1) Employ trained local security forces to isolate and contain the threat.

(2) Employ trained first responders to isolate the effects of a terrorist incident.

(3) Notify appropriate civilian or host nation security and law enforcement agencies.

(4) Support execution of operations by civilian or host nation security or law enforcement agencies to neutralize the threat. In most cases these agencies will have primary jurisdiction over terrorist incidents occurring on Army installations. In those cases where civilian or host nation security or law enforcement agencies decline jurisdiction in a terrorist incident, execute operations to neutralize the threat using the minimum force required.

(5) Investigate and apprehend alleged perpetrators in accordance with the provisions of applicable law, and, where appropriate, monitor the investigation of local law enforcement agencies.

3–6. Risk management

a. Risk management allows commanders to assess and control the risks associated with any Army mission or operation. Commanders will integrate risk management in the planning, coordinating, and developing of AT plans, orders, and operations. Leaders at all levels must be aware of how to integrate risk management into troop leading procedures when conducting any mission or operation in accordance with FM 100–14. Effective integration of risk management will enable the leader to identify hazards, assess the initial risk of the hazards, 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.

b. Commanders will conduct risk assessments to integrate threat assessment 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. While conducting risk assessments, commanders will consider the factors of threat, asset criticality, and vulnerability of facilities, programs, and systems. Risk assessments will analyze the following four elements:

(1) The terrorist threat.

(2) The criticality of assets.

(3) The vulnerability of facilities, programs, and systems to terrorist threats.

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

3–7. Travel Security Policy

When official business requires travel to or through HQDA designated high or potential physical threat countries, DA personnel and family members will travel, whenever possible, by military air or U.S. Air Force Air Mobility Command (USAFAMC) charter. When such travel is not practicable, U.S. air carriers will be utilized to the maximum extent possible. DA personnel and family members may not use foreign flag carriers for official travel unless U.S. flag carriers are not reasonably available as defined in Joint Federal Travel Regulations (JFTR), para U3125C.

a. As a limited exception to the Joint Federal Travel Regulations (JFTR) and providing the commander determines that the security conditions in a designated high or potential physical threat country at the time of travel warrant use of foreign flag airlines or indirect routing, DA military and civilian personnel may use foreign flag airlines and/or indirect routings to avoid DOD-designated high physical or potential threat countries, and airports designated by the FAA as not meeting minimum security standards set by the International Civil Aviation Organization (ICAO).

(1) Approval based on security threats must be in writing on a case-by-case basis. A travel advisory notice issued by the FAA and the Department of State must support determination and approval of foreign air carrier use based on a threat against an U.S.-flag air carrier. Determination and approval of foreign air carrier use based on a threat against Government employees or other travelers must be supported by evidence of threat that forms the basis of the determination and approval (see JFTR, para U3125 C3j).

(2) Transportation officers who arrange travel by indirect routing or on a foreign flag carrier to avoid such areas should cite JFTR, para U3125 C, as the justification. The use of that citation must be documented in each case and attached to each travel voucher.

(3) Travelers hereby authorized to avoid specific areas must disembark at the nearest interchange from point of origin and continue their journey on U.S. flag carrier.

b. Blanket approval and reimbursement for the use of regular-fee passports are not authorized.

(1) The passport policy for DA personnel and family members traveling on official orders to and/or from non-high or non-potential physical threat countries remains unchanged. DA personnel will travel on no-fee official passports or on official orders with identification cards as required by the country visited.

(2) DA personnel and family members traveling via commercial airline on official orders to, through, and/or from high or potential physical threat countries or to/through airports designated by the FAA as not meeting minimum security standards established by the ICAO are authorized, but not required, to obtain and use the regular-fee passport for security reasons. Travelers electing to exercise this option are responsible for obtaining the regular-fee passport and all required visas. Reimbursement for passports and visas obtained under those conditions is authorized by the JFTR, and payment will be made on submission of appropriate documentation. Some countries have strict rules concerning the type of passport or visa required for entry. Information on the restrictions on use of regular-fee passports may be obtained from local personnel offices or transportation offices prior to travel.

(3) Individuals traveling solely by military air or USAFAMC charter will not be reimbursed for regular-fee passports unless U.S. Government transportation became available on short notice (that is, after commercial travel arrangements had been made and the passport purchased) or priority of travel was sufficiently high to require backup travel arrangements.

(4) Reimbursement for regular-fee passports for personal/unofficial travel is not authorized.

c. Commercial airline tickets will not be annotated to show an obvious affiliation of the traveler with the U.S. Government.

d. Travel itineraries of HRP (to include general officers or civilian equivalents) will be marked, at a minimum, "FOR OFFICIAL USE ONLY" and handled in accordance with command directives when travel takes them to or through DOD-designated high physical or potential threat countries. Such itineraries may be classified when warranted by the threat and authorized by appropriate classification authority guidelines. Security classifications should be assigned to extremely detailed itineraries (those that include exact dates, times, and locations), which would be of substantial value to threat entities planning an attack.

e. PCS/TDY travel orders will be annotated "Travel in civilian clothes authorized and recommended" for personnel traveling to and through DOD-designated high or potential security threat countries.

Chapter 4
Army AT Standards and Implementing Guidance

4–1. General

a. This chapter provides a critical task list framework that defines eight AT critical tasks commanders must implement to obtain DOD's 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).

b. All of the AT critical tasks are discussed below. The discussion of 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.

4–2. Critical task 1: Establish an Antiterrorism Program

a. 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.

b. Implementing guidance.

(1) All commanders are responsible for developing a full working knowledge of AT policies.

(2) Commanders will ensure that their AT Program is proactive and include the tenets of countersurveillance, counterintelligence, and other specialized skills as a matter of routine. To that end, commanders will incorporate proactive assets to detect and deter terrorists.

(3) 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 (MOA) clearly outlining AT responsibilities. Additionally, commanders will verify that 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.

(4) MACOM commanders will—

(a) Develop formal programs, documented in writing for proactive planning.

(b) Establish an AT Committee and Working Group that focuses on planning, coordinating, and executing the command's AT Program.

(c) Designate and have a person formally trained and certified as an AT Officer. AT officers will operate under the direction of the Chief of Staff or within a staff organization best suited to execute the program (DCSOPS).

(d) Provide supplemental guidance regarding policy and procedure when required.

(e) Ensure funding requirements are identified during Programmed Objective Memorandum (POM) budgetary cycles.

(5) Installation commanders will—

(a) Establish an AT Committee and Working Group that focus on planning, coordinating and executing the installation's AT Program.

(b) Designate and have a person formally trained and certified as an AT Officer. (AT officers will operate under the direction of the Chief of Staff, Garrison Commander, operations officer, or within a staff organization best suited to execute the program (DCSOPS, Director, Plans, Training, and Mobilization (DPTM), G3 or S3).

(c) 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. These plans will implement all applicable Army AT standards.

(d) 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.

(e) 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.

(f) 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 in accordance with applicable regulations and directives.

(6) State Adjutants General will issue operations plans, orders, or regulations that provide AT implementing guidance to subordinate organizations. The requirement to develop supporting plans or orders at subordinate levels will be addressed in the plan or order issued by the adjutant general.

(7) USARC will issue operations plans, orders, or regulations that provide AT implementing guidance to subordinate organizations. The requirement to develop supporting plans or orders at subordinate levels will be addressed in the plan or order issued by the USARC Commander.

(8) Commanders OCONUS will—

(a) Comply with applicable Status-of-Forces Agreement (SOFA) when planning and executing AT operations.

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

(c) Coordinate AT plans with the appropriate CINC and U.S. Embassy or Consulate. Provide copies of approved AT

plans to CINC in accordance with command policies and to the regional security officer (RSO), or other appropriate DOS officials.

(d) Where specific CINC and DA AT standards/requirements conflict to the detriment of the unit, the CINC AT standard/requirement will take precedence.

