Department of the Army
Headquarters, United States Army
Training and Doctrine Command
Fort Monroe, Virginia 23651-5000

12 December 1997

Military Operations

UNITED STATES ARMY TRAINING AND DOCTRINE COMMAND (TRADOC)
FORCE PROTECTION PROGRAM (FPP)

Summary. This regulation prescribes responsibilities, policies, procedures, and minimum standards for developing, implementing, and managing a Force Protection Program (FPP). It is written with HQ TRADOC staff and installations in mind. Force Protection (FP) is the security program designed to protect soldiers, civilian employees, family members, facilities, and equipment, within the TRADOC area of responsibility; at home station, during mobilization, during deployment, and in conjunction with overseas temporary duty or permanent change of station.

Applicability. This regulation applies to all TRADOC subcommands, installations, and activities.

Supplementation. Do not supplement this regulation without approval from Commander, TRADOC, ATTN: ATBO-J, Fort Monroe, VA 23651-5000.

Suggested improvements. The proponent of this regulation is the Deputy Chief of Staff for Base Operations Support (DCSBOS). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC, ATTN: ATBO-J, Fort Monroe, VA 23651-5000. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal.

Availability. This publication is also available on the TRADOC Homepage at http://www.tradoc.army.mil.

Contents

Chapter 1
Introduction

1-1. Purpose. This regulation prescribes responsibilities, policies, procedures, and minimum standards for developing, implementing, and managing TRADOC's FPP. In addition to outlining base operations responsibilities for installation commanders, it fixes responsibility for force protection proponency across the TRADOC domain: doctrine, training, leadership, organization, materiel, and soldier (DTLOMS).

a. The Downing Report is a comprehensive report by General Wayne A. Downing on the facts and circumstances surrounding the June 1996 terrorist bombing of the Khobar Towers in Saudi Arabia. The report recommended numerous changes in the way the Department of Defense (DOD) has traditionally managed FP. Based on the findings of the report, the Department of the Army (DA) has identified five areas where enhancements are required: theater specific FP training, PS standards for facilities and installations, resourcing FP requirements, intelligence collection, processing and dissemination, and better use of technology.

b. The TRADOC FPP is a security program designed to protect soldiers, civilian employees, family members, facilities and equipment, in all locations and situations. Threats include: terrorists and criminals, disaffected persons, hostile intelligence gathering, paramilitary forces, protesters, and saboteurs. Effective FPP is centralized and tightly focused on a holistic management approach at the command, installation, and unit/activity level. FP requirements must be identified, consolidated and synchronized, risk assessment conducted and distribution of resources prioritized. FPP must be continuously assessed and updated.

1-2. References. Appendix A contains the required and related publications.

1-3. Explanation of abbreviations and terms. The glossary contains abbreviations and special terms used in this regulation.

Chapter 2
Responsibilities

2-1. CG, TRADOC. The CG, TRADOC will designate both a DTLOMS (CAC) proponent and HQ TRADOC staff (DCSBOS) proponent for the FPP.

2-2. CG Combined Arms Center (CAC). The CG CAC will--

a. Be the TRADOC DTLOMS proponent for FP. Oversee all FP DTLOMS functions within TRADOC to include those specific areas designated by this regulation to TRADOC DCS.

b. Serve as the FP integrator/coordinator for the TRADOC doctrine domain.

c. Embed FP doctrine into field manuals, as well as other applicable doctrinal publications for which CAC is proponent. Provide guidance to CASCOM and branch schools regarding inclusion of FP in their respective field manuals.

d. Ensure Center for Army Lessons Learned (CALL) routinely collect, archive, and publish FP lessons learned during OCONUS deployments to high-threat environments, combined training center (CTC) rotations, installation exercises, past terrorist incidents and other relevant events.

2-3. DCG Combined Arms Support Command (CASCOM). The DCG CASCOM will embed FP doctrine developed by CAC into field manuals and other doctrinal publications for which CASCOM is the proponent. Ensure required FP individual and collective training programs are conducted in schools for which CASCOM is responsible.

2-4. DCS Base Operations Support (DCSBOS). The DCSBOS is designated by the CG, TRADOC as the HQ TRADOC staff proponent for FPP. DCSBOS will--

a. Designate the CPM as the HQ TRADOC Force Protection Officer (FPO).

b. Establish and chair a HQ TRADOC Force Protection Committee (FPC), with representation from appropriate staff agencies. The FPC will continually monitor the FP posture of the command, update the threat as required, and make recommendations on FP issues.

c. Publish guidance for all subordinate commands concerning implementation of the FPP; to include command-specific guidance concerning implementation of threat condition (THREATCON) measures.

d. Ensure FP is aggressively managed in compliance with DOD, DA, and TRADOC plans, policies, and guidance.

e. Closely monitor and evaluate the FP programs of subordinate commands and installations. Formally review FP plans and reports every two years (or as directed) to ensure standardization and program effectiveness. These plans are to be exercised at installation level on an annual basis.

f. Manage PS and AT management decision packages (MDEPs). Establish a system to monitor expenditure of FP funds from programming through budget execution.

g. Program funds and identify personnel to attend specialized FP training. Ensure all installation personnel with significant FP responsibilities in operations, intelligence, criminal investigation, and law enforcement receive specialized training.

2-5. Command Provost Marshal (CPM). The CPM is designated as the TRADOC FPO.

2-6. Staff Judge Advocate (SJA). The SJA will provide legal representation to the TRADOC FPC.

2-7. Director, Safety (SAFE). Safety will--

a. Provide planning, coordination, and guidance to adjacent, subordinate, and higher commands on risk management issues and policies related to this regulation.

b. Require installation safety and fire marshals review FP countermeasures to ensure security measures do not endanger personnel.

c. Serve as a member of the TRADOC FPC.

2-8. DCS Training (DCST). The DCST will--

a. Embed FP training requirements into institutional training and education systems as appropriate.

b. Serve as the FP integrator/coordinator for the TRADOC training and leadership domains.

c. Serve as a member of the TRADOC FPC.

2-9. DCS Intelligence (DCSINT). The DCSINT will--

a. Develop and distribute the TRADOC AT threat statement on an annual basis.

b. Develop and maintain the CG, TRADOC AT statement (Black Book).

c. Ensure SAEDA training (AR 381-12) is being conducted at HQ TRADOC and all TRADOC installations for all military and civilian personnel.

d. Provide MACOM program management for intelligence and security MDEPS.

e. Serve as a member of the TRADOC FPC.

2-10. DCS Doctrine (DCSDOC). The DCSDOC will embed FP into doctrine to include:

a. FP principles into Army echelon above corps (EAC) doctrine.

b. Review Army FP doctrine to ensure consistency with joint FP doctrine when applicable.

c. Assess and provide feedback to CAC concerning FP lessons learned published by CALL.

d. Serve as a member of the TRADOC FPC.

2-11. DCS Combat Development (DCSCD). The DCSCD will--

a. Embed FP issues and principles into concepts and requirements development.

b. Serve as the FP integrator/coordinator for TRADOC organization and materiel domains.

c. Serve as a member of the TRADOC FPC.

2-12. DCS Resource Management (DCSRM). The DCSRM will--

a. Provide budget guidance on FP to TRADOC installations and activities.

b. Serve as a member of the TRADOC FPC.

2-13. Chief of Public Affairs (CPA). The CPA will--

a. Plan, coordinate, and direct public affairs (PA) support for the TRADOC FP program.

b. Provide public affairs guidance (PAG) on FP issues to TRADOC installations and activities.

c. Serve as the command's official spokesperson responsible for coordinating the release of cleared FP information to the news media.

d. Serve as a member of the TRADOC FPC.

2-14. TRADOC Surgeon. The TRADOC Surgeon will--

a. Act as a liaison between TRADOC and the USA Medical Command (MEDCOM). The Director of Health Services (DHS) (normally the hospital/clinic commander) at each installation will develop a well-planned, coordinated, flexible, and effective Medical Response and Consequence Management Program.

b. Serve as a member of the TRADOC FPC.

2-15. DCS Information Management (DCSIM). The DCSIM will--

a. Provide guidance and support to the TRADOC Executive Committee on ISSP issues.

b. Serve as a member of the TRADOC FPC.

2-16. Commandants. Commandants will--

a. Embed FP principles into the DTLOMS domain.

b. Ensure the Level III module on FP is taught at battalion/brigade precommand courses.

c. Conduct required FP training.

2-17. Installation commanders. Installation commanders will--

a. Appoint an FPO.

b. Publish and maintain an installation FP plan as described in paragraph 3-5 and update annually.

c. Develop, implement, and maintain an overarching installation FP program which synchronizes the five existing security programs:

(1) Physical security.

(2) Information security.

(3) Protective services.

(4) Law enforcement.

(5) Antiterrorism.

d. Establish an FPC with representation from law enforcement, plans and training, security and intelligence, engineer, information management, logistics, medical, legal, safety, resource management, and PA. FPC will meet twice annually and incorporate the responsibilities of the PS Council required by AR 190-13.

e. Ensure FP requirements are granted a high budget priority and maintain a strict audit trail for FP funds.

f. Ensure FP is aggressively managed in compliance with DOD, DA, and TRADOC plans, policies, and guidance.

g. Ensure all service members, DOD civilians, and other civilians traveling to negligible/low, medium/high, potential physical threat countries, and processing through continental United States (CONUS) replacement centers (CRC) or individual deployment sites (IDS) attend the appropriate Level I briefings and receive individual protective measure handouts (chapter 9).

h. Ensure individual and unit augmentees deploying to high-threat areas on temporary duty are provided (prior to departure) protective equipment, CTA 50-900 and other items as required by the supported command.

i. Coordinate with the DHS for development of a Medical Response and Consequence Management Program.

j. Conduct an annual FP exercise that includes a mass casualty (MASCAL) exercise. Report an executive summary and lessons learned to TRADOC, ATTN: ATBO-J.

k. Incorporate FP special interest inspection items in the Command Inspection Program.

Chapter 3
Force Protection Program

3-1. General.

a. Protecting TRADOC assets, information, and personnel is a primary responsibility of all

commanders and leaders. FP is an overarching security program developed to protect soldiers, civilian employees, family members, facilities, and information and equipment, in all locations and situations. It is a holistic program accomplished through the planned integration of PS, INFOSEC, protective services, law enforcement, and AT, all supported by the synchronization of operations, intelligence, training and doctrine, policy and resources. This synchronization and integration is accomplished through the TRADOC FP standards located at appendix H of this regulation.

b. The TRADOC commander directs or delegates authority to installation commanders to establish the level of security measures in accordance with the Joint Chiefs of Staff (JCS) THREATCON system . The DCSBOS provides overall staff supervision and coordination for FP. Installation commanders exercise geographic command and control for their area of responsibility (AOR) and will develop and implement a comprehensive FPP designed to accomplish all the standards contained in this document.

c. Commanders should not develop their FPP in isolation. All agencies involved in program execution, to include non-DOD agencies at the local, state, and federal level, must be fully integrated into the program's development, coordination, and maintenance. The FPP must provide for the protection of critical assets, information, and personnel on the installation or facility on a daily basis. Additionally, the program must address units and individuals going outside of the U.S., during deployment and mobilization operations. Since the absolute and continuous protection of the many structures, activities, equipment, and personnel under the commander's control is unrealistic, resources and assets must be prioritized and the required level of protection, during various periods of time, clearly specified.

d. Actions necessary to meet the established standards must be identified, prioritized, and resourced. Where local resources are insufficient to meet minimum standards, commands must forward prioritized and justified requirements to this headquarters and initiate appropriate compensatory measures. Commanders must be personally involved in the FPP.

e. All installations will establish a FPC that meets twice annually when THREATCON Normal conditions prevail. The installation commander will review the requirement to convene on a more frequent basis when THREATCON increases. A report of the meeting will be forwarded to TRADOC, ATTN: ATBO-J, no later than 30 days from the date of the meeting.

f. All installations will establish a fusion cell that meets frequently to discuss the current criminal and terrorist threat, and evaluate security measures that have been implemented or planned for implementation.

g. TRADOC's operational concept for implementation of FP is based on eight fundamentals:

(1) Threat assessment.

(2) Established security standards.

(3) Mission impact.

(4) Viable THREATCON system.

(5) Planned, coordinated, and focused effort.

(6) Individual and leader training.

(7) Effective information flow.

(8) Continuous program assessment and update.

h. Prior to 15 November of each year, provide the Commander, TRADOC, an assessment of FPP. The assessment will include:

(1) A narrative discussion of the command's FP status.

(2) A copy of the updated FP plan.

(3) Identification of all FP upgrades completed during the preceding fiscal year.

(4) The amount of funds spent on FP upgrades during the preceding fiscal year.

(5) Programmed FP upgrades for the next fiscal year.

(6) Prioritized list of unresourced FP projects, with justification.

(7) A summary of lessons learned from the annual FP exercise.

3-2. Threat. The nature and degree of threat to the Army varies widely with geographical location, criticality, and vulnerability of the target, and level of hostile intent. FP is a flexible program designed to meet all these threats, not just terrorism. There are four general categories of groups that pose threats to the Army:

a. Terrorists. National and international terrorist events have highlighted that TRADOC and its subordinate commands and installations are faced with a continuing terrorist threat. This threat may come from individuals or groups who oppose U.S. policy, military operations, or the military presence in overseas locations. As the primary source of the nation's training and doctrine capability, TRADOC is a tempting target. Many of these individuals or organizations are not terrorist in philosophy, but organize to demonstrate, march, or conduct activities to disrupt normal operations. These organizations may be infiltrated by militants who intend to cause damage, provoke security forces, or escalate peaceful activities to violence. The end result of their efforts is property damage, injury to personnel, or unfavorable publicity which may adversely affect the TRADOC mission. Terrorism is not a recent phenomenon in the U.S. or overseas. The threat to the Army is real and will continue. Bombings, shootings, and kidnappings are still the most likely methods used by terrorists, but there is a growing trend to use different types of weapons, with the emphasis on lethality and producing mass casualties. Other types of terrorist attacks include: arson; hostage-taking; hijacking / skyjacking; seizure; raids/attacks on facilities; commercial/ industrial sabotage; hoaxes; use of weapons of mass destruction; information warfare; and, ecological terrorism. Terrorists attack weak/soft and unprepared targets which will garner the maximum amount of attention/ support for their cause.

b. Criminals. Criminals, whose goals are to profit from the theft of government property or information, are a threat to numerous Army assets. Types of criminals range from organized to unsophisticated, and act for personal rather than political or ideological gain. Organized criminal groups plan in detail, and possess superior security system bypass and physical security barrier breaching equipment. Their targets include: arms, ammunition, and explosives (AA&E), specialized equipment, and large sums of money. However, most criminal threats directed at the Army are unsophisticated and focus on crimes of opportunity. Many are committed by insiders (government employees) who act alone without detailed planning. Their success largely depends upon the ability to circumvent security systems.

c. Protesters. Violent and nonviolent protesters are considered to be a threat. Protesters include the two general groups of vandals/activists and extremist protesters. The primary objectives of both groups commonly include destruction and publicity. Vandals/ activists are very adept at interrupting normal missions in order to achieve their objectives. This group includes disaffected government employees. Extremist protesters are more sophisticated and destructive. They normally attack symbolic targets and authority figures and will damage or destroy property or equipment.

d. Subversives. Subversives include people from foreign governments or from groups trying to overthrow the U.S. Government by force. This category includes saboteurs and spies. Sabotage, usually conducted by well-armed, well-trained guerrillas and unconventional warfare forces, is normally targeted at mission-critical personnel or equipment, information systems and military operations. Likely targets include AA&E storage and manufacturing facilities. Amateurs and disgruntled employees also conduct acts of sabotage against information systems and other attractive targets. Spies operate covertly to gain access to and steal military information. U.S. government employees who spy, use their workplace as a protective screen to provide vital information to foreign countries

e. Threat objectives will normally fall into one of the following areas:

(1) Gain media attention for their cause.

(2) Disrupt normal operations.

(3) Promote distrust between military and local authorities.

(4) Demoralize U.S. military and their families.

(5) Assassinate key personnel.

(6) Take hostages.

(7) Damage or destroy property.

(8) Disrupt communications and information systems.

3-3. Risk management. Risk management is a process the commander uses to assist him/her in assessing and controlling the risks associated with any Army mission or operation.

a. Risk management is embedded as a natural part of the military decision making process. FM 100-14 and Annex J of FM 101-5, present specifics on how this process is accomplished.

b. Used effectively, this process will identify the hazards (threats) for any given situation.

c. The staff will apply risk management when developing a course of action (COA) for the commander's approval. Commanders must require the integration of risk management by the staff during the decision making process, in the planning, coordinating and development of plans, orders, and operations for FP.

3-4. Weapons of Mass Destruction.

a. The threat of terrorist delivered WMD is real. The relative ease of acquisition and delivery of WMD, coupled with their potential terrorist use against U.S. forces (including family members and surrounding communities), dictate that commanders at all levels include the WMD threat into all FP plans and procedures.

b. While it is currently impossible to provide 100% around the clock protection to all personnel from a terrorist's use of WMD, commanders can take steps to lessen the effects of such an attack, and in many cases, avert an attack by conducting a thorough threat analysis and assessment coupled with active and passive protection measures.

c. Readiness is achieved once all assigned and attached personnel are aware of the WMD threat, are trained to Army standards in nuclear, biological and chemical (NBC) avoidance, protection, and decontamination IAW AR 350-41, and have exercised AT contingency plans which include a WMD threat. Exercises will include civilians, contractors, family members, and local first responder teams.

d. Plans, orders, standing operating procedures (SOPs), threat assessments, and coordination measures will address terrorist WMD threat. Units and individuals must be aware of the WMD threat and have practiced response procedures. Clear command, control, and communication lines will be established between local, state, and federal emergency assistance agencies, first responders, criminal investigation teams, and follow-on forces.

e. Successful consequence management after a terrorist WMD attack is highlighted by all personnel knowing exactly what their roles and responsibilities are during the attack, and executing them to defined standards. Consequence management ends when the force is able to continue its pre-attack mission without any residual or long-term degradation. Decontamination operations are complete when the area is cleaned to statutory standards, exposed personnel are returned to duty, normal unit functions are restored, an after action review has been completed, and all remedial action plans (RAP) are completed.

f. First-responders, security forces, and follow-on support personnel will be equipped with the proper types and quantities of chemical defense equipment (CDE). All individuals and teams will be trained on the proper use and maintenance of their CDE. Shortfalls and additional requirements are forwarded through command channels for resolution.

3-5. Force Protection Plan.

a. All installation commanders will prepare a FP Plan. At a minimum, the plan should cover the following areas:

(1) A current localized threat assessment.

(2) Clearly describe local protective and preventive measures to be initiated during periods of higher THREATCON. Identify forces or units required to implement measures.

(3) Prescribe appropriate actions for reporting threat information, responding to an attack, and reporting incidents.

(4) Coordination instructions on procedures to request support from and notify the Federal Bureau of Investigation (FBI), and state and local law enforcement agencies in the event of an incident. The plan will also contain instructions on providing support to

the FBI and, state and local law enforcement agencies when requested in response to an attack in the civil communities.

(5) Organization, training, equipment, and operational procedures for the SRT and other response forces.

(6) Exercise schedule for the plan certification.

(7) List latest internal and external FP vulnerability assessment results along with resourcing strategy required to address deficiencies. Clearly state when corrective action has been deferred and for how long it has been deferred.

b. All FP plans must be reviewed by the servicing SJA to ensure compliance with appropriate local, state, and federal laws and regulations.

c. Coordinate plans, procedures and changes in THREATCON levels with higher headquarters, tenant organization/activities, nearby communities, and appropriate local, state, and federal agencies.

d. Coordinate with local civil authorities on installation access, information systems support (to include requirements for emergency radios, systems, frequencies, with emergency and/or police/FBI support agencies) and installation operations which must be maintained during FP action operations, or during demonstrations on or off the installations which affect U.S. installations and facilities.

e. The installation PS plan, described in paragraph 4-2, and the FP plan serve the same purpose and should be combined as one document.

f. As an annex to the installation FPP, commanders will prepare installation-wide terrorist incident response plans. These plans will include procedures for determining the nature and scope of post-incidence response measures, and plans to reconstitute the installation's ability to perform AT/FP measures.

(1) Response plans should address the full scope of an installation's response to a terrorist incident. The nature of the response will depend on many factors. The character of operations underway at the time of the terrorist incident will have significant bearing on the scope, magnitude, and intensity of response.

(2) Response plans should include emergency response and disaster planning for installation engineering, communications, networks, information systems, security, logistics, medical, mass casualty response, transportation, personnel administration, and local support. Terrorist use of WMD or terrorist attacks on foreign dignitaries while visiting TRADOC installations will require immediate close coordination with this headquarters.

3-6. Force Protection Resources.

a. The downsizing of the DOD has placed pressure on every aspect of resource management. Resources provided for base operations have been particularly austere and have required intensive management. FP and security resources are not fenced and may be reprogrammed at the commanders discretion to fund other installation requirements. This places installations in a position to accept a higher level of vulnerability to terrorist or criminal attack. Recent events indicate accepting higher levels of vulnerability to terrorist or criminal attack, in order to fund other priorities, is not always a prudent course of action.

b. Identifying FP requirements.

(1) On an annual basis, installation level program managers will develop and prioritize a list of resource requirements to be funded under the MDEPs for PS equipment (PSE) (RJC6) and AT (VTER). The program should address prioritized requirements through the next five fiscal years and include statements of justification. These programs should be closely integrated with the overall command level program for information systems security (ISS) to insure continuity and coherent objectivity of both of these critical programs.

(2) The respective installation program managers will provide the resource requirements to the designated TRADOC program manager. The TRADOC program manager will review and validate program requirements. Validated requirements will be submitted to HQDA for funding consideration.

c. Funding provided in the following MDEPs are designed to improve the PS of TRADOC installations and facilities or protect

mission essential information that might be used to plan a terrorist attack.

(1) The MDEP VTER AT protects personnel, facilities, and equipment from terrorist/criminal threats. AT programs consist primarily of FP, training, and operations. Programs directly support unit readiness and deployments by reducing unit and installation vulnerability during higher levels of threat. The goal is to provide security to units, families, and facilities; and reduce the number of deployable soldiers used for FP missions during mobilization and deployment. Examples of VTER Other Procurement, Army (OPA) (over $100,000) force protection equipment (FPE) purchases include:

(a) Closed circuit televisions (CCTV).

(b) Intrusion detection systems/access control systems.

(c) Radio communication equipment.

(d) Explosive detectors.

(e) Portable barriers, fencing, and lighting.

(f) Security upgrades/hardening of mission essential vulnerable areas (MEVAs), general officer (GO) quarters, and emergency operation centers.

(g) Van and peripheral equipment for the SRT.

(h) Riot control equipment.

(2) The MDEP VTER Operation and Maintenance, Army (OMA) funds FPE, communications systems, and training requirements under $100,000.

(3) The MDEP RJC6 OPA funds PSE design, research and development, test and evaluation, procurement, installation, and maintenance of select PS equipment and systems (to include intrusion detection systems and alarm monitoring systems). PS systems enhance security for nuclear and chemical storage facilities, sensitive AA&E storage, mission essential and critical facilities, and equipment and personnel protecting against terrorism, espionage, and theft. Examples of RJC6 supported expenditures are:

(a) Intrusion detection systems.

(b) Sensors and entry control systems.

(c) Alarm displays.

(d) Monitors.

(e) CCTV.

(f) Mobile detection assessment response system (MDARS).

Chapter 4
Physical Security

4-1. General.

a. PS is an integral part of the FPP. Its objective is to provide protection from terrorist and other criminals, disaffected persons, hostile intelligence, paramilitary forces, protesters, and saboteurs. PS is designed to deter, detect, and defend against all of the above threats. PS employs physical measures such as fences, lights, cameras, blast walls, vehicle barriers and alarm systems; and procedural measures such as security checks, training and awareness programs, property accountability/inventory requirements, PS inspections (PSIs) of MEVA and PS surveys of installations.

b. A successful PS program (PSP) cannot be achieved without active teamwork, cooperative efforts of every entity of the commander's installation staff, and appropriate command emphasis. PS must be a priority issue within the command and an active part of the command's FPP.

c. Commanders will continuously review and evaluate daily PS measures under THREATCON normal for their applicability and ease of transition to FP requirements under increased THREATCONs.