(9) Units down to battalion level will have a Level II trained AT officer (SFC or higher), who serves as the commander's planner/advisor on AT matters and serves as the instructor for Level I unit AT training.

(10) 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).

(11) At HQDA, The AT Steering Committee Board of Directors, chaired by the Deputy Director, DAMO-OD is the horizontal integrator for Army AT initiatives. This Board is composed of key functional staff elements and commands responsible for oversight of the Army AT Program. The Board's oversight responsibilities ensure requirements are identified, tracked, and completed. Additionally, the Board develops and allocates tasks based on the threat, assessments, intelligence, and JCS guidance.

4–3. Critical task 2: Collection, analysis, and dissemination of threat information

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

b. Implementing guidance.

(1) 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.

(2) 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 (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.

(3) MACOM commanders will incorporate terrorist threat into their annual MACOM FP threat assessment for use by subordinate units/installations in preparing their specific threat statements. A copy of the MACOM threat assessment will be forwarded to their subordinate elements and HQDA (DAMO–ODL). The results of threat assessments will be disseminated to all affected organizations (for example, organic, tenant, and supported RC units).

(4) Commanders will—

(a) 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. Determination of FPCON levels will be in accordance with appendix B. All commanders can set a local FPCON; subordinate commanders can raise but not lower a higher-level commander's FPCON.

(b) Ensure FPCON procedures contain provisions to notify all organic, tenant, and supported units, to include supported RC units.

(c) Implement the DOD Terrorist Threat Level classification system to identify the threat in a specific overseas country. CINCs with geographic responsibilities set terrorist threat levels for personnel, units, and installations within the AOR. Army commanders will use this threat analysis 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.

(d) Ensure the appropriate intelligence and law enforcement organizations within their command collect and analyze criminal threat information. Outside the U.S. some intelligence organizations may also collect and analyze foreign criminal elements.

(e) 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.

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

(g) Ensure the command uses the DOD Intelligence Production Program to validate and receive intelligence community support for international terrorism analysis and products to support their AT Programs that are beyond the capabilities of the intelligence organizations under their command.

(5) Because of the political and strategic implications of threat attacks on U.S. Army personnel and facilities, HQDA must be informed of threat attacks and updated periodically during the course of such incidents. Timely and accurate reporting serves two purposes: permits HQDA to provide appropriate support to threatened commands and permits DOD and HQDA, in conjunction with the local PAO, to provide consistent, accurate information to the public. Reports will be provided in accordance with appendix D.

(6) Additionally, commanders will ensure that—

(a) The first priority is to notify the affected installation/activity. Written procedures are established for disseminating time sensitive threat information during duty and non-duty hours and subordinate commanders, through company (or equivalent) level, have developed supporting procedures.

(b) All information pertaining to threat attacks involving DA personnel or assets in their AOR is forwarded throughout the chain of command or line of authority, as appropriate.

(7) Production and analysis requirements are focused and based on the commander's PIR/contingency plans to support the commander's ability to assess the risk when designating FPCON for operational planning.

(8) Threat information is coordinated with other staff elements involved in the AT Program through the AT committee working group.

(9) AT and threat information is distributed to relevant military and civilians.

(10) Threat information prepared by the intelligence community, USACIDC and PM/SO, technical information from information management, security and engineering planners, and information from other sources will be used when conducting threat assessments.

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

(12) Threat assessments will be part of leader's reconnaissance in conjunction with deployments. Follow-on threat and vulnerability assessments will be conducted for all deployments as determined by the commander, or directed by higher headquarters.

(13) Due to AR 381–10 restrictions on U.S. person information, consolidated (MI and criminal intelligence data) threat assessments cannot be filed, stored, or maintained as an intelligence product. These assessments must be filed, stored, and maintained within operational channels.

4–4. Critical task 3: Assess and reduce critical vulnerabilities (conduct AT assessments)

a. 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-deployment assessments.

b. Implementing guidance.

(1) 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 and CINC standards.

(2) MACOM commanders will review subordinate installation AT Programs for compliance with this regulation at a minimum of once every three years.

(3) Installation commanders will conduct a self-assessment of their AT Programs within 60 days of assumption of command and annually thereafter. This assessment will be conducted using the Management Control Evaluation Checklist at appendix C to ensure an Army-wide baseline. The incorporation of additional tasks are authorized. An assessment from a higher headquarters, that is HQDA, MACOM, JCS, or CINCs can be used to meet the self-assessment annual requirement.

(4) Installation commanders are also 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:

(a) Physical security.

(b) Engineering.

(c) Operations, training, and exercises.

(d) Military intelligence.

(e) Criminal intelligence.

(f) C2 Protect.

(g) Law enforcement.

(h) Threat options.

(i) OPSEC.

(j) Medical.

(k) Executive protection/high risk personnel.

(5) Special events such as Independence Day and Armed Forces Day Celebrations normally draw large crowds in open environments. As such, they may be more vulnerable and warrant special consideration. Antiterrorism 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.

(6) Installation commanders will prioritize, track, and report all vulnerabilities documented by installation and any higher headquarters vulnerability assessment to their MACOM headquarters within 60 days of the receipt of the

vulnerability assessment final report. MACOM headquarters will track all reported installation vulnerabilities to resolution/closure. Assessment results will be retained on file for no less than three years.

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

(8) Vulnerability assessments will be part of 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.

(9) 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 APOEs, POEs, GLOCs, base camps, support structures (contract and host nation), and local operating communities.

(10) 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.

4–5. Critical task 4: Increase antiterrorism awareness in every soldier, civilian, and family member

a. 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.

b. Implementing guidance.

(1) Within this standard are seven subordinate tasks as follows:

(a) Ensure AT training is an integral part of unit training plans, major training exercises/events, and a special interest item at training management reviews.

(b) Enhance the general awareness of terrorism issues (Command Information Program, PAO effort, etc.).

(c) Conduct annual AT awareness training.

(d) Ensure unit level AT officers are formally trained and certified.

(e) Provide senior level leadership with AT knowledge (Level IV AT training).

(f) In significant and high threat areas, ensure personnel receive training concerning hostage survival.

(g) 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.

(2) 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. Commanders also will develop an awareness program to ensure visibility of the AT Program and enhance awareness of all personnel. 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 policies outlined in subsequent paragraphs of this section. The PAO remains the sole spokesperson for the command until responsibility for AT is transferred to another Federal agency (for example, the FBI or DOS). 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.

(3) Commanders will ensure all military and DA civilians associated with their command receive annual antiterrorism awareness and receive an area of responsibility (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 area of responsibility (AOR) update prior to traveling OCONUS. Units will maintain a memorandum for record documenting an individual's training. Additionally, family members, age 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. AT awareness training will be in accordance with current TRADOC approved training requirements and lesson plans or the CJCS-approved, web-based AT Awareness Course (see app F).

(4) Formal AT training will be provided to individuals that perform duties as an AT officer at the unit/installation and standalone facilities levels. Commanders will identify those key positions that require formal or refresher AT training prior to assumption of duties. Requirements will be forwarded through MACOMs to ODCSPER who will ensure assignment orders clearly delineate special instructions for training prior to assignment to the gaining theater/command. For personnel not in transit, MACOM commanders will review and forecast training needs through established training channels. 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. Unit AT officers must be certified. As an exception, the first 0-6, or equivalent, in the chain of command is the lowest level authorized to designate individuals who have not attended formal training at the TRADOC approved school. Commanders can only certify those individuals who have received formal training in AT (for example, other DOD AT courses) or by virtue of previous assignments and experience, have extensive knowledge in AT.

(5) Battalion and brigade level commanders will receive AT training in the Army pre-command (PCC) training courses at Fort Leavenworth, KA. Instruction, using the TRADOC-developed PCC training support package, will

provide commanders with knowledge, skills, and abilities necessary to implement the Army AT. Additionally, all students will view the Secretary of Defense/Chairman Joint Chiefs of Staff AT video and receive instruction on understanding the use of force and rules of engagement. This training will include terrorist scenarios and hostile intent decisionmaking.