4-2. Physical Security Plan.

a. Installation commanders are required to develop and maintain an installation PS plan. Developing the plan requires extensive coordination and liaison between all installation activities and tenant units and lateral federal and state agencies.

b. The PS plan will be developed per AR 190-13 and FM 19-30. Annexes will include: installation threat statement, AT plan, bomb threat plan, installation closure plan, natural disaster plan, civil disturbance plan, resource

plan, communications plan, designated restricted areas, and list of installation MEVAs with required PS measures.

c. The PS plan will be an integral part of the FP plan described in paragraph 3-5.

4-3. Threat.

a. Commanders will prepare and maintain a PS vulnerability assessment for installations and activities. The assessment will address the broad range of physical threat to the security of personnel, facilities, and installations.

(1) It is expected that PS vulnerability assessment will occur at the installation level. These assessments should consider a wide range of identified and projected threats against a specific location or installations personnel, facilities and other assets.

(2) The assessment should identify vulnerabilities and propose suggestions for enhanced protection for personnel and resources against such attacks.

b. Essential to the PSP is a continuous analysis of the local threat. Security planning and measures to be implemented will be based on this threat assessment.

(1) Ideally, upon request, the local FBI field office and other local law enforcement agencies will provide periodic intelligence to the installation commander. The installation provost marshal (PM) is a key player in the installation commanders FP mission and is the focal point for receipt of domestic threat information from domestic law enforcement agencies. The PM is the conduit for domestic threat information flow between the FBI and the installation commander. Normally, the PM must initiate a request for intelligence information from these outside agencies to formulate a "local threat analysis."

(2) Information received may be current or perceived. A serious detriment to a security program is to assume there is no threat because nothing has ever occurred.

4-4. Risk analysis.

a. Not all Army assets at all locations require the same degree of protection. The risk analysis allows the commander to prioritize assets so that PS resources can be applied in the most efficient and cost effective manner possible. Risk indicates both the impact of the compromise of an asset and the potential for it being compromised. Risk is associated with individual assets and with different types of aggressors or threats.

b. Risk analysis will be conducted on all MEVAs. Risk analysis will be conducted when:

(1) A unit or activity is activated.

(2) A unit permanently relocates.

(3) Every 3 years (if no prior record of risk analysis exists).

(4) During planning stages for a new, addition to, or renovation of facility.

(5) An incident occurs in which assets are compromised.

c. Risk analysis is a joint endeavor between the using unit or activity and the installation PS officer, or equivalent security officer, or their representative.

d. Risk concerns assets rather than facilities. Risk is composed of two factors: severity and likelihood of aggressor activity. Aggressors consist of criminals, protesters, terrorists, and any other threat which may impact the use or availability of that asset.

e. The risk analysis procedure is performed in six steps:

(1) Identify the unit.

(2) Identify the asset.

(3) Determine asset value.

(4) Determine likelihood of aggressor activity.

(5) Determine the risk levels for assets.

(6) Determine required protective measures.

4-5. Physical security survey.

a. In accordance with AR 190-13 and DA Pamphlet 190-51, DA Form 2806-R (PS Survey Report) is a formal recorded assessment of the overall security posture of an installation's PSP. Several physical and procedural security measures are evaluated during the survey. Installations and/or facilities will be surveyed

based upon varying criteria. Those installations storing conventional AA&E will be surveyed every 18 months. Only trained PS personnel should conduct a PS survey. Commanders are required to program resources to correct deficiencies noted during the survey. The installation PM or security officer will reassess the installation's PS posture based on:

(1) Risk analysis per DA Pam 190-51.

(2) Mission.

(3) Threat (known and/or perceived).

(4) Findings of the survey.

(5) Previously conducted surveys and inspections.

(6) MEVA protection requirements.

(7) Availability of resources.

(8) Electronic security systems.

(9) Site enhancements and/or new construction.

b. Results of an installation PS survey will be used to develop a resource plan with recommended prioritized allocation of resources. The resource plan is included in the installation's PS plan.

4-6. Electronic Security Systems (ESS).

a. ESS, if effectively utilized, decreases and eliminates the requirement for guards. The Joint Services Interior Intrusion Detection System (J-SIIDS) and the Integrated Commercial Intrusion Detection System (ICIDS) are the DOD standard intrusion detection systems (IDS). Initial issue of these systems are not charged to the installation. Repair or replacement parts/components are chargeable to the installation. Commercial intrusion detection systems (CIDS) are funded under the MDEP RJC6 and purchased by the installation. ICIDS are a DOD/DA program which updates existing installation IDS. ICIDS can interface with existing J-SIIDS and CIDS. ICIDS is designed to monitor over 300 protected areas (zones). The alarm monitor group (AMG) is a computerization of the J-SIIDS monitors. The AMG is designed to interface with J-SIIDS.

b. Installations are responsible for conducting pre-installation site surveys for IDS. All government-owned IDS maintenance and repairs are the responsibility of the installation Directorate of Logistics (DOL) or Public Works (DPW). The installation Directorate of Contracting (DOC) is responsible for obtaining contract maintenance services for IDS. The IDS, when installed, is classified as "personal property, equipment in place" and will be accountable by the using unit or activity.

c. CCTV should only be installed for interface with existing or planned IDS as an assessment device. CCTV should not be solely installed for surveillance purposes.

d. Commanders must forecast J-SIIDS and/or CIDS requirements 5 years in advance of desired installation. Failure to identify and properly justify IDS requirements will result in non-availability of IDS resources.

e. Technical assistance regarding site surveys, contracts, design, installation, and maintenance of IDS can be obtained from the Chief of Engineers (COE), Huntsville Center of Expertise for Intrusion Detection Systems (IDS-MCX), Huntsville, Alabama, or the PS Equipment Management Office (PSEMO), Fort Belvoir, VA.

4-7. Structural Design.

a. Commanders must ensure every aspect of PS structural design is incorporated into the initial planning or renovation of facilities. PS officers are required to authenticate all DD Form 1391s (Military Construction Project Data) certifying that PS considerations have been thoroughly reviewed and are integrated into the proposed construction as applicable. The PS officer should maintain close liaison with installation engineers for early coordination of proposed new construction projects. The PS officer should be an active voting member on the installation planning board.

b. AA&E must be properly stored in certified storage facilities as prescribed in AR 190-11. DPW must certify the structural standards of the storage facility utilizing DA Form 4604-R, Security Construction Statement. A re-certification is required when:

(1) A new facility is built.

(2) No prior record of certification exists.

(3) A change in unit occupancy occurs.

(4) Any modifications have occurred to the structure or the IDS.

(5) Any incident of actual or suspected compromise to the facility has occurred.

(6) Five years have passed since the last certification.

c. An engineer is required to authenticate the DA Form 4604-R.

d. Commanders are encouraged to consider additional structural security measures for soft targets within his/her area of responsibility based on the threat and vulnerability of these facilities. Guidance and information for enhanced structural measures can be found in the United States Army Corps of Engineers (USACE) Security Engineering Manual.

4-8. Perimeter barriers. Where property requires fencing as a protective measure, the type and quantity of fencing will meet the requirements of USACEs specifications. Other barriers such as bollards, walls, gates, berms, will be constructed and installed to provide the maximum protection needed for the risk level associated with targeted assets. All barriers must have and maintain an adequate clear-zone to counter any attempted breech. Barriers will be forecast in the MDEP VTER as needed.

4-9. Access controls.

a. Commanders are required to designate areas or facilities subject to special restrictions or control for security reasons or to safeguard property or material. The type depends on the nature and varying degree of significance, from a security standpoint, of the security interest or other matter contained therein. The three types, or levels, of restricted areas used are:

(1) Exclusion area; only those personnel required to have access.

(2) Limited area; personnel may have access with an authorized escort.

(3) Controlled area; personnel may have unescorted access.

b. A limited access installation or activity may be designated under specific criteria:

(1) No perimeter fence exists, but entry can be temporarily closed to vehicular traffic.

(2) Permanent barriers exist and access is controlled only after normal duty hours (i.e., gates are secured or manned after dark, or no permanent barriers exist, but vehicular traffic and other movements using roads and other points of entry are continuously controlled).

4-10. Inspections.

a. Commanders will designate facilities which are considered MEVA. IAW AR 190-13 and FM 19-30, commanders will have all MEVAs formally inspected. DA Form 2806-1-R (PS Inspection Report) is the formal, recorded assessment of PS procedures and measures implemented to protect assets. A PSI is required when:

(1) A MEVA is activated.

(2) No record exists of a previous inspection.

(3) A change in unit or activity impacts on the current PS plan.

(4) There is an indication or reported incident of significant or recurring criminal activity.

(5) 18 months have passed since the previous PSI for, conventional AA&E, critical ADP service center activities.

(6) The commander determines greater frequency is needed.

b. Checklists may be adapted for use by commanders to support a pro-active security program.

c. Deficiencies noted during the inspection may be correctable on-site during the inspection. Findings that are beyond the capability of the local commander because of a lack of resources will be reported to the next higher commander with a request for resource assistance, which includes a justification and impact statement.

d. PSIs and surveys are intended to ensure commanders can sustain the highest degree of capability and readiness to meet mission requirements. Lack of pro-active PS checks and balances will severely impact on

the ability of commanders to properly account for and secure their critical warfighting assets.

4-11. Transportation.

a. Loss or theft of sensitive items of the Army's critical warfighting assets can severely impact a unit's wartime mission capability. Significant losses and theft of sensitive items, ammunition, and weapons during shipments and unit movements occur due to noncompliance with regulatory guidance pertaining to security and accountability of property, failure to establish and maintain security and accountability discipline throughout unit movements, and acts by criminal opportunists.

b. Unit personnel should coordinate all installation shipments prior to movement with their transportation, PM, and logistics points of contact. The following items will assist units and transport managers during deployments and routine shipments.

(1) PS plans for property movement should be established during initial preparation for deployment. Plans should provide for security of government property from the originating installation to the port of debarkation. PM and transportation personnel should also assist in the development of redeployment security.

(2) Sensitive, high-dollar value equipment, (night vision devices, communications and electronics equipment, tool kits, etc.) will not be stored in vehicles being shipped. These items should be secured in locked unit containers with equipment of comparable value and sensitivity and accounted for IAW established supply procedures.

(3) Units should coordinate with security and transportation personnel to determine the transportation security requirements for the type of equipment being shipped. If at any time the security risk increases, use of supplemental security measures, such as unit guards, is encouraged.

(4) AA&E shipped via rail flat car will be placed in locked milvans or conex containers. The door to the container should be blocked or made inaccessible to preclude entry. To accomplish this, the container should be positioned on the flat car so the door is flush against an immovable object and door-to-door if more than one container is utilized. If needed, negotiate with the carrier through the Military Traffic Management Command (MTMC) to place an empty container on the rail car to preclude leaving a full container vulnerable.

(5) Units should consider numbering locks and keys and identifying which vehicle is secured by the respective lock. An additional set of keys should be sent with unit personnel during shipment for use at debarkation points. This will eliminate equipment and vehicles arriving at the destination point without keys, thus causing the cutting of locks in order to unload items.

(6) Units must initiate inventories of equipment being shipped in vehicles and/or shipping containers to include, as a minimum, serial numbers, nomenclature, and quantity. A copy of the inventory should be maintained in unit files and a copy placed in the vehicle or shipping container.

(7) Units must ensure the provisions of AR 190-11 are adhered to during movement. Commanders should ensure coordination is effected with their PM and transportation offices for assistance and security guidance prior to movement. AA&E must be specifically accounted for and properly secured during shipment. Accurate accountability records, to include shipping information, must be kept by the shipping unit.

(8) Upon discovery of a loss of government property, units should ensure law enforcement personnel are notified immediately. Early incident reporting not only enhances investigative activity, but provides dissemination of crime conducive conditions, modus operandi, system irregularities, and associated lessons learned.

Chapter 5
Information Security (INFOSEC)

5-1. General. INFOSEC, as one of the components of FP, encompasses continuous military operations that protect the security of information systems. The threat to Army information and information systems (INFOSYS) falls into two general categories: unintentional and intentional.

a. The unintentional threat usually stems from ignorance as a result of poorly trained INFOSYS administrators, operators and maintainers; from accidental damage to

storage media; or from improper application of security access protection procedures.

b. The intentional threat involves deliberate, overt or covert acts against the INFOSYS, among which are the physical threat to tangible property and the threat of electronic, radio frequency or computer-based attacks on the information or communications components that control or make up critical Army command and control (C2) infrastructures. The intentional threats come from a range of sources: unauthorized users, insiders, terrorists, non-state and state-sponsored groups, hostile intelligence/military organizations and political/religious opponents. In most cases, the target of the threat is the information itself, rather than the system that transports it.

(1) Unauthorized users such as hackers are the source of most of today's attacks, primarily against personal computers. The threat they pose to Army INFOSYS networks and mainframe computers is growing.

(2) Insiders. Individuals with legitimate access to an INFOSYS pose one of the most difficult threats from which to defend. Whether recruited or self-motivated, the Army INFOSYS insider has access to systems normally protected by ISS against attack.

(3) Terrorists. In the past, in order to gain access to, or collect intelligence on, a target, terrorist may have had to climb a security fence or pass through a locked door. Today, this same terrorist can gain access by entering through a computer network. Although his presence would be virtual, the damage he could do could be equal or greater than that achieved by traditional intrusions. Thus, while traditional means are still needed to protect unwanted access to information, the Information Age has added a new dimension of concern for the commander, and new opportunities for threat elements.

(4) Non-State. In many scenarios, it is extremely difficult to identify any national sponsorship of an activist threat, no matter how positive the appearance of affiliation or the existent level of conflict, if any. Since it is already apparent that activists of all persuasions are taking advantage of the possibilities offered by the Information Age, there is no reason to suspect that the Army's INFOSYS will be immune from a non-sponsored adversary's interest in disturbing U.S. military information or communications infrastructures. The easy availability of low-cost technological capabilities, coupled with the universal span of today's automated information webs, intensifies the likelihood that there are potential INFOSYS adversaries of the known, suspected or unknown variety seeking penetration opportunities.

(5) Hostile Intelligence/Military. We can be assured that nationally-sponsored hostile intelligence services (HIS), either civil or military, are active over the entire spectrum of conflict. In peacetime, they are more likely to be targeted against U.S. commercial and scientific networks than military information infrastructures. Yet, with little additional resource expenditure, a dissident's peacetime intrusiveness could easily be refocused on Army INFOSYS using the entire range of assets in the portfolio of threats.

(6) Political/Religious. The geopolitical landscape of today is often difficult to navigate, crowded as it with splintered ideologies of religious extremism and political radicalism (or a combination thereof) harboring a wide range of grievances against the U.S. and its allies. We can expect that religious and/or political animosities would be most virulent during open conflict; however, to gain public recognition, an attempt to cripple any element of our information infrastructure, including the Army's INFOSYS, might be an incentive worthy of adversary consideration.

c. The natural threat phenomena (fire, flooding, severe weather and other natural disasters) can cause severe damage to INFOSYS. Threats in this category are most easily identified with, but are not limited to, fixed and garrison facilities, and must be given serious consideration, particularly in CONUS, because of the reliance on CONUS-based INFOSYS to support and sustain the force-at-large.

5-2. Information Systems Security Program (ISSP).

a. Define and develop C2 protect personnel and staffing procedures.

(1) Appoint an Information System Security Manager (ISSM) at each installation.

(2) Appoint an Information System Security Officer (ISSO) for each automated information system (AIS) or group.

(3) Appoint a Network Security Officer (NSO) for each identified network.

(4) Appoint a Terminal Area Security Officer (TASO) for each terminal or group of terminals not under the control of an ISSO or NSO.

b. Implement definitive C2 protect tactics, techniques, and procedures which will develop information operations (IO) SOPs to detect and deny unauthorized intrusion.

c. Ensure that C2 protect common tools are integrated into designated echelons for management, detection, protection and reaction to C2 system vulnerabilities.

d. Develop management methodology, IAW AR 380-19, to evaluate risks associated with the operations of information systems.

e. Develop and implement the C2 protect Training Management Plan that articulates the overarching direction for C2 protect education and training in the Army.

(1) Identify and include specific training requirements, source(s) of training for computer security education and awareness.

(2) Formal security training must be included in IDPs annually for security and systems administrator and network managers.

f. Develop an operations security program that protects friendly C2 capability against adversarial attacks.

Chapter 6
Protective Services

6-1. General. Protective service operations are the commander's primary means of protecting high risk personnel. The mission of protective services is to protect the principal from assassination, kidnapping, injury, and embarrassment. Protective service operations will be conducted IAW U.S. laws and regulations and international agreements to which the U.S. is a party.

6-2. High Risk Personnel (HRP).

a. HRP security supports the Army FPP by providing additional security to designated individuals who by virtue of their rank, assignment, symbolic value, vulnerabilities, location, or specific threat are at a greater risk than the general population. HRP security consists of:

(1) Formal identification and designation of eligible individuals;

(2) U.S. Army Criminal Investigation Command (CID) Special Agents performing personal security vulnerability assessments (PSVA) for HRP.

(3) Hardened car support and domicile to duty authorization.

(4) Special training for HRP, their family members, and selected support personnel such as drivers.

b. There are two categories of HRP:

(1) HRP Level 1 (HRP1) personnel have such a significantly high potential as terrorist or criminal targets as to warrant assignment of full-time protective services. This would include long-term protective services based on assignment location, or short-term protective service based on a specific threat.

(2) HRP Level 2 (HRP2) personnel do not warrant assignment of full-time protective services but require such additional office, residential, and travel security measures as deemed appropriate based on local conditions. Installation commanders are authorized to designate installation personnel as HRP2.

c. HRP and their family members must be aware of risks and trained in personal protective measures they can apply. Additionally, support staff such as drivers, aides, and protective services details must be trained and properly equipped.

6-3. Protective service detail. The objectives of the protective service detail are:

a. Deter possible harm to the principal through protective service operations.

b. Detect threatening situations affecting the personal safety and security of the principal.

c. Defend the principal from physical harm or embarrassing situations.

d. Quickly and safely remove the principal from the threatening environment to a more secure location.

Chapter 7
Law Enforcement

7-1. General.

a. Maintaining readiness is critical to the Army. Unit readiness rests on the morale, discipline, and training of its soldiers. It rests equally on having soldiers and their families feel confident about quality of life in the Army community. Our soldiers and their families must have a safe and secure environment in which to live, work, and train. The military police (MP) accept that challenge daily.

b. LE is a vital component of an effective FP program. The installation Provost Marshal (PM) is a key player in the commander's FP mission and is the focal point for receipt of domestic terrorist threat information from domestic LE agencies.

c. The discussion below highlights the important elements of an installation LE program.

7-2. Military Police Management Information System (MPMIS). Provides automated tool for MP records management. Reduces administrative burden on PM staff. Increases awareness of problem areas by management of crime information. MPMIS applications available for use are the Offense Reporting System (ORS-2), Correctional Reporting System (CRS-3), Security Management System (SMS), Registration and Access Control (RACS), and Prisoner of War Information System (PWIS-3). ORS-2 will also become the feeder system for the mandated National Incident Based Reporting System (NIBRS).

7-3. Law enforcement patrols. MP practice preventive patrolling. Preventive patrolling places a uniformed patrol in the right place at the right time. It has as its major feature the protection of people, not property. The primary emphasis of preventive patrolling is having uniformed patrols work areas where analysis shows many people gather at times when the likelihood of crime is greatest. Emphasis is placed on establishments such as the post exchange, commissary, package beverage store, hospital (during evening shift changes), banks, gas stations, and recreational facilities. Patrol requirements are established by the installation commander on the advise of the PM. The PM uses crime analysis and a FP threat assessment to determine patrol requirements. The MP on patrol works for positive community relations. Public cooperation and understanding benefit both the community and the MP.

7-4. Traffic control. The objective of military traffic control is to attain the maximum safe flow of vehicles, with minimum control and direction. The PM has the following responsibilities:

a. Prepare plans, policies, and procedures for traffic control.

b. Prepare the traffic control plan.

c. Coordinate traffic control activities with other headquarters, staff offices, and civil authorities.

d. Provide timely information to commanders about MP assistance they may expect during road movements.

e. Implement plans and policies concerning traffic accident investigation and prevention.

f. Implement traffic control studies and surveys.

g. Implement necessary traffic enforcement programs.

h. Assist in implementing traffic education/safety programs.

i. Supervise circulation control activities in a tactical environment.

7-5. Special Reaction Team (SRT). A SRT is a specially trained and equipped team of military and civilian security personnel, serving as the installation commander's principal response force in the event of a major disruption of a threat situation on the installation. The SRT will be deployed to preserve human life and restore normal activity on the installation. Select member(s) of SRT will attend the protective services detail training.

7-6. Military Working Dogs (MWD). Like other highly specialized items of equipment, MWDs complement and enhance the capabilities of the MP. When used by existing MP organizations, MWD teams enable the MP to perform their mission more effectively and in many cases, with significant savings of manpower, time, and money. The MWD team also provides a strong psychological deterrent

to potential offenders. The MWDs unique capabilities are used by the MP to:

a. Secure installation and property.

b. Help enforce military laws and regulations.

c. Detect explosives and drugs.

d. Increase the effectiveness of the combat support provided by the MPs.

7-7. Community oriented policing (COP). The concept of COP seeks to increase interaction between police and citizens to improve public safety and quality of life in the community. Community partnership and problem solving, the two core components of COP, can be accomplished in a variety of ways. The means selected should fit the installation's needs and resources. An effective COP program is designed to reduce crime by stimulating appropriate crime prevention attitudes, procedures ,and behavior; protecting potential victims or property from criminal activities by anticipating crime possibilities and eliminating or reducing opportunities for the acts to occur; and discouraging potential offenders from committing criminal acts. Although not all inclusive, the following are some elements of an effective COP program:

a. Crime Hot Lines.

b. Publicity campaigns.

c. Residential security surveys.

d. Juvenile crime prevention programs.

e. Neighborhood Watch program.

f. Operation Identification program.

g. Neighborhood Walk program.

h. Project Lock campaigns.

i. Helping Hand program.

j. Drug Abuse and Resistance Education (DARE) program.

k. Incentive based crime reporting system.

l. MP participation at Town Hall meetings.

m. MP participation at installation Newcomers briefings.

n. MP participation at new CDR/1SG orientations.

o. MP bicycle patrols.

p. Housing area MP sub-stations.

7-8. Violence in the workplace. The Center for Disease Control has identified that homicide in the workplace is reaching epidemic proportions. In 1994, violence was the third cause of workplace deaths, and the number one reason for occupational injury deaths of women. Prevention programs should focus on risk management, awareness, education, stress and stress indicators. A leader's interpersonal and professional skills are important in recognizing and taking appropriate action on potential offenders.

Chapter 8
Antiterrorism (AT)

8-1. General. Terrorism is characterized as the unlawful use of violence or threat of violence to coerce or intimidate a government or a society. Protection against the terrorist threat requires both an offensive counterterrorism (CT) capability and a defensive AT program. CT requires special expertise and extensive training of elite units, and basic AT measures can be learned and implemented by virtually anyone.

8-2. Terrorist threat. The terrorist threat to TRADOC is real, varied, and not clearly understood. Defining the enemy is the first step toward identifying the threat.

a. Domestic terrorism, involving groups or individuals whose activities are directed at elements of our government or population without foreign direction.

b. International terrorism, involving groups or individuals whose activities are foreign-based, and/or directed by countries or groups outside the U.S., or whose activities transcend national boundaries.

c. Extremist groups are organizations that espouse supremacist causes, foster discrimination based on race, creed, color, gender, religion, or national origin, and advocate the use of force or violence, or otherwise engage in efforts to deprive individuals of their civil rights.

d. Terrorist threats can be assumed to be directed against communications and information management systems, to include both known and unknown (recognized and unrecognized) attacks against those systems. Appropriate measures for safeguarding such information and communications systems must also be addressed by the plan.

e. The Federal Bureau of Investigation (FBI) has requested the establishment of a single point of contact common to all installations to whom domestic terrorist threat information may be disseminated. The PM is the conduit for domestic terrorist threat information flow between the FBI and the installation commander. The PM is responsible for the receipt of information and notifying the commander of the information. Information regarding potential terrorist threats involving CONUS Army installations will be passed from FBI field offices or special agent to the installation PM. Should military intelligence or USACIDC intelligence gathering assets obtain information of domestic terrorist nature, this information should be relayed to the respective installation PM.