(6) 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. Target audience is 0-6 to 0-8 commanders/ personnel, nominated by MACOM commanders, who have responsibilities for AT policy, planning, and execution.

(7) Commanders will ensure DA personnel and dependents assigned to significant or higher threat locations are given guidance, at least annually, on appropriate conduct in the event they are taken hostage or kidnapped. Training can be accomplished via the commands information program and appropriate Army videotapes, distance learning, or during scheduled AT awareness training.

(8) Personnel who are at a higher risk to terrorist attack than the general population will receive additional training in accordance with the Army's High-Risk Personnel Security Program, see AR 190–58.

(9) Commanders will ensure AT training is included in mission rehearsals and pre-deployment training for all units (platoon level or above) prior to deployment to heightened threat areas. Multi-echelon individual training using vignettes and AT scenarios is required.

(10) Commanders will ensure units, which are deploying to or moving through high threat areas, conduct pre-deployment training that includes rules of engagement, AOR threat orientation, defensive TTPs/exercises, and the operation and use of security equipment.

4–6. Critical task 5: Maintain installation defenses in accordance with FPCON

a. 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.

b. Implementing guidance.

(1) Installation commanders will formally identify all installation high-risk targets (HRT) and use HRT as the focus for developing AT plans and implementing 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).

(2) Installation commanders will ensure that installation vehicle access procedures are implemented in accordance with AR 190–16.

(3) 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 HRP to make them eligible for special control/security measures. HRP will be identified and protected in accordance with AR 190–58.

(4) In significant or high terrorist threat level areas, commanders will ensure that all personnel (U.S. persons, host country nationals, or third country nationals), who are employed by contractor support agencies receive security/ background checks, in accordance with MACOM, CINC, and/or Embassy approved procedures, prior to being given unescorted access to U.S. installations, facilities, or equipment.

(5) OCONUS Commanders will ensure that the logistics contracting process will incorporate AT as a primary concern. AT considerations will be a part of every step of the contracting requirements, award, execution, and evaluation process. Commanders, in coordination with the cognizant county team, will ensure all logistics support contracts and agreements optimize force protection for the particular security environment and that future contract awards are contingent upon adequate AT performance.

(6) Installation commanders 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 as listed within appendix B.

(7) Installation commanders will have a formally documented Random Antiterrorism Measures Program (RAMP), under the supervision of the AT officer.

(8) 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.

(9) RAMP will test implementation of all FPCON measures on at least an annual basis.

(10) All commanders will utilize the concept of RAMP in providing AT for their unit. Below installation level, however, the program requires no formal documentation.

(11) AT officers will coordinate with a physical security specialist to ensure the AT threat is considered in the application of overall physical security measures.

(12) In significant or high terrorist threat level areas, commanders will conduct residential security assessments of off-post residences for permanently assigned and TDY personnel. Based on the assessment results, the individual may not be allowed to enter into a lease unless the facility owner takes certain measures. DA personnel not provided on-installation or other Government quarters will be furnished guidance on the selection of private residences to mitigate

risk of threat attack. Commanders will utilize the guidance contained in DOD 0-2000.12-H and supplement with local threat considerations, as appropriate. Commanders will complete residential security assessments as soon as personnel have identified and entered into contract negotiations for the lease or purchase of a residence. These assessments will use similar threat and vulnerability assessment criteria as that used to assess the safety and security of other facilities or installations housing Army personnel on installations within the AOR.

(13) 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. Commanders will develop lists targeted to address the appropriate level threat and vulnerability assessment and based on guidance contained in DOD 0-2000.12-H.

4–7. Critical task 6: Establish civil/military partnership for WMD crisis

a. Army standard 6. Commanders will coordinate with local civilian communities to establish working relationships to formulate partnerships to combat and defend against terrorism.

b. Implementing guidance.

(1) 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.

(2) 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 (MOUs) and/or Memoranda of Agreements (MOAs) with the local authorities to foster relationships that facilitate the shared use of critical resources.

(3) It is highly encouraged that commanders include local agencies, that is, police, FBI, fire and medical authorities in committee meetings and working groups to assist in the development and execution of AT plans.

(4) Commanders will ensure that any support provided to civilian law enforcement agencies complies with AR 500–51.

4–8. Critical task 7: Terrorist threat/incident response planning

a. Army standard 7. Commanders and heads of agencies/activities will develop reactive plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents.

b. Implementing guidance.

(1) 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. At the installation level, the plans must tie into other installation response plans.

(2) At installation level, commanders 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.

(3) 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. Such plans will provide for enhanced security measures and/or possible evacuation of DA personnel and their dependents.

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

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

(6) 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.

(7) CONUS commanders will—

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

(b) Take appropriate action to prevent loss of life and/or mitigate property damage before the FBI response force arrives. 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.

(8) OCONUS commanders will—

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

(b) Coordinate reactions to incidents of a political nature with the U.S. Embassy and the host nation, subject to instructions issued by the combatant command CINC with geographical responsibility.

(9) USACIDC will investigate threat incidents in accordance with paragraph 2–17*c*.

(10) AT plans, orders, SOPs, threat assessments, and coordination measures will consider the potential threat use of WMD. Commanders will assess the vulnerability of installations, facilities, and personnel within their area of responsibility (AOR) to terrorist use of WMD. Clear command, control, and communication lines will be established between local, state, Federal, and host nation 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 (that is accidental chemical spills) are sufficiently comprehensive.

4–9. Critical task 8. Conduct exercises and evaluate/assess AT plans

a. 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.

b. Implementing guidance.

(1) Installation commanders 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:

(a) Implementation of FPCON levels.

(b) Implementation of individual FPCON measures.

(c) Terrorist use of WMD.

(d) Initial response and consequence management capabilities.

(e) Threat attacks on Army information systems.

(f) Use and evaluation of attack warning systems.

(g) Medical mass casualty (MASCAL) scenarios.

(2) MACOM commanders will conduct AT operational assessments such that each of their installations is assessed once every two years or at least once during every Garrison Commander's tour of duty. To execute this action, MACOMs will develop AT operational assessment teams designed to test security procedures and installation defensive measures to protect from terrorist attack. AT operational assessments will include the following elements:

(a) Pre-operational phase: Test and evaluate installation procedures for detecting and reporting threats.

(b) Installation Defense phase: Test the installation's ability to implement FPCON BRAVO with security measures 1–28.

(c) After-action review phase: MACOMs will lead after-action reviews immediately following AT operational assessment exercises to identify installation shortcomings and provide recommendations and advice for procedural adjustments.

(d) The formal findings of these assessments will remain on file until the next exercise.

(e) AT operational assessments can be conducted in conjunction with other mandatory exercises (that is, EDRE, MASCAL, annual AT exercise, etc.) to maximize effort and conserve resources.

(3) WMD response measures and MASCAL scenarios may be sensitive to HN or local civil authorities. Commanders will coordinate, as appropriate, with local authorities prior to conducting such exercises if held in a location visible to the public.

(4) Where practicable, use of Joint, HN, local, state and/or Federal assets, as identified in the AT plan, will be considered for participation in these exercises.

(5) Commanders will incorporate AT planning into all major training exercises and CTC/BCTP exercises. Realistic AT scenarios will be included in these exercises. Exercises will include terrorist intelligence flow, unit protective measures, establishment of FPCON, and transitions to higher threat levels, reporting procedures, and incident response planning.

(6) Appropriate OPSEC measures will be taken to prevent disclosure of vulnerabilities during the planning, conduct, and evaluation of exercises.

Appendix A
References

Section I
Required Publications

AR 190–58
Personal Security. (Cited in paras 2–1, 2–8*b*, 2–20*k*, 4–5*b*(8), and 4–6.)

AR 360–1
The Army Public Affairs Program. (Cited in app E.)

AR 380–13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations. (Cited in para 4–3*b*(4)*(e)*.)