8-3. DOD Terrorist Threat Level. The DOD terrorist threat level classification system identifies the terrorist threat in a specific overseas country.

a. The DOD terrorist threat level classification system is a set of standardized terms used to quantify the level of terrorist threat on a country-by-country basis. The threat level terms are negligible, low, medium, high, and critical. The system evaluates the threat using the following threat analysis factors: existence of a terrorist threat, history, capability, intentions, targeting, and security environment.

b. The Defense Intelligence Agency (DIA) sets a general terrorist threat level identifying the potential risk to U.S. personnel in a particular country. Threat levels are estimates, with no direct relationship to specific THREATCONS. Threat levels should not be confused with threat conditions.

8-4. Terrorist Threat Condition System.

a. The terrorist THREATCON system describes the progressive level of protective measures implemented by all DOD components in response to terrorist threats.

b. There are five THREATCON levels. The circumstances under which and the purposes of each protective posture are prescribed in appendix F.

c. Declaration of THREATCONs is the prerogative of the installation commander. As a general rule, installations will adopt terrorist threat measures consistent with the THREATCON declared by the MACOM.

d. Specific THREATCON measures appropriate for installations and airfields are included in appendix F. Local commanders retain authority to implement terrorist threat measures (THREATCON measures) to defend against a greater than expected terrorist threat. Local commanders will not implement measures less rigorous than those appropriate for declared THREATCON level for their particular facility.

8-5. Antiterrorism Program. An AT program is no different from any other military operation. Leaders must be constantly cognizant of the threat unique to their unit or facility and know what resources they have available to protect their people and material.

a. Identifying the potential terrorist threats to personnel and assets is the first step in developing an effective AT/FP program. Once commanders understand the threat they can assess their ability to prevent, survive, and respond to an attack.

b. Installation commanders will prepare a terrorist threat assessment for their area of responsibility. The TRADOC Installation Threat Modeling Workbook is a valuable tool for installation FPC in assessing possible threat scenarios in a Low threat environment.

(1) The terrorist threat assessment is the tool which commanders use to arrive at a judgment of risk and consequences of terrorist attack.

(2) Integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Information systems which include both telecommunications and other network systems are also targets of opportunity or desire for terrorist threat or attack. As such, they should be included in the overall assessment by each commander.

(3) The pattern of terrorist surveillance, targeting and planning is best recognized through sharing of information. These efforts should include the chain of command and the interagency process at the appropriate level.

(4) Coordinate with appropriate government agencies. This ensures awareness of terrorist threat information available through agencies such as the FBI and local law enforcement.

(5) Terrorist threat assessments should be the basis and justification for recommendations on force protection enhancements and program/budget requests.

c. Develop a process, based on terrorist threat information and/or guidance from higher headquarters, to raise or lower THREATCON levels.

d. Develop measures or actions for each THREATCON level as the threat situation increases from THREATCON Normal to THREATCON Delta. Maintain a full-time capability to report and rapidly disseminate time sensitive indications and warnings concerning possible terrorist threats to personnel and facilities.

e. Integrate the risk management system of logical steps to balance resource restraints with the risk of terrorism.

f. Establish and rehearse procedures for responding to a terrorist attack. AT training ranges from extremely sophisticated programs for the response teams to simple effective instruction for family members. Aim local training emphasis at the entire organization and its members' families.

g. A Terrorist Incident Report (TIR) will be submitted when a terrorist incident or suspected terrorist incident occurs. Initial TIRs will be provided telephonically to the following within two hours of the incident:

(1) Army Operations Center (AOC), DSN 225-8491/2, commercial (703) 695-8491/2.

(2) TRADOC Emergency Operations Center (EOC), DSN 680-2256, commercial (757) 727-2256.

h. A TIR in message text format by IMMEDIATE precedence electrical message to HQDA (Msg address: DA WASH DC//DAMO-AOC/DAMO-ODL-FP/DAMO-ODO/DAMI-CIC//), CID Command (CDR USACIDC WASH DC//CIOP-IA//), INSCOM (CDR INSCOM FT BELVOIR VA//IAOPS-IS//); AND TRADOC (CDR TRADOC FT MONROE VA//ATBO-J/ATCS-EOC/ATIN-S. Facsimile number for HQDA is DSN 223-6580 or commercial (703) 693-6580.

i. If credible threat information concerning a planned terrorist attack against U.S. Army personnel, facilities, or other assets is developed, a Terrorist Threat Report (TTR) will be submitted.

j. The Security Officer will determine proper local reporting channels for TTR. If attack is imminent, installation is required to transmit a FLASH precedence electrical message directly to HQDA , CDR INSCOM, and this headquarters. If attack is not imminent, the report will be sent by IMMEDIATE precedence message with four hours of receipt of information.

Chapter 9
Training

9-1. General.

a. TRADOC commanders ensure that FP training and awareness is emphasized at all levels.

(1) Selected personnel appointed to the FPC or fusion cell should be trained at the Combating Terrorism on Military Installations Course (7H-F13/830-F17).

(2) GO and HRP personnel will attend Evasive Driving for Senior Officers and Select Personnel Course (1A-F3).

(3) Drivers will attend Evasive Driving for General Officer Drivers Course (7H-F23/830-F16).

(4) Personnel assigned to the SRT will satisfactorily complete training at Special Reaction Team Training Course (Phase I) (7H-F17/830-F12). Sharpshooters will satisfactorily complete the Phase II Marksman/ Observer Training Course (7H-F17/830-F12).

b. Units must incorporate FP training in their daily activities and operations. In addition, added emphasis is required before and during deployments outside CONUS and during times of increased threat. Ensure training exercises include scenarios that

incorporate terrorist threats and attacks. Exercise scenarios will also incorporate THREATCONs.

c. Ensure DOD personnel deploying outside of the 50 U.S. receive focused training on combating terrorism and FP prior to deployment. These personnel include individual soldiers deploying as part of a unit, as an individual staff augmentee or unit filler, or on temporary duty (TDY), DA civilians traveling outside of the 50 U.S. for TDY, and family members. Commanders should certify collective unit FP training programs prior to OCONUS deployment.

d. Ensure training is provided to enhance travel security of individuals while enroute to foreign destination. The gaining command will be responsible for providing more detailed training when soldier or DA civilian arrives. Provide soldiers and DA civilians scheduled for an outside the 50 U.S. permanent change of station (PCS), a tailored threat awareness briefing. The briefing will focus on the soldier's mode of travel and hotel security tips relevant to the gaining command. Family members traveling with a soldier or DA civilian for an outside of the 50 U.S. PCS will be offered the opportunity to attend the threat awareness briefing received by the soldier or DA civilian.

9-2. Level I training. The objective is to provide individual awareness training to soldiers, DA civilians and family members deploying or traveling on government orders outside of the 50 U.S. Training must be accomplished within six months prior to deployment/travel date. Level I consists of two categories: (1) training required for deployment/travel to negligible/low threat areas and (2) training required for deployment/travel to medium/high threat areas.

a. Minimum training requirements for travel to negligible/low threat are viewing the FP/AT Level I video, receipt of a self help handbook and individual protective measures pocket size folding card. Level I (negligible/low threat area) training does not require a Level II qualified instructor to present the required training.

(1) TVT 19-79, Introduction to Terrorism.

(2) TVT 19-125, Self Protection Measures Against Terrorist, parts 1 & 2.

(3) TVT 19-81, Surveillance Detection.

(4) GTA 21-3-11, Individual Protective Measures.

(5) GTA 19-4-3, Individual Protective Measures To Combat Terrorism or JS Guide 5260, Service Members Personal Protection Guide: A Self-help Handbook to Combating Terrorism.

b. Level I minimum training standards for deployment to medium or higher threat areas are as follows:

(1) Same requirements as Level I negligible/low threat areas (video, guide, folding card, and AOR update) and

(2) instruction by a qualified instructor using the approved lesson plans. The approved lesson plans are those from module A: FP Level I Training, developed by United States Army Military Police School (USAMPS). A minimum of 3 training hours should be presented from the 11 hours of training material provided by USAMPS.

(3) A qualified instructor is: an individual who has completed Level II training; or, an individual who has received formal training in AT individual protection. Colonel (O-6) level commander is lowest level authorized to designate qualified instructors of those who have not completed Level II training. FP Level I lesson plans may be obtained by providing a letter request, signed by the Colonel (O-6) commander to:

Commandant USAMPS
ATTN ATZN MP TD
Ft McClellan AL 36205-5030

c. Installation Military Personnel Division ensure all soldiers and family members traveling to negligible/low, medium/high and potential physical threat countries (PCS, deployments or rotations) attend the appropriate level threat briefings and receive information of individual protective measures prior to initiation of travel.

d. Unit commanders will ensure all soldiers on TDY receive the appropriate level threat briefings and information of individual protective measures prior to initiation of travel, IAW the regulation and AR 55-46

(Travel Overseas) and AR 600-8-10 (Leave and Passes).

9-3. Level II training. The objective of level II training is twofold. First objective is to provide trained AT/FP unit advisors/subject matter expert to the unit commanders. Second objective is to provide trained personnel to serve as qualified AT/FP instructors at unit level. Target audience is Staff Sergeant (E-6) through Major (O-4) and warrant officer at battalion level and above. A formal training course entitled "The Force Protection Unit Advisors Course" developed by USAMPS satisfies the Level II training requirement.

9-4. Level III training. Level III training targets Lieutenant Colonel (0-5) and Colonel (0-6) students in precommand (PCC) training courses. Instruction is designed to provide commanders with knowledge, skills, and abilities necessary to apply FP components to ensure unit combat power preservation.

9-5. Level IV training. Level IV is an executive level seminar providing focused updates, detailed briefings, and panel discussions. Seminar will include a tabletop AT/FP wargame focusing on AT, intelligence, THREATCON management and implementation of FP/AT actions. Target audience is Colonel (O-6) to Major General (O-8) commanders/personnel, selected by service/CINC/DOD agency who have responsibilities for FP/AT policy, planning, and execution.

Chapter 10
Medical Response

10-1. General. Although not specifically mentioned in the definition of FP, the role of the medical function in the overall FPP is to provide an immediate medical response to reduce the severity and number of casualties resulting from threat entity use of WMD, NBC, directed-energy weapons, and conventional munitions. This is achieved through a well planned, coordinated, flexible, and effective Medical Response and Consequence Management Program.

10-2. Medical Response and Consequence Management Program. DHS must play an active role in FP. DHS must integrate the Medical Response and Consequence Program into the FPP and validate the program's effectiveness through regularly scheduled MASCAL exercises and command and staff simulations. DHS must ensure medical personnel are well trained to perform the medical response mission through the use of Emergency Medical Response Teams (EMRTs).

10-3. Preventive medicine threats. DHS will ensure the preventive medicine threats are addressed (i.e., protection from and education on insects/rodents which carry diseases; weather related injuries - heat/cold/wind/humidity; unsafe/contaminated food/water) and communicate these threats to the installation commander.

Chapter 11
Intelligence

11-1. General.

a. U.S. Military Intelligence activities are specifically prohibited from conducting intelligence operations against non-DOD related U.S. persons. The military must use all available intelligence resources and closely coordinate with appropriate local, state, and federal agencies to ensure the protection of TRADOC personnel and other resources.

b. Program Elements. Intelligence support to FP will be tailored to meet the local commander's need and will include the following elements:

(1) Use of intelligence database.

(2) Development and maintenance of local criminal and terrorist threat assessment.

(3) Reporting and disseminating criminal and terrorist activity information IAW AR 381-10.

(4) Conduct of a threat awareness briefing program.

(5) Conduct of a SAEDA briefing program which incorporates information regarding the criminal/terrorist threat.

(6) Intelligence participation in FPC, fusion cells, FP plans and exercises.

(7) Intelligence liaison with the 902d Military Intelligence Group and intelligence sections of local LE.

(8) Protection of mission essential information.

11-2. Reporting and disseminating terrorist threat information. The objective

of intelligence support to FP is to provide accurate and timely threat information to leaders and personnel. To accomplish this, the security officer must develop a workable plan for dissemination of threat information. The specific provisions of the plan will be dependent on the installation or command mission and organization. Dissemination of threat information is required on both a routine and immediate basis.

a. Routine dissemination includes the provision of threat briefings, the publication of local threat documents, and the distribution of threat related briefing information.

b. Immediate dissemination is required when the installation or organization obtains credible intelligence regarding an imminent threat to U.S. Government personnel, facilities, and information.

c. The security officer will ensure that each major unit or activity located within his/her installation or organization has designated a threat information point of contact. This individual will be responsible for :

(1) Receiving threat information updates from the security officer and further disseminating the information throughout the organization.

(2) Receiving immediate threat warnings, informing the unit leadership and disseminating the information throughout the organization.

(3) Beginning the TTR process, in the event that credible threat information is developed at the unit level.

d. The security officer will be responsible for personally presenting threat update and immediate threat briefings to the installation commander and the senior intelligence officer .

e. The plan for immediate dissemination of information will--

(1) Maximize the fastest, most dependable existing means of communication.

(2) Be directed to designated FP personnel and key leadership.

(3) Be incorporated in the annual FP exercise.

f. The routine dissemination of information will--

(1) Be provided through FP points of contact.

(2) Include the provision of briefings to units, soldiers, dependents, and DA civilians who travel outside the 50 U.S. To ensure that all personnel receive required briefings, Security Officer will coordinate with local orders issuing authorities. Security officer will then be notified of each foreign travel order issued.

(3) Include periodic updates to FPC and senior leadership.

g. In the event of an actual terrorist attack, the FPO will submit a TIR.

h. The security officer will ensure dissemination of terrorist threat information to the lowest possible levels. Classification of information will be kept at the lowest possible level.

11-3. Conduct of Threat Awareness Briefings. The security office is responsible for the conduct of the threat awareness briefing program. If members of the installation security office do not conduct each briefing, they are required to ensure all personnel presenting terrorist threat briefings are qualified and have current information.

a. When possible, terrorist threat awareness briefing will be conducted by intelligence and security personnel who have completed recognized terrorist threat briefing training. In the event of an immediate requirement, other intelligence and security personnel may provide the briefing.

b. The intelligence database will be used as the principle source of threat awareness briefing information. As a minimum, intelligence threat awareness briefings will include information on the existence, history, capability, targeting, intentions and security environment of terrorist or criminal organizations in the area.

11-4. Conduct of Subversion and Espionage Directed Against the U.S. Army (SAEDA) Briefing Program.

a. Conduct of an effective SAEDA program greatly enhances FP efforts by providing

possible early detection of intelligence agents or potential terrorists.

b. AR 381-12 requires all military and DA civilian personnel to receive SAEDA briefing at least once every 2 years. Briefings must be conducted by trained counterintelligence personnel.

c. The installation security office has the responsibility to coordinate availability of instructor personnel. Instructor personnel may be available from the local 902d MI Detachment, the installation security office, or unit counterintelligence sections/elements.

11-5. Intelligence participation in FPCs and fusion cells, FP plans and exercises.

a. The security officer will be a participating member in the FPC and fusion cells. These organizations must be continually updated on the local terrorist or criminal threat assessment.

b. The security officer will provide an intelligence annex or input to all FP plans or documents.

c. Preparation for exercises will require development of realistic intelligence scenarios that exercise key aspects of the installation FP plan.

11-6. Intelligence Liaison with the 902d MI Group and Intelligence Sections of Local Law Enforcement.

a. The security officer must establish liaison with the local representatives of the 902d Military Intelligence Group to ensure adequate maintenance of the local terrorist and criminal threat assessment. The 902d MI GP will facilitate coordination between the security officer and the intelligence elements of local law enforcement agencies (LEA). In some cases 902d MI GP offices are not collocated with the installation. In these instances, the security officer may be required to conduct more direct coordination with the local LEA. The security officer has the responsibility to keep the 902d MI GP informed of these activities.

b. In conducting coordination and liaison, the security officer will observe the following restrictions and limitations.

(1) The purpose of the liaison is to establish a local intelligence community to access information regarding possible terrorist or criminal threats. Issues regarding implementation of law enforcement will be immediately referred to the installation PM.

(2) Collection and reporting limitations of AR 381-10 must be strictly observed. Immediate issues should be coordinated with the installation Inspector General (IG) and SJA.

(3) Information provided to the installation by LEA may be marked as "LEA Sensitive". This information should be protected consistent with the procedures of the providing agency, but at least in the manner of that protection provided to U.S. Army "For Official Use Only" material.

Chapter 12
Public Affairs (PA)

12-1. General. Public affairs (PA) is a force multiplier for the commander when dealing with the challenges of FP. The rapid, accurate and timely flow of information from the command to internal and external audiences is critical to reduce force vulnerability, support FP efforts, and project a strong image to potential terrorists and the American people.

12-2. Public Affairs' FP role and responsibilities.

a. The PA program must support command efforts to increase the awareness of the Total Army Family about the local criminal and terrorist threat and supplement or support personal protection and FP training programs. To accomplish this, PA has four goals:

(1) Provide on-scene PA support as requested or directed by competent authority.

(2) Provide accurate and timely information to minimize speculation, dispel rumors and instill confidence that the DOD, the Army, and TRADOC can reduce the vulnerability of personnel, property, and equipment from potential threats.

(3) Provide timely and accurate PAG to supplement FP messages.

(4) Provide for a comprehensive and continuing command information program to maintain general FP and situational awareness among internal audiences.

b. PA operation will ensure, to the maximum extent possible, that all official Army information originates from a single source, thereby reducing the possibility of compromising key information and of releasing conflicting or inconsistent information.

c. Every effort will be made to stress military-civilian police and governmental cooperation and joint efforts to deal with the situation.

12-3. Execution.

a. During an actual or potential criminal or terrorist incident, information released must effectively keep audiences informed while at the same time avoiding the image that the command is "under siege." The presentation of such an image will further the potential terrorists or criminal goal of creating fear and confusion.

b. TRADOC installation PAOs will prepare a PA annex to the local installation/activity FP plan. The annex will:

(1) Provide for a comprehensive and continuing command information program to maintain general FP and situational awareness among internal audiences.

(2) Identify responsibilities and procedures for coordinating the clearance and release of FP information in support of news media requirements IAW applicable PA and FP policies and guidance.

(3) Provide accurate and timely information to minimize speculation, dispel rumors, and instill confidence that the DOD, the Army, and TRADOC can reduce the vulnerability of personnel, property, and equipment from potential threats.

(4) Provide for the training of PA personnel in FP procedures.

Appendix A
References

Section 1
Required Publications

AR 190-13
The Army Physical Security Program

AR 190-45
Law Enforcement Reporting

AR 190-58
Personal Security

AR 195-2
Criminal Investigation Activities

AR 360-5
Army Public Affairs, Public Information

AR 380-19
Information Systems Security

AR 381-10
U.S. Army Intelligence Activities

AR 381-12
Subversion and Espionage Directed Against the U.S. Army (SAEDA)

AR 415-15
Army Military Construction Program Development and Execution

AR 525-13
The Army Combating Terrorism Program

AR 525-20
Command and Control Countermeasures (C2CM)

DA PAM 190-51
Risk Analysis for Army Property

DODD 2000.12
DOD Combating Terrorism Program

DOD Handbook 2000.12H
Protection of DOD Personnel Against Terrorists Acts

DODI 2000.14
DOD Combating Terrorism Program Procedures

GTA 21-3-11
Individual Protective Measures

Section II
Related Publications

AR 55-46
Travel Overseas

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

AR 190-16
Physical Security

AR 190-30
Military Police Investigations

AR 190-51
Security of Unclassified Army Property

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

AR 360-61
Community Relations

AR 360-81
Command Information Program

AR 380-5
Department of the Army Information Security Program

AR 380-13
Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations

AR 380-19
Information Systems Security

AR 381-20
The Army Counterintelligence Program

AR 381-100
(S) Army Human Intelligence Collection Programs

AR 500-50
Civil Disturbances

AR 530-1
Operations Security (OPSEC)

AR 550-51
Emergency Employment of Army and Other Resources - Support to Civilian Law Enforcement

DA PAM 50-6
Chemical Accident or Incident Response and Assistance (CAIRA) Operations

FM 3-4
NBC Protection

FM 3-5
NBC Decontamination

FM 3-21
Chemical Accident Contamination Control

FM 3-100
Chemical Operations, Principals, and Fundamentals

FM 8-9
NATO Handbook on the Medical Aspects of NBC Defensive Operations

FM 8-10-7
Health Service Support in a Nuclear, Biological and Chemical Environment

FM 8-55
Planning for Health Service Support

FM 8-285
Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries

FM 16-1
Religious Support

FM 19-10
The Military Police Law and Order Operations

FM 19-20
Law Enforcement Investigations

FM 19-30
Physical Security

FM 34-60
Counterintelligence

FM 100-5
Operations

FM 100-14
Risk Management

FM 100-19
Domestic Support Operations

FM 101-5
Staff Organization and Operations

Appendix B

Level I-IV Training Requirements

Level	Target Audience	Minimum Training Standard
Level I (Negligible/ Low Threat)	Soldiers, DA Civilians, and family members deploying/ traveling on government orders Deploying or traveling to Negligible or Low Terrorist Threat Level Areas	Within six months prior to travel: View TVT; Individual Protective Measures Receive AT/FP Awareness Handouts: - JS Guide 5260 and DoD wallet card; or GTA 19-4-3; - GTA 21-3-11; "Individual Protective Measures" May 1990
Level I (Medium/ High Threat)	Soldiers, DA Civilians, and family members deploying/ traveling on government orders Deploying or traveling to Medium or High Terrorist Threat Level Areas Conducted within 6 months prior to travel	Same requirements as above, plus: View AT/FP Awareness Videos: - TVT; Terrorist Surveillance Detection - TVT; Hostage Survival Techniques - TVT; Terrorist THREATCON Implementation Recent AOR update for area of travel Level II AT/FP officer using an approved USAMPS lesson plan, containing a minimum of the following subjects: - Individual & Unit Protective Measures - Hostage Survival Techniques - Terrorist Surveillance Detection - THREATCON Measures
Level II FP Officer	FP Officers who are then certified/current to serve as the Commanders FP advisor, and provide Level I instruction and training for hostage/kidnapping situations	Attend USAMPS's "The Force Protection Unit Advisors Course" Module A: FP Level I Training - Intro to Terrorism (RJ1200) - Terrorism Operations (RJ1205) - Individual & Unit Protective Measures (RJ1215) - Hostage Survival Techniques (RJ1225) - Terrorist Surveillance Detection (RJ1235) Module B: Force Protection Advisor Training - Physical Security - Command Control Protect - THREATCON Measures - Risk Analysis - Improvised Explosive Devices/Contingency Planning - Threat Assessment
Level III	O-5/O-6 Commanders	"Implement the Army's Force Protection Program" - Taught in branch PCCs & Garrison Command Course View Sec Def/CJCS AT Awareness video: TVT; "You May Be The Target"
Level IV (optional)	O-6 to O-8 Commanders/ personnel responsible for FP programs or involved in FP policy, planning and execution	Executive level seminar providing pertinent current updates, briefings, panel discussions topics. Seminar will conclude with a tabletop FP wargame aimed at facilitating interaction and discussion among the participants.

Appendix C
Commander's Assessment Tool.

C-1. Policy.

a. TRADOC Standard 1. TRADOC Force Protection Policy. Major subordinate commands and installation commanders will develop a full working knowledge of FP policies. Further, they will communicate the spirit and intent of these policies throughout the chain of command or line of authority. Commanders are responsible for development of subsequent installation unique standards.

Questions:

(1) Has the installation published a supplement to TR 525-13, implementing guidance, or an operations order outlining installation unique requirements?

(2) If a supplement to TR 525-13 has been published, was it approved by HQ TRADOC?

C-2. Operations.

a. TRADOC Standard 2. Assignment of FP Operational Responsibility. Commanders will clearly establish operational responsibility for FP for all units and individuals whether permanently or temporarily assigned.

Questions:

(1) Are procedures in place to ensure that each individual and unit is aware of who is operationally responsible for FP?

(2) Are procedures in place to ensure those personnel operationally responsible for FP are notified upon the arrival and departure of individuals and units?

b. TRADOC Standard 3. Program and Planning. FP programs will be based on assessments of threats and vulnerabilities. FP operational planning will identify, coordinate, allocate and employ resources to ensure FP measures are developed that provide the appropriate level of protection for all applicable threats.