AR 381–10
U.S. Army Intelligence Activities. (Cited in paras 2–18*c*, 2–22*a*, and 4–3*b*(4)*(e)*.)

AR 381–12
Subversion and Espionage Directed Against the U.S. Army (SAEDA). (Cited in paras 2–18*d* and 4–3*b*(4)*(e)*.)

AR 500–51
Support to Civilian Law Enforcement. (Cited in para 4–7*b*(4).)

Section II
Related Publications
A related publication is merely 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 25–1
Army Information Management

AR 75–15
Responsibilities and Procedures for Explosive Ordnance Disposal

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 190–59
Chemical Agent Security Program

AR 195–2
Criminal Investigation Activities

AR 360–1
The Army Public Affairs Program

AR 380–5
Department of the Army Information Security Program

AR 380–19
Information Systems Security

AR 380–53
Information Systems Security Monitoring

AR 415–15
Army Military Construction Program Development and Execution

AR 530–1
Operations Security (OPSEC)

DA PAM 190–51
Risk Analysis for Army Property

DODD 2000.12
DOD Antiterrorism/Force Protection (AT/FP) Program (www.dtic.mil/whs/directives/)

DOD O–2000.12–H
Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence (www.dtic.mil/whs/directives/)

DODI 2000.16
DOD Antiterrorism Standards (www.dtic.mil/whs/directives/)

FM 3–19.1
Military Police Operations

FM 3–19.30
Physical Security

FM 19–10
Military Police Law and Order Operations

FM 19–20
Law Enforcement Investigations

FM 34–60
Counterintelligence

FM 100–6
Information Operations

FM 100–14
Risk Management (www.adtdl.army.mil/atdls.htm)

FM 100–25
Doctrine for Army Special Operations Forces

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
The following form is available on the Army Electronic Library (AEL) CD–ROM (EM 0001) and the USAPA Web site (www.usapa.army.mil):

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 DOD Directive 2000.12 and DOD Instruction 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 0-2000.12-H, 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.

a. There are five FPCONs:

(1) *FPCON NORMAL.* Applies when there is no discernible terrorist activity. Under these conditions, only a routine security posture, designed to defeat the routine criminal threat, is warranted. The minimum FPCON for U.S. Army commands is NORMAL.

(2) *FPCON ALPHA.* Applies when there is a general threat of possible threat activity against personnel and/or installations, the nature and extent of which is unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. Commands must be capable of maintaining FPCON ALPHA measures for extended periods, with only limited impact on normal operations.

(3) *FPCON BRAVO.* Applies when an increased or more predictable threat exists. Commanders must be capable of maintaining the measures of this FPCON for several weeks without causing undue hardship to personnel, substantially affecting operational capabilities, or aggravating relations with local authorities and members of the local civilian or host nation community.

(4) *FPCON CHARLIE.* Applies when an incident occurs or intelligence is received indicating imminent terrorist action. Implementation of FPCON CHARLIE measures for more than a short period probably will create hardships for personnel and affect the peacetime activities of units and personnel.

(5) *FPCON DELTA.* Applies when a terrorist attack has occurred, or intelligence indicates likely terrorist action against a specific location. Normally declared as a localized warning and requires implementation of mandatory security measures. Commanders are authorized and encouraged to supplement these measures. Implementation of FPCON DELTA cannot be sustained by commands for extended periods without causing significant hardships for personnel and affect the peacetime activities of units and personnel.

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 RAMP. 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

No credible threat of terrorist activity. Routine security measures are implemented with an installation physical security plan and in accordance with AR 190–13, The Army Physical Security Program, and are designed to defeat the spectrum of criminal threat.

B–3. FPCON ALPHA

The following measures will be implemented—

a. Measure 1. At regular intervals, 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 other activity considered suspicious.

b. Measure 2. 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).

c. Measure 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 4. Increase unannounced security spot checks (inspection of personal identification; vehicle registration; and the contents of vehicles, suitcases, briefcases and other containers) at access control points for U.S. installations and facilities.

e. Measure 5. Reduce the number of access points for vehicles and personnel to minimum levels, consistent with the requirement to maintain a reasonable flow of traffic.

f. Measure 6. As a deterrent, randomly apply measures 14, 15, 17, or 18 from B–4, FPCON BRAVO, either individually or in combination with each other.

g. Measure 7. Review all operations plans and orders and SOPs, which pertain to implementation of FPCONS BRAVO through DELTA.

h. Measure 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 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 10. Spare for MACOM or installation use.

B–4. FPCON BRAVO

In addition to the measures required by FPCON ALPHA, the following measures will be implemented—

a. Measure 11. Increase the frequency of warnings required by Measure 1 and inform personnel of additional threat information, as appropriate.

b. Measure 12. Keep all personnel involved in implementing AT contingency plans on-call.

c. Measure 13. Review provisions of all operations plans and orders and SOPs associated with implementation of FPCON CHARLIE.

d. Measure 14. Move automobiles and objects such as trash containers and crates away from HRT and mission essential/vulnerable areas (MEVAs) to a distance based upon countering the assessed threat. 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, etc.).

e. Measure 15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

f. Measure 16. At the beginning and end of each workday and at frequent 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.

g. Measure 17. 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.

h. Measure 18. Inspect all deliveries to messes, exchanges, guesthouses, clubs, libraries, schools, and other locally designated common use facilities to identify explosive and incendiary devices. Use trained EDD teams for some inspections, when available. Encourage family members to report suspicious packages to local law enforcement agencies, and refrain from handling them until cleared by appropriate authority.

i. Measure 19. Increase both overt and covert security force surveillance of messes, commissaries, exchanges, guesthouses, clubs, libraries, schools, chapels, and high-risk targets (HRTs) to improve deterrence and build confidence among staff and family members.

j. Measure 20. Inform soldiers, civilian employees, and family members of the general threat situation to stop rumors and prevent unnecessary alarm. Periodically update all personnel as the situation changes.

k. Measure 21. Brief representatives of all units and activities on the installation concerning the threat and security measures implemented in response to the threat. Implement procedures to provide periodic updates for these unit and activity representatives.

l. Measure 22. Verify the identity of all personnel entering the installation, 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. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of inspections of suitcases, briefcases, and other containers.

m. Measure 23. Increase the frequency of random identity checks (inspection of identification cards, security badges, and vehicle registration documents) conducted by security force patrols on the installation.

n. Measure 24. Increase security provided to off-post personnel in conjunction with host nation law enforcement agencies, where required and/or practicable, or transport off-post personnel to protected areas in accordance with local contingency plans. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.

o. Measure 25. 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.

p. Measure 26. 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 27. 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 on their operations in the local community.

r. Measure 28. est attack warning system and supporting evacuation plans, ensuring proficiency and appropriate OPSEC.

s. Measure 29. Spare for MACOM or installation use.

B–5. FPCON CHARLIE

The following measures will be implemented—

a. Measure 30. Continue all FPCONS ALPHA and BRAVO measures or introduce those, which have not already been implemented.

b. Measure 31. Keep all personnel responsible for implementing AT plans at their place of duty.

c. Measure 32. Reduce installation and HRT access points to the absolute minimum necessary for continued operation.

d. Measure 33. Verify the identity of all personnel entering U.S. installations, facilities, and activities (to include housing areas, schools and other facilities that are not located on installations). Inspect identification cards, security badges, or other forms of personal identification. Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of inspections of suitcases, briefcases, and other containers.

e. Measure 34. Remove all vehicles parked within or near MEVAs and HRTs specified in local plans to a distance based upon countering the assessed threat. Implement centralized parking and shuttle bus service, where required.

f. Measure 35. Issue weapons to all law enforcement personnel, security guards, and guard force augmentation personnel, if not already accomplished. Ensure that all personnel have been briefed concerning policies governing the use of force/rules of engagement, particularly criteria for use of deadly force. Ensure that ammunition is available for immediate issue (for those personnel not already issued ammunition) and that supervisory personnel are familiar with policies governing issuance of ammunition.

g. Measure 36. Increase security patrol activity to the maximum level sustainable. Weight the effort toward HRTs.

h. Measure 37. Position guard force personnel in the vicinity of all HRTs and MEVAs. In OCONUS areas where permitted by the host nation, position additional security personnel in the vicinity of otherwise unprotected housing areas, schools, hospitals, and other soft targets. Request additional security augmentation from host nation law enforcement and security agencies, particularly in otherwise unprotected areas.

i. Measure 38. Erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.

j. Measure 39. Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attacks.

k. Measure 40. Spare for MACOM or installation use.