Questions:

(1) Does the command have an established FPP with implementing plans and guidance?

(2) Are plans based on a published threat statement?

(a) Does planning coordinate and synchronize related plans (i.e., Threat Collection Plan, Information Security Plan, Crisis Management Plan, Terrorist Response Plan, and the Physical Security Plan) from all areas of the TRADOC FPP?

(b) Is FP included in all phases of deployment planning?

(c) Are tenant units included in planning?

(3) Do Interservice Support Agreements, Memoranda of Understanding, and Memoranda of Agreement consider FP?

(4) Does the command monitor the effectiveness of the FP programs at subordinate commands/units? Are deficiencies and corrective actions identified, documented, and tracked?

c. TRADOC Standard 4. Committees and working groups. Commanders at installation level will establish FPC to assist in the development, integration, and management of the FPP. Additionally, commanders will establish FP working groups which include representation by staff officers with FP responsibilities from operations (S3, G3, DPTMS), Provost Marshal, Intelligence, Engineer, and other staff sections dependent on the situation. FP working groups should meet frequently to discuss the current threat and evaluate security measures that have been planned or implemented. FP working groups will operate under the direction of the installation's FP officer to develop issues for presentation to the FPC.

Questions:

(1) Does the FPC meet at least semi-annually?

(2) Do all of the personnel required by TR 525-13 sit on the committee (i.e., OPS, PM, Intel, EN, IO, Log, Med, SJA, PAO, Chem, etc.)?

(3) Does the FPC provide the commander with a written record of the meetings and maintain those records on file for two years?

(4) Does the FP working group meet frequently during times of increased threat?

(5) Does the FP working group develop issues for presentation to the FPC.

d. TRADOC Standard 5. Exercises. Commanders will institute an exercise program which develops and refines the command's FP procedures and responses to the entire spectrum of FP threats.

Questions:

(1) Is there a system in place to exercise FP related plans and attack warning systems at least annually?

(2) Do the scenarios involve the staff (that have FP responsibilities)?

(3) Is there a feedback mechanism to route After Action Review results through the FPC to the commander?

e. TRADOC Standard 6. Risk Management. The Army's five step risk management process will be integrated into all FP related planning and program execution.

Questions:

(1) Do the commander and staff understand the Army's five step risk management process?

(2) Is risk management incorporated into all FP planning and program execution by both the commander and staff?

(3) Is risk management considered in all elements of the FPP (i.e., physical security, Information Operations, resource management, etc.)?

f. TRADOC Standard 7. Periodic Program Review. Installation FP programs will be reviewed at least once every three years.

Questions:

(1) Have installation programs been reviewed by MACOMs within the last three years?

(2) Were the inspection results documented?

(3) Were deficiencies corrected?

g. TRADOC Standard 8. FP Officer. All major subordinate commands and installations, and deployable units to battalion level will designate an FP Officer. Questions:

(1) Has the commander appointed an FP Officer on orders?

(2) Does the FP officer have direct access to the commander?

(3) Has the FP Officer attended Level II Training?

(4) If not, has the FP officer received the required written waiver from the first 0-6 Commander in the chain of command?

h. TRADOC Standard 9. Development of Local THREATCON Levels. Commanders will develop a process based on terrorist threat information and/or guidance from higher headquarters to raise or lower THREATCON levels. THREATCON transition procedures and measures will be disseminated and implemented by all subordinate and tenant commanders.

Questions:

(1) Is there a process in place to change THREATCON levels, when required?

(2) Has the process been tested within the past year?

(3) Are there sufficient assets to implement all THREATCONs? If not, are there procedures to:

(a) Divert/acquire local assets on an emergency basis?

(b) Notify higher headquarters of shortfalls?

(4) Are enhanced security measures planned for post housing areas in the event of a heightened THREATCON?

(5) Is there a process to continuously review the effectiveness of daily physical security measures under THREATCON normal?

i. TRADOC Standard 10. WMD planning. FP plans, orders, SOPs, threat assessments, and coordination measures will address potential terrorist WMD threats. Commanders will assess the vulnerability of installations,

facilities, and personnel within their AOR to terrorist use of WMD. Clear command, control, and communication lines will be established between local, state, and federal emergency assistance agencies to detail support relationships and responsibilities.

Questions:

(1) Are terrorist WMD threats assessed?

(2) Is WMD included in the Crisis Management Plan?

(3) Does this plan address potential threats and vulnerability assessments?

(4) Are probable WMD targets identified?

(5) Are plans coordinated with local, state, federal, and host nation authorities and do they participate in exercises?

(6) Do Staff Duty instructions include WMD terrorist response procedures?

(7) Is there a WMD attack warning system and are procedures established and exercised?

(8) Are there provisions to establish rapid communications between military, local, state, federal, and host nation agencies?

j. TRADOC Standard 11. First Response and Consequence Management. First responders will be officially identified, trained, and equipped to respond to both conventional and WMD attack. Detailed response plans will include: casualty triage, decontamination, evacuation, and tracking; site security, evidence preservation, and contamination control measures; and detailed interagency support and coordination measures. Periodic FP exercises will test medical response and consequence management procedures; including WMD response measures.

Questions:

(1) Are first responders officially designated?

(2) Are first responders trained to respond to conventional and WMD attacks?

(3) Do first responders have adequate protective equipment, including CDE?

(4) Are emergency first responder equipment shortfalls considered in FP planning?

(5) Are local hospitals capable of treating mass casualties, including WMD casualties?

(6) Are patient decontamination responsibilities assigned in FP plans?

(7) Are location and status of casualties tracked?

(8) Are medical MASCAL and WMD scenarios included in the FP exercise program?

(9) Are Installation staffs integrated into WMD/MASCAL training?

(10) Is the PAO a participant in MASCAL and WMD exercises?

(11) Are adequate resources available to support the emergency response plan?

(12) Do WMD response plans address mass casualty scenarios in high density population areas?

k. TRADOC Standard 12. Command Information Program. Commanders will incorporate FP into their Command Information Programs.

Questions:

(1) Does the commander incorporate FP program information into the Command Information Program?

(2) Is FP information being effectively disseminated through multiple means (e.g., briefings, posters, newspaper/newsletter articles, chain of concern, radio, and television)?

(3) Is FP information formatted for the total Army (soldiers, family members, DA civilians)?

(4) Is OPSEC included in all PAs operations?

C-3. Intelligence.

a. TRADOC Standard 13. Collection of Force Protection Intelligence Information. Commanders will have a fully integrated FP intelligence program focused and based on

priority intelligence requirements (PIR) that provides the appropriate threat information to protect personnel, family members, facilities, and material in all locations and situations. The commander will ensure that production and analysis requirements are focused and based on the commander's PIR.

Questions:

(1) Are collection operations being conducted consistent with the provisions and limitations of AR 381-10?

(2) Does the command have connectivity to receive threat related information from all available sources (e.g., FBI, local law enforcement, and Intell Link)?

(3) Is the activity familiar with the Army Counterintelligence Center (ACIC) and does it know how to obtain ACIC products?

(4) Is the activity receiving the Monthly International Terrorism Summary (MITS)?

(5) Has the commander established PIR?

(6) Are the commander's PIR the basis for production requirements?

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

(8) Is the DOD Terrorist Threat Level Classification system utilized to identify the threat?

b. TRADOC Standard 14. Threat and Vulnerability Assessments. Commanders will prepare a threat assessment for their AOR. Where the threat assessment indicates a general threat, and prior to any deployment, commanders will prepare a vulnerability assessment.

Questions:

(1) Have multi-disciplined threat and vulnerability assessments been conducted?

(2) Is the entire spectrum of threats, to include terrorist use of WMD, part of the threat and vulnerability assessments?

(3) Are the results of the vulnerability assessment reviewed and used as part of the commander's criteria for setting specific THREATCON measures?

(4) Are the results of the vulnerability assessment disseminated to affected organizations (e.g., organic, tenant and supported Reserve Component units)? Where specific vulnerabilities are identified are they reviewed for appropriate classification?

(5) Is the ACIC utilized as a tool to conduct vulnerability assessments?

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

c. TRADOC Standard 15. Dissemination of FP Intelligence Information. Commanders will ensure FP intelligence information is disseminated in a timely manner. Current intelligence will be integrated into the FP training program.

Questions:

(1) Is terrorist information being coordinated with other staff elements involved in the FPP?

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

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

C-4. Training.

a. TRADOC Standard 16. Individual Training. Commanders will ensure that all military and DA Civilian personnel in their command receive the appropriate training for individual antiterrorism awareness prior to deploying or traveling outside the United States and/or territories. The individual's records will be updated in accordance with local policy. Family members will receive similar training prior to traveling outside the United States and territories on official government orders.

Questions:

(1) Do policies and guidance ensure that personnel (military, DA civilians, and family members) are provided with the appropriate

level of antiterrorism training, education, and awareness?

(2) Is the command aware of Army requirements for levels I and II AT training and have they implemented the program?

(3) Does the program train all personnel in FP procedures, guidance, and instructions?

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

(5) Are theater specific predeployment requirements for the CINC AORs being accomplished?

(6) Is there a validation process to ensure that Level I training is accomplished for deployments, PCS, leave, and TDY?

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

(8) Are AT/FP training materials readily available (e.g., Level I videos, GTA wallet cards, etc.)?

(9) Are personnel with specific FP duties sent to required courses in accordance with applicable regulations?

b. TRADOC Standard 17. Leader Training. Individuals identified as having significant responsibilities for the command FP program will receive adequate training that provides them with the ability to train others, as well as advise the commander.

Question:

(1) Are key leaders with FP responsibilities trained?

c. TRADOC Standard 18. Hostage Training: Personnel assigned to Medium or High Terrorist Threat Level areas, will receive guidance at least annually on appropriate conduct in the event they are taken hostage or kidnapped.

Question:

(1) Is training being conducted by a certified instructor?

d. TRADOC Standard 19. Training in Support of High Risk Personnel. Commanders will ensure that HRP and their family members are made aware of risks and trained in personal protective measures. Additionally, support staff such as drivers, aides, and protective services details will be trained and equipped.

Questions:

(1) Is evasive driving training offered to HRP?

(2) Is training in supplemental individual protective measures provided to HRP?

(3) Is similar awareness training provided to the families of HRP?

(4) Is awareness training provided to support staff such as drivers and aides?

C-5. Resources.

a. TRADOC Standard 20. Resource Management. FP requirements will be prioritized by the Commander (with assistance by the FP Committee) based on the threat, documented vulnerabilities, regulatory requirements, and/or command directives. Funds supporting the FP program will be tracked and accounted for.

Questions:

(1) Are the appropriate staff activities (e.g., PM, EN and OPS) involved in developing program requirements?

(2) Are staffs reviewing their areas for FP requirements based on DA Standards, the threat and assessed vulnerabilities?

(3) Are projects prioritized based on coordinated threat and vulnerability assessments at each level of command?

(a) Does the justification include specific impacts if the project is not completely funded?

(b) Is the methodology used to validate and prioritize projects documented?

(c) Does the commander approve the prioritized requirements list at each level of command?

(d) Are there established procedures to submit or update annual programs, or expeditiously resource critical FP requirements?

C-6. Information Operations.

a. TRADOC Standard 21. Information Operations (IO) Integration. Commanders will ensure that IO is integrated into all FP planning and program execution. Commanders will ensure integration of relevant laws and regulations pertaining to security monitoring of the command's network information infrastructure.

Questions:

(1) Have the provisions of AR 380-19, Information Systems Security (ISS), been integrated into the command's FPP?

(2) Are the following elements of IO being integrated into the FP Program?

(a) OPSEC?

(b) Public Affairs?

(c) COMSEC monitoring?

(d) Computer monitoring?

(3) When incidents occur on the network are they reviewed, and are trends developed indicating significant weaknesses?

(4) Is the IO representative an active participant on the command's FPC?

(5) Are incident reporting procedures published for system administrators IAW C2 Protect Implementation Plan?

(6) Have warnings been devised to alert the command of incidents?

(7) Is the command familiar with the roles of the Land Information Warfare Activity (LIWA)/Army's Computer Emergency Response Team (ACERT)?

(8) Does the OPSEC plan include the provisions of AR 530-1? Are OPSEC threats identified? Is OPSEC part of the unit's training program?