B–6. FPCON DELTA

The following measures will be implemented—

a. Measure 41. Continue all FPCONS ALPHA, BRAVO and CHARLIE measures, or introduce those that have not already been implemented.

b. Measure 42. Augment guard forces to ensure absolute control over access to the installation, MEVAs, and HRTs.

c. Measure 43. 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.

d. Measure 44. 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.

e. Measure 45. Limit access to installations, facilities, and activities to those personnel with a legitimate and verifiable need to enter.

f. Measure 46. Inspect all baggage, such as suitcases, packages, and briefcases brought on the installation for presence of explosive or incendiary devices, or other dangerous items.

g. Measure 47. Take measures to control access to all areas under the jurisdiction of the U.S. command or agency.

h. Measure 48. 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 and MEVAs.

i. Measure 49. Cancel or delay all administrative movement that is not mission essential.

j. Measure 50. 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.

k. Measure 51. Spare for MACOM or installation use.

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 shall 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 host nation/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 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. Formal, specific terrorism warnings are issued separately by DIA, the Services, or the combatant commanders.

(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 (FIS)); 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 is the Director of Diplomatic Security.

(4) All commanders shall 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
Management Control Evaluation Checklist

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

C–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.

C–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 4–4. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2–R (Management Control Evaluation Certification Statement).

C–4. Questions
a. Critical task 1, Army standard 1: Establish an Antiterrorism Program.

(1) Has a formal AT Program been established in writing at installation/MACOM level?

(2) Has the MACOM/State AG/USARC published implementing guidance such as a supplement to AR 525–13 or an operations order outlining MACOM/State AG/USARC unique security requirements?

(3) Has an AT officer been designated within operational channels or an organizational staff best suited to execute the AT Program (MACOM/installation level)?

(4) Are AT funding requirements documented and tracked?

(5) Are plans coordinated with local, state, Federal, host nation, and other military security program plans as appropriate?

(6) Was the AT Program based in part on both threat and vulnerability assessments? (Also see related questions in standards 2 and 3.)

(7) Is an AT committee organized and functioning?

(8) Are AT working groups organized and functioning?

b. Critical task 2, Army standard 2: Collection, analysis, and dissemination of threat information.

(1) Is a system in place to determine and disseminate the terrorist threat?

(2) Is the terrorist threat integrated into the overall FP threat?

(3) Is threat information being coordinated with other staff elements involved in the AT Program?

(4) Are procedures in place to disseminate threat information and intelligence products to higher/subordinate activities and tenant organizations (during duty and non-duty hours)?

(5) Is the “no double standard policy” (threat information distributed to military, civilian, and contractor workforce) followed/understood when disseminating threat information?

(6) Are military intelligence collection operations being conducted consistent with the requirements of AR 381–10 and other applicable regulations and directives?

(7) Are law enforcement collection operations being conducted consistent with the requirements of AR 380–13, DODD 5200.27, and other applicable regulations and directives?

(8) For CONUS commanders, is this full integration conducted outside the intelligence office in accordance with the limitations of AR 381–10 and other applicable regulations and directives?

(9) Does the command have connectivity to receive threat-related information from all available sources (for example, ATOIC, FBI, CID, local law enforcement, Intelink-S, and Intelink)?

(10) Is the activity familiar with the DOD Intelligence Production Program and does it know how to obtain intelligence products?

(11) Is the activity receiving the MITS?

(12) Has the commander established PIR?

(13) Are the commander’s PIR the basis for production requirements?

(14) Are there sufficient sensitive compartmented information (SCI) billets to support the mission?

(15) Is the DOD Terrorist Threat Level Classification system utilized to identify the threat in a specific overseas country?

(16) Are the results of the threat and vulnerability assessment disseminated to affected organizations (for example,

organic, tenant, and supported RC units)? Note: Where specific vulnerabilities are identified are they reviewed for appropriate classification?

(17) Are procedures in place to conduct follow-on threat and vulnerability assessments of deployed forces?

c. Critical task 3, Army standard 3: Assess and reduce critical vulnerabilities (conduct AT assessments).

(1) Has the installation program been reviewed internally annually?

(2) Has the MACOM reviewed the installation AT Program within the last three years?

(3) Has the installation conducted a comprehensive self-assessment within the past three years?

(4) Does the installation prioritize, track, and report all vulnerabilities documented by installation and any higher headquarters vulnerability assessments to their MACOM headquarters within 60 days of the receipt of the vulnerability assessment final report?

(5) Are all identified physical vulnerabilities addressed in AT, physical security, or other installation supporting security plans? Are operational solutions included as additional FPCONs and exercise checklists?

(6) Are pre-deployment vulnerability assessments conducted for units deploying OCONUS, whether the deployment is for an exercise or an operational mission/support?

d. Critical task 4, Army standard 4: Increase antiterrorism awareness in every soldier, civilian, and family member.

(1) Does the commander incorporate AT Program information into the command information program?

(2) Is AT information being effectively disseminated through multiple means (for example, briefings, posters, newspaper/newsletter articles, chain of concern, radio, and television)?

(3) Is PA involvement in AT documented in proactive planning?

(4) Is OPSEC considered in all public affairs operations?

(5) Are PA responsibilities included in installation terrorist threat/incident response planning?

(6) Do policies and guidance ensure personnel (military, DA civilians, and family members) are provided with the appropriate level of AT training, education, and awareness?

(7) Is the command aware of Army requirements for Level I AT training, and have they implemented the program?

(8) Does AT awareness training incorporate the postulated threat?

(9) Are theater specific pre-deployment requirements for the CINC AORs being accomplished?

(10) Is there a validation process to ensure appropriate Level I training is accomplished for all travel and deployments, and so documented?

(11) Is the DOD-designated list of high physical and potential threat countries maintained and disseminated throughout the command?

(12) Are AT training materials readily available (for example, Level I videos, GTA wallet cards, etc.)?

(13) Are key leaders with AT responsibilities Level II trained?

(14) For personnel assigned to medium or higher terrorist threat level areas, is a certified and current instructor conducting hostage training at least annually?

e. Critical task 5, Army standard 5: Maintain installation defenses in accordance with FPCON.

(1) Is the installation level AT Program implementing RAMP at all FPCON levels?

(2) Is the installation RAMP documented in writing and controlled by the AT officer?

(3) Does the installation RAMP test all FPCON measures at least annually?

(4) Do units employ the techniques of RAMP as part of their AT effort?

(5) Are required residential security assessments conducted on initial occupancy and periodically thereafter?

(6) Is an up-to-date listing of residences for TDY and permanently assigned personnel maintained and safeguarded, and are they considered in the AT plan?

(7) Is there a prioritized list of AT factors for site selection teams reviewed and approved by the commander?

(8) Is the list utilized?

(9) Have HRT been formally designated?

(10) Are appropriate security measures employed to protect HRT at FPCON Normal, and are plans developed for enhanced protection at increased FPCON?

f. Critical task 6, Army standard 6: Establish civil/military partnership for WMD crisis.

(1) Have the installation plans been coordinated with outside agencies (that is, local authorities such as police, fire, medical emergency response personnel, etc.)?

(2) Do inter-service support agreements, MOU, and MOA regarding incident response consider AT?

(3) Do local agencies participate in AT committee group meetings?

g. Critical task 7, Army standard 7: Terrorist threat/incident response planning.

(1) Does the command have a reactive plan to deal with terrorist threats and incidents?

(2) Does the plan provide a process to change FPCON levels when required?

(3) Does the plan provide sufficient detail concerning the execution of individual FPCON measures to determine responsibilities, resource requirements, and timelines for implementation?

(4) Does the plan cover required terrorist related reporting?

(5) Are emergency evacuation procedures in-place and are they tested?

(6) Is there an attack warning system that utilizes a set of recognizable alarms with reactions to potential emergencies, as determined by the threat and vulnerability assessment?

(7) Are personnel trained and proficient in recognition of the attack warning system?

(8) Have HRT been identified and incorporated into response plans?

(9) In significant and high threat areas, do response plans contain current residential location information?

(10) Does the capability exist to implement all FPCONs?

(11) If the capability does not exist to implement all FPCONs, are there procedures to divert/acquire local assets on an emergency basis consistent with the Federal Acquisition Regulation?

h. Critical task 8, Army standard 8: Conduct exercises and evaluate/assess AT plans.

(1) Are installation terrorist threat/incident response plans exercised at least annually?

(2) Are all necessary installation staff agencies exercised?

(3) Do exercises test WMD and mass casualty contingencies?

(4) Is there a system in place to exercise attack-warning systems at least annually?

(5) Is there a feedback mechanism to route after-action review results through the AT committee to the commander?

(6) Is OPSEC considered in the planning, conduct, and evaluation of exercises?

(7) Does the MACOM have an AT Operational Assessment Team?

(8) Is the installation tested through the AT Operational Assessment Program once every two years or at least once during every Garrison Commander's tour of duty?

(9) Do MACOM Commanders provide written guidance to subordinate unit commanders for incorporating AT planning into major exercises and training center rotations?

(10) Do unit commanders exercise deployment AT plans during major exercises and training center rotations?

C–5. Supersession

This checklist supersedes the checklist published in the 1998 publication of AR 525–13.

C–6. Comments

Submit comments for improvement of this management controls tool to:
HQDA (DAMO–ODL–FP), ODCSOPS, 400 Army Pentagon, Washington, DC 20310–0400.

Appendix D
Required Reports

D–1. Terrorist Threat Report [RCS exempt: AR 335–15, para 5–2e(2)]

a. Terrorist Threat Reports (TTRs) will be submitted using the OPREP–3 format when a command receives credible information concerning a planned terrorist attack against U.S. Army personnel (soldiers, civilian employees, or their family members), facilities, 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 targeted to counter a specific threat.

b. The OPREP–3 will be provided immediately by telephone to the Army Operations Center (AOC) (phone DSN 227–0218/9 or commercial (703) 697–0218/9). Local commanders will comply with any additional MACOM guidance concerning dissemination of such time-sensitive information.

c. A follow-up OPREP–3 will be transmitted within six hours of receiving the information by IMMEDIATE precedence electrical message to HQDA (DA, Washington, DC//DAMO-AOC/DAMO-ODL-FP/DAMO-ODO/DAMI-CHI//), USACIDC (CDRUSACIDC Ft. Belvoir, VA//CIOP-IN//), and INSCOM (CDRINSCOM Ft. Belvoir, VA//IAOPS-IS//). Local commanders will include their MACOM (and the MACOM with geographical responsibility for the location of the incident) as information addressees and comply with any additional MACOM guidance concerning dissemination of such information.

d. OPREP–3 updates should be submitted when additional substantive information concerning the terrorist threat becomes available. Such reports will be submitted upon receiving the information by PRIORITY precedence electrical message directly from the command receiving the information to the addressees in para D–1.*c*. All information addressees for the initial OPREP–3 will be provided in this and future updates.

e. The initial OPREP–3 will include date, time, and location and brief description of the threatened attack and response thereto.

f. 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 host nation actions taken, if any, since receiving the threat.
(8) Any additional amplifying information.

D–2. Terrorist Incident Report [RCS exempt: AR 335–15, para 5–2e(2)]

a. Terrorist Incident Reports (TIRs) will be submitted utilizing the OPREP–3 format when a terrorist incident or suspected terrorist incident occurs, involving U.S. Army personnel (soldiers, civilian employees, or their family members) or facilities. A "suspected terrorist incident" is one in which involvement by terrorists has not been ruled out by lead agencies conducting the investigation.

b. The initial OPREP–3 will be provided immediately by telephone to the AOC. 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, the local commander will submit an OPREP–3 by IMMEDIATE precedence electrical message to HQDA (DA, Washington, DC//DAMO-AOC/DAMO–ODL-FP/DAMO-ODO/DAMI-CHI//), USACIDC (CDRUSACIDC Ft. Belvoir, VA//CIOP-IN//), and INSCOM (CDRINSCOM Ft. Belvoir, VA//IAOPS-IS//). Local commanders will include their MACOM (and the MACOM with geographical responsibility for the location of the incident) as information addressees and comply with any additional MACOM guidance concerning dissemination of such information. The OPREP–3 will be as complete as possible, with omitted information transmitted as soon as known. Army components of unified commands may report threat incidents under the OPREP–3 system, with addressees listed above, as long as timelines and information requirements as specified in this regulation are met. The following information will be included in the OPREP–3:

(1) A complete description of the terrorist incident, including the following:
(a) Type of incident and location.
(b) Date and time of incident.
(c) Detailed description of incident.
(d) Weapons/explosives used.
(e) Likely perpetrators.
(f) Claims of responsibility.

(g) Number of personnel killed and number of personnel injured and their conditions.

(2) Threats received prior to the incident that could be related.

(3) Local FPCON prior to the incident.

(4) Other AT measures in effect prior to the incident.

(5) U.S. and host nation actions taken since the incident.

(6) Any amplifying information available.

D–3. After Action Report [RCS exempt: AR 335–15, para 5–2e(7)]

After Action Reports, containing comprehensive discussion of lessons learned, will be forwarded by MACOMs to HQDA (DAMO–ODL–FP) and the CALL within 30 days of a reported terrorist threat or terrorist incident.

D–4. FPCON Report [RCS exempt: AR 335–15, para 5–2e(2)]

a. FPCON reporting requirements in this section apply to MACOMs.

b. MACOMs are responsible for monitoring and reporting FPCONs and FPCON changes of all subordinate commands including those located in another MACOM's geographical AOR.

c. MACOMs will maintain a reporting system within their respective commands. OCONUS, MACOMs will establish FPCONs for all countries (within the joint command AOR) in which they have installations or deployed forces.

d. MACOM-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. If the change involves FPCONs CHARLIE and/or DELTA, initial report will be provided immediately.

(2) A follow-up report will be provided via electrical message within six hours. 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.

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

(a) MACOMs will report FPCON changes of subordinate commands if they involve a change to/from FPCONs BRAVO, CHARLIE and/or DELTA. This does not absolve MACOM and subordinate 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 para D–4*d*(1)(2).

(4) MACOMs will provide monthly FPCON reports to HQDA in accordance with the following procedures:

(a) Monthly reports will be provided to HQDA (DA, Washington, DC //DAMO/ODL-AT/DAMI-CHI//) 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) Monthly reports will include the following:

(1) Overall MACOM FPCON. In most cases, this is the minimum FPCON level established by the MACOM commander. When a substantial majority of MACOM subordinate commands have implemented a FPCON higher than the minimum FPCON within the MACOM, the commander may designate that higher FPCON as the MACOM FPCON (as an exception to normal policy).

(2) FPCON measures implemented (listed by measure number).

(3) Exceptions to the overall MACOM FPCON (with rationale), including countries, subordinate commands, or installations that have implemented a FPCON other than the MACOM FPCON.

Appendix E
Public Affairs Officer Guidance

E–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 host nation security forces to ensure maximum coordination for appropriate protective measures." (In those rare instances where the U.S. and host nation 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 MACOM public affairs channels to HQDA (SAPA–MR), Washington, DC 20310. HQDA (SAPA–MR) will coordinate requests with OASD (PA) and ODCSOPS, HQDA.

d. Prior to releasing Army-produced AT training photos, videotapes, films, or slides to the media, PAOs must obtain OASD (PA) and HQDA ODCSOPS 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, ODCSOPS.

(1) PAOs, after coordinating proposed releases with their local crisis management team, will forward the proposal through the appropriate MACOM to HQDA (SAPA–PP). HQDA (SAPA–PP) will coordinate release with OASD (PA) and HQDA, ODCSOPS.

(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, ODCSOPS. 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.

E–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, ATTN: AOPA, Ft. 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 F
Antiterrorism Training Requirements

F–1. Antiterrorism awareness training

a. All military, and DOD civilians, will receive annual AT awareness training. Personnel traveling outside the 50 United States, its territories and possessions (to include leave, pass or temporary duty) will receive an AOR update within two months of travel and have received annual AT awareness training within 12 months of travel.

b. All military and DOD civilian family members will receive mandatory AT awareness training within 12 months of travel, on official government orders, outside the United States, its territories, and possessions and permanent change of station OCONUS travel.

c. All DOD-employed contractors will be offered, under terms and conditions specified in the contract, annual AT awareness training and an AOR update prior to traveling outside the 50 United States, its territories and possessions (to include temporary duty).

d. Training required is as follows:

(1) Conducted within twelve months prior to travel.

(2) CJCS-approved, Web-based AT Awareness Course or course instructed by a certified Level II instructor using an approved USAMPS lesson plan, containing a minimum of the following subjects:

(a) Introduction to terrorism.

(b) Terrorist operations.

(c) Individual protective measures.

(d) Terrorist surveillance techniques.

(e) Improvised explosive device (IED) attacks.

(f) Kidnapping and hostage survival.

(g) Explanation of terrorism threat levels and FPCON System.

(3) Recent AOR update for the area of travel view AT/FP Awareness Videos on the following:

(a) Individual protective measures.

(b) Terrorist surveillance detection.

(c) Hostage survival techniques.

(4) Receive AT awareness handouts:

(a) JS Guide 5260, July 96 and DOD Antiterrorism Individual Protective Measures wallet card; or,

(b) GTA 19–4–3 (Individual Protective Measures), July 97 and GTA 21–3–11, Army Antiterrorism Individual Protective Measures wallet card; or,

(c) CINC/HQDA approved equivalent.

F–2. Training for Antiterrorism Officers

a. The training described below applies to E6 to 04 military personnel or GS5 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 critical tasks:

(1) Understand AT roles and responsibilities (including policy, standards, and references).

(2) Organize for AT (including command and staff relationships and AT committees and working groups).

(3) Assess vulnerabilities (including baseline unit AT posture and a practical exercise on conducting assessments).

(4) Assess threat (including intelligence and counterintelligence integration and information operations).

(5) Prepare AT plans (including templates and planning tools, WMD considerations, implementation of RAMP, and development/writing plans).

(6) Conduct AT training (including AT awareness training and AT exercises).

(7) Create and execute AT Program (including use of threat levels/FPCONs, unit/installation protective measures, and mitigating vulnerabilities).

(8) AT resource management (including requirements generation and prioritization and Cbt-T readiness initiative fund).

F–3. Antiterrorism pre-command training

a. The training described below applies to O5/O6 Commanders/Command Select.

b. Training required:

(1) Attend AT training during the Army Pre-Command Course (PCC) or the Garrison Commanders' Pre-Command Course.

(2) A TRADOC approved program of instruction for antiterrorism pre-command training, which contains a minimum of the following subjects, will be used.

(a) Understand AT responsibilities (including policy, assessments and off-installation housing).

(b) Organize for AT (including command and staff relationships and AT committees and working groups).

(c) AT plans and programs (including baseline AT posture, mitigating WMD attack, MOU/MOA, AT plans and AT training).

(d) Understanding the local threat picture (including fusion).

(e) Building and sustaining an AT Program (including the linkage of threat assessments, vulnerability assessments, updating AT plans, RAMP, and implementation of FPCON Normal through Delta).

(f) Resource responsibilities (including resourcing the AT Program and MILCON standards).

(g) Implementing Rules of Engagement and Use of Force (including terrorist scenarios and hostile intent decisionmaking).

(h) View SEC DEF/CJCS AT Awareness Video TVT; *You May Be the Target.*

F–4. Antiterrorism executive level training

a. The training described below applies to O–6 to O–8 Commanders (and civilian equivalent) responsible for AT programs, policy, planning & execution.

b. Training required: Executive level seminar that provides pertinent briefings, current updates and panel discussion topics. Seminar includes a tabletop AT wargame that facilitates interaction & discussion on power projection, WMD, FPCON management and AT implementation.

Appendix G
Defensive Information Operations Integration, Training, and Assessments

G–1. Defensive Information Operations

a. Commanders should ensure that Defensive Information Operations are integrated into all AT/FP planning and program execution, and supporting training is planned for and resourced. Commanders will ensure integration of, and adherence to, relevant laws and regulations pertaining to security of the command's information infrastructure.

b. Commanders must ensure that—

(1) Provisions of AR 380–19 governing the use of automated tools to conduct assessments and analysis for continuity of operations are integrated into the command's AT Program.

(2) Provisions of AR 380–53 governing security monitoring, exploitation, and penetration activities are adhered to and integrated into the command's AT Program.

(3) All components of Defensive Information Operations (for example, OPSEC, electronic security, physical security, intelligence, ISS, counter-deception, and counter-PSYOPS), and, when published, the provisions of AR 25–1 are integrated into the AT Program.

(4) Incidents occurring on networks are reviewed and analyzed to identify significant weaknesses.

(5) Incident reporting procedures are published for system administrators in accordance with AR 380–19, AR 25–1, and ACERT reporting procedures.

(6) A warning system has been devised to alert the command of incidents.

(7) Provisions of AR 530–1 are integrated into all elements of the command's AT/FP Program (for example, physical security, law enforcement, and operations).

(8) Defensive Information Operations components are included in threat briefings and assessments provided to the command, as appropriate.

(9) Designation of a MACOM information assurance manager (IAM).

(10) Designation below MACOM, and at DA Staff and field operating agencies, of an IAM at all appropriate levels.

(11) Designate an information assurance security officer (IASO) for each AIS.

(12) Training programs are established, based upon local need and applicable regulations and directives, to ensure experts and users are properly trained in these procedures.

G–2. Defensive Information Operations procedures and techniques

a. Commanders will ensure that Defensive Information Operations procedures and techniques are developed to protect the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

b. Commanders will ensure that—

(1) An annual threat and vulnerability assessment of their information systems is conducted by authorized U.S. Army activities or approved contractors using U.S. citizens only.

(2) A methodology is in place to protect, detect, and react to computer intrusions. Commanders will utilize the Information Assurance Vulnerability Assessment Program to ensure the integrity of AIS and C2 systems by developing a proactive program to detect and deny threat access.

(3) The command is registered in the Terminal Server Access Controller System for access to the Army tool set and identified specific requirements for tools.

(4) Procedures are in place to report incidents to the ACERT.

(5) The OPSEC process is applied in determining threats and vulnerabilities to the command's communications infrastructure and implementing appropriate countermeasures.

(6) ISS procedures are routinely reviewed and tested (for example, user IDs, passwords, audit trails, and system configurations).

(7) All security incidents/violations (for example, viruses, unauthorized entries or attempts, and password compromises) are analyzed, reviewed, investigated, and reported in accordance with AR 380–19, AR 25–1, and ACERT reporting procedures.

(8) Security measures are employed to control the external access (for example, callback and tokens) and an automated audit capability (that is, log security-related events) is available and used in all systems.

(9) Identification and authentication (that is, user id/password, biometric devices, and tokens) are required for access to all systems.

(10) Any monitoring operations are conducted consistent with the requirements of AR 380–53 and other applicable regulations and directives.

Glossary

Section I
Abbreviations

ACSIM
Assistant Chief of Staff for Installation Management

AOC
Army Operations Center

AOR
area of responsibility

APOE
aerial port of embarkation

ARGUS
Army National Guard of the United States

ARNG
Army National Guard

ARSOF
Army Special Operations Forces

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

ASD(ISA)
Assistant Secretary of Defense (International Security Affairs)

AT
antiterrorism

ATO
Antiterrorism Officer

ATOIC
Antiterrorism Operations and Intelligence Cell

C2 Protect
command and control protect

C4
command, control, communications, and computers

CALL
Center for Army Lessons Learned

CAR
Chief of the Army Reserve

Cbt–T
combating terrorism

CG
commanding general

CI
counterintelligence

CINC
Commander in Chief

CJCS
Chairman, Joint Chiefs of Staff

COM
Chief of Mission

CONUS
continental United States

CPA
Chief of Public Affairs

CT
counterterrorism

CTL
composite threat list

DARNG
Director, Army National Guard

DCSINT
Deputy Chief of Staff for Intelligence

DCSLOG
Deputy Chief of Staff for Logistics

DCSOPS
Deputy Chief of Staff for Operations and Plans

DCSPER
Deputy Chief of Staff for Personnel

DIA
Defense Intelligence Agency

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

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

FAA
Federal Aviation Administration

FBI
Federal Bureau of Investigation

FORSCOM
United States Army Forces Command

HN
host nation

HRP
high-risk personnel

HQDA
Headquarters, Department of the Army

ICAO
International Civil Aviation Organization

IG
Inspector General

INSCOM
United States Army Intelligence and Security Command

ISS
information system security

ISSO
information system security officer

JCS
Joint Chiefs of Staff

JFTR
joint federal travel regulations

LFA
lead Federal agency

LIWA
Land Information Warfare Activity

MACOM
major Army command

MCA
military construction, Army

MDW
United States Army Military District of Washington

MEVA
mission essential or vulnerable area

MI
military intelligence

MILCON
military construction

MITS
Monthly International Terrorism Summary

MP
military police

MOA
Memorandum of Agreement

MOU
Memorandum of Understanding

NBC
nuclear, biological, and chemical

NCIC
National Crime Information Center

OCONUS
outside continental United States

OCPA
Office of the Chief of Public Affairs

ODCSINT
Office of the Deputy Chief of Staff for Intelligence

ODCSLOG
Office of the Deputy Chief of Staff for Logistics

ODCSOPS
Office of the Deputy Chief of Staff for Operations and Plans

ODCSPER
Office of the Deputy Chief of Staff for Personnel

OMA
Operation and Maintenance, Army

OPA
Other Procurement, Army

OPLAN
operation plan

OPORD
operation order

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

POE
port of embarkation

PM
provost marshal

POM
program objective memorandum

PSVA
personal security vulnerability assessment

RC
Reserve Component

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

SCI
sensitive compartmented information

SOFA
Status of Forces Agreement

SOP
standing operating procedures

TDY
temporary duty

TIG
The Inspector General

TIR
Terrorist Incident Report

TRADOC
United States Army Training and Doctrine Command

TSG
The Surgeon General

TTR
Terrorist Threat Report

USACE
United States Army Corps of Engineers

USACIDC
United States Army Criminal Investigation Command

USAR
U.S. Army Reserve

USARPAC
U.S. Army, Pacific

USCG
United States Coast Guard

USDR
U.S. Defense Representative

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.

Combating terrorism
Combating terrorism within the Army encompasses all actions, including antiterrorism, counterterrorism, consequence management, and intelligence support taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE).

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism. Within the Army, Army Special Operations Forces have the primary mission to preclude, preempt, and resolve terrorist incidents abroad. Sensitive and compartmented counterterrorism programs are addressed in relevant Presidential Decision Directives, National Security Directives, classified contingency plans, and other relevant classified documents.

Credible threat
A threat that is evaluated as serious enough to warrant a FPCON change or implementation of additional security measures.

Criminal intelligence
The product that results from the collection, analysis, and interpretation of all available information concerning known and potential criminal threats and vulnerabilities of supported organizations.

Crisis situation
Any emergency so declared by the National Command Authority (NCA) or the overseas combatant commander, whether or not U.S. Armed Forces are involved, minimally encompassing civil unrest or insurrection, civil war, civil disorder, terrorism, hostilities buildup, wartime conditions, disasters, or international conflict presenting a serious threat to DOD interests.

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 (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.

Doctrine
Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.

DOD-designated high physical threat countries
Countries determined to be of significant terrorist threat to DOD travelers, as designated by the Assistant Secretary of Defense (Special Operations Low Intensity Conflict) ASD(SOLIC) in coordination with ASD(ISA).

DOD-designated potential threat countries
Countries determined to be of potential terrorist threat to DOD travelers, as designated by the ASD(SO/LIC) in coordination with the ASD(ISA).

Domestic terrorism
Terrorism perpetrated by the citizens of one country against fellow countrymen. That includes acts against citizens of a second country when they are in the host country, and not the principal or intended target.

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.)

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 force protection condition (FPCON) is a DOD-approved system standardizing the military Services' identification of and recommended preventive actions and responses to terrorist threats against U.S. 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 to be at risk as potential terrorist targets because of mission sensitivity, ease of access, isolation, symbolic value, and/or potential for mass casualty.

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

Improvised explosive device
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.

In-flight
The condition of an aircraft from the moment when all external doors are closed following embarkation until the moment when one such door is opened for disembarkation.

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

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

b. 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.

National Command Authorities

National Command Authorities (NCA) are the President and Secretary of Defense or their duly deputized alternates or successors.

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-

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 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.

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.

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.

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

Security procedural measures
Physical security measures to counter risk factors that will periodically change over a period of time such as criminal, terrorist, and hostile threats. The procedures can usually be changed within a short amount of time and involve manpower.

Special operations forces
Those active and reserve component forces of the military Services designated by the Secretary of Defense and specially organized, trained and equipped to conduct and support special operations. Such forces engage primarily in direct action, unconventional warfare, psychological operations, counterterrorism, and intelligence missions.

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.

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
a. 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.
b. 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. Can be nuclear, chemical, biological, radiological or high-yield explosive 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, this includes the use of very large improvised explosive devices and environmental sabotage, which is capable of destruction at the same magnitude.

Section III
Special Abbreviations and Terms
This publication uses the following abbreviations, brevity codes, and acronyms not contained in AR 310–50:

ACERT
Army Computer Emergency Response Team

ACIC
Army Counterintelligence Center

AIQC
AT Instructor Qualification Course

AIS
automated information systems

ASD(SOLIC)
Assistant Secretary of Defense (Special Operations Low Intensity Conflict)

CBR
chemical, biological, and radiological

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

EDD
explosive detector dog

FIS
foreign intelligence service

FP
force protection

GLOC
ground lines of communication

HRT
high-risk target

IAM
information assurance manager

IASO
information assurance security officer

IED
improvised explosive device

INTAC
Individual Terrorism Awareness Course

IO
information operations

MASCAL
mass casualties

PIR
priority intelligence requirements

PM/SO
provost marshal/security officer

RAMP
Random Antiterrorism Measures Program

RSO
regional security officer

SBCCOM
U.S. Army Soldier and Biological Chemical Command

SJA
staff judge advocate

USAFAMC
U.S. Air Force Mobility Command

USASOC
U.S. Army Special Operations Command

USSOCOM
U.S. Special Operations Command

WMD
weapons of mass destruction

Index

This index is organized alphabetically by topic and by subject within a topic. Paragraph number identifies topics and subtopics.

USAPA

ELECTRONIC PUBLISHING SYSTEM
OneCol FORMATTER .WIN32 Version 171

PIN: 063256–000
DATE: 01-30-02
TIME: 12:00:10
PAGES SET: 53

DATA FILE: C:\wincomp\r525-13.fil
DOCUMENT: AR 525–13
DOC STATUS: NEW PUBLICATION