(9) Is IO, C2 Protect, and ISS included in threat briefings and assessments provided to the commander?

(10) Is there a computer security awareness program?

(11) Does the command monitor the effectiveness of IO integration at the subordinate command and unit level?

b. TRADOC Standard 22. Information Operations Threat and Vulnerability Assessments. Commanders will ensure friendly information systems are included in threat and vulnerability assessments. Commanders will ensure C2 Protect procedures and techniques are developed to detect and deny unauthorized intrusion to the communication network.

Questions:

(1) Is the command registered in the Terminal Server Access Controller System for access to the Army tool set and are requirements for tools identified?

(2) Are procedures to report incidents to the Army Computer Emergency Response Team (ACERT) in place and incidents reported?

(3) Do network operators obtain assistance installing security patches (fixes to vulnerabilities) from the ACERT?

(4) Are Automated System Security Incident Support Team (ASSIST) Bulletins issued from the Defense Information Systems Agency (DISA/ACERT) received by all system and network administrators?

(5) Has the OPSEC process been applied in determining threats and vulnerabilities to your communications infrastructure?

(6) Are countermeasures routinely tested (e.g., user IDs, passwords, and audit trails)?

(7) Is information systems security training performed at appropriate levels?

(8) Are security incidents/violations (e.g., viruses, unauthorized entries or attempts, and password compromises) analyzed, reviewed, investigated and reported?

(9) Are security measures employed to control the external access? (e.g., callback and tokens)

(10) Is an automated audit capability (i.e., log security-related events) available and used in all systems?

(11) Is identification and authentication (i.e., user id and password) required for access to all systems?

(12) Was the OPSEC process applied in developing countermeasures for the communication infrastructures?

c. TRADOC Standard 23. IO Training. Commanders will develop information security and awareness training and will develop management methodologies to evaluate risks associated with operations of information networks.

Questions:

(1) Are system administrators and network administrators adequately trained in ISS?

(2) Does the available training meet program requirements?

(3) Is ISS training provided to the user IAW 380-19?

(4) Has C2 Protect training been developed?

(5) Has the C2 training Tool Kit been acquired and implemented?

(6) Is there a training plan developed to ensure continual operations in event of major disruptions IAW AR 380-19?

(7) Are all personnel familiar with their OPSEC responsibilities IAW AR 530-1?

(8) Are vulnerability assessments performed on the Army communications infrastructures?

(9) Are countermeasures identified and in place based on the results of vulnerability assessments?

(10) Is there a written security plan to document implementation of countermeasures?

(11) Are sufficient secure communications available to the command?

(12) Are appropriate security personnel appointed and trained (e.g., ISSPM, ISSM, or ISSO)?

(13) Where both system security and network maintenance functions are performed by the same person, are requirements of AR 380-19 and the C2 Implementation Plan met?

C-7. Physical Security.

a. TRADOC Standard 24. Security Engineering. FP will be considered in standard Army design practice with security measures that are based on risk and threat analysis.

Questions:

(1) Are PS and THREATCON considerations incorporated into the installation master plan and site selection?

(2) Are the results of threat analyses incorporated into the installation's military construction design program?

(3) Are risk analyses performed and are FP measures considered for all new and existing facilities either designated or likely to be designated MEVAs ?

(4) Are local engineers familiar with the resources (such as the Protective Design Center and the Electronic Security Systems Center) available to them in security engineering?

b. TRADOC Standard 25. Security Planning. Commanders at all levels will plan, based on risk analysis, for security of assets entrusted to them. Plans will be affordable, effective, and attainable. Plans will tie security measures together and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. Planning must ensure that requirements at each THREATCON have been addressed.

Questions:

(1) Is there a current PS Plan IAW AR 190-13 approved by the commander?

(2) Does the plan contain the basic requirements IAW AR 190-13 (e.g., Bomb Threat, Installation Closure, Threat Statement, etc.)?

(3) Are the components of the plan tested IAW AR 190-13?

(4) Is the process of risk analysis/management well defined, understood and incorporated into physical security planning and execution?

c. TRADOC Standard 26. PS Threat Assessment. PS Programs will be based on local threat and vulnerability assessments which are updated at least annually.

Questions:

(1) Is there a published local threat assessment?

(2) Does the threat assessment address a broad range of physical security threats taken from the overall force protection threat assessment?

(3) Is the threat assessment coordinated with the FPC?

(4) Are current threat assessments adequate for determining vulnerabilities?

d. TRADOC Standard 27. MEVA: MEVAs which are critical to mission accomplishment or are vulnerable to theft/damage/ attack, will be identified in order to focus security efforts.

Questions:

(1) Are MEVAs identified, prioritized, and approved by the commander IAW AR 190-13?

(2) Are periodic reviews conducted IAW AR 190-13 to update areas designated as MEVAs?

e. TRADOC Standard 28. Restricted Areas. Areas which are considered critical or sensitive will be identified and formally designated as Restricted Areas in order to give commanders legal authority to impose special access controls.

Questions:

(1) Are restricted areas identified and designated IAW AR 190-13?

(2) Are restricted areas correctly posted?

f. TRADOC Standard 29. Inspections and Surveys. Periodic formal reviews by security specialists will be conducted in order to assess physical security programs and to ensure compliance with security standards for protection of MEVA.

Questions:

(1) Are installation surveys conducted at least every three years to assess installation physical security posture?

(2) Are physical security inspections of MEVAs conducted every 18 months for arms, ammunition and explosives storage facilities and every two years for others types of MEVA?

g. TRADOC Standard 30. Employment of Security Measures. Appropriate physical and procedural measures will be employed which provide integrated deterrence, detection and defense capabilities in order to safeguard all personnel and material assets.

Questions:

(1) Are detection and assessment measures integrated with defense (delay) measures to protect personnel and material assets?

(2) Are security engineering surveys conducted when planning new facilities or renovating existing facilities?

(3) Was risk and threat analysis utilized in the development of any protective measures beyond those specifically requiring employment by regulation?

(4) Is TM 5-853-1 used in the development and employment of security measures?

C-8. Combating Terrorism.

a. TRADOC Standard 31. Antiterrorism. Commanders will develop AT programs that provide standards, policies and procedures to reduce the vulnerabilities of all personnel including DOD military, civilians, and family members from terrorist attack. AT programs will include installation-wide terrorist response plans which include procedures for determining the nature and scope of terrorist incidents, post incident response and reconstitution.

Questions:

(1) Does the installation/unit possess a terrorist incident response plan?

(2) Does the installation have a plan to conduct post incident response? Has it been tested in conjunction with the terrorist response plan?

(3) Does the installation have plans and procedures in place to reconstitute after a terrorist attack? Has that portion of the plan been tested?

(4) Are emergency evacuation plans in-place and are they tested?

(5) Is there an attack warning system which utilizes a set of recognizable alarms with reactions to potential emergencies, as determined by the threat and vulnerability assessment? Are personnel trained in recognition? Is the system exercised as part of the FP Exercise Program?

b. TRADOC Standard 32. Residential Security Assessment for Off-Post Housing. Commanders in Medium or High Terrorist Threat Level areas will conduct physical security assessments of off-post residences for permanently assigned and TDY personnel. Based on the assessment results, commanders will provide antiterrorism recommendations to the residents and facility owners. Personnel assigned to Medium or High Terrorist Threat Level areas and not provided on-installation or other government quarters, will be furnished guidance on the selection of private residences to mitigate risk of terrorist attack.

Questions:

(1) Are physical security assessments conducted on initial occupancy and annually thereafter?

(2) Is an up-to-date listing of residences for TDY and permanently assigned personnel maintained and safeguarded, and are they included in Terrorist Incident Response Plans?

c. TRADOC Standard 33. Facility and Site Evaluation/Selection Criteria. Commanders will develop a prioritized list of FP factors for site selection teams. These criteria will be used to determine if facilities, either currently occupied or under consideration for occupancy, can adequately protect occupants against terrorist attack.

Questions:

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

(2) Is the list utilized?

C-9. Law Enforcement.

a. TRADOC Standard 34. Law Enforcement Operations. Law enforcement operations will support installation FP requirements through the commander's authority to enforce federal law and Army regulations. In the event of acts of terrorism on installations, Military and DOD police will take immediate action to resolve the incident and prevent loss of life. Terrorist incident response plans will include the use of law enforcement as first responders and provide procedures for employing police resources effectively.

Questions:

(1) Is the Provost Marshal (PM) adequately resourced to conduct law enforcement operations in support of the installation FP program?

(2) Have adequate law enforcement contingency plans for emergency situations (e.g., bomb threats, hostage taking, base closures and increased THREATCON levels) been developed and exercised?

(3) Are exercise results provided to the commander through the FPC?

(4) Has each command/activity supporting these plans been given the opportunity to participate in the creation of the plan and are they in receipt of a copy of the plan?

(5) Do plans address backfill of law enforcement personnel during deployments?

b. TRADOC Standard 35. Law Enforcement Liaison: Provost Marshals will conduct effective liaison with Federal, State, local and host nation agencies, as appropriate, to ensure criminal intelligence is shared and that plans and operations supporting FP are coordinated.

Questions:

(1) Does coordination of security plans include applicable federal, state, local and host nation officials outlining movement, security, and jurisdictional responsibilities?

(2) Is liaison conducted to ensure criminal intelligence, to include U.S. domestic threat information, is properly gathered, processed, and passed?

(3) Is this information coordinated through the FPC process?

(4) Are law enforcement operations coordinated with the appropriate federal, state, local and host nation agencies?

C-10. Personal Security.

a. TRADOC Standard 36. Identification and Designation of HRP. Commanders will ensure that 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 in order to make them eligible for special control/security measures.

Questions:

(1) Is there a formal procedure for designating HRP? Have HRP been designated?

(2) Is there a periodic review of HRP designations?

b. TRADOC Standard 37. Protective Measures for Safeguarding HRP. Commanders will take appropriate measures to provide enhanced protection to HRP:

(1) Are HRP receiving PSVAs from CID?

(2) Are PSDs available to protect HRP1?

(3) Have safe havens been established?

(4) Are alarms installed in quarters and offices of HRP?

(5) Are MWD available to conduct explosives detection sweeps?

Appendix D
Potential Sources of Intelligence Information

1. General. The intelligence database is developed from a diversity of sources. The most effective FP Intelligence Action Officer (FPIAO) will continually look for additional sources. The list provided in table D-1 is by no means exhaustive, but is intended to provide examples of potential sources.

Table D-1
FP Information Sources

AGENCY	TITLE	POC
DISA	Computer Security Advisories	http://www.distt.mil/css
HQDA	FP Update	U.S. Army Antiterrorism Opns & Intelligence Cell DSN: 227-5484/85
NIST	Computer Security Advisories	http://nvi.nist.gov.80
NCSA	Computer Security Advisories	http://www.nusa.com
DOS	Travel Advisories	http:/www.stolaf.edu/ network/travel.advisories. htlm
USAF	Weekly OPSEC Highlights	Electronic Threat Branch DSN 969-4551
ASIS	Miscellaneous Security Info	http://www.asisonline.org (703) 522-5800
Pinkerton	Travel Risk Assessment	Pinkerton Risk Assessment 200 N. Glebe Rd, Ste I011 Arlington, VA 22203 (703) 525-6111

Appendix E
Approved Questions and Answers

1. PURPOSE. The purpose of this appendix is to provide guidance for responding to media inquiries about military actions related to FP.

2. The following questions and answers have been excerpted from HQDA OCPA MSG 211525 APR 86 - PA Guidance - Terrorism. They are current and may be used in the situations outlined below.

a. News media request the PAO to discuss specific AT or other FP Measures.

(1) Response: Appropriate security precautions are being taken. Some of these measures may be obvious. However, I will not discuss specific initiatives.

(2) PA spokespersons may, if appropriate, acknowledge the obvious, but must ensure operational security is not violated.

b. The following two quotes may be used to respond to questions about CBT/T and FP: (Use the appropriate response)

(1) Response: The Army's policy prohibits discussing specific defensive measures in our FP program. Such disclosure

could adversely affect the success of the program.

(2) Response: Military authorities are working closely with local security forces to ensure maximum coordination for appropriate protective measures.

c. For use in response to questions concerning counterterrorism (for use by PA officers at any level):

(1) Response: The U.S. government has trained forces and equipment from all four services to cope with terrorist incidents. Command and control elements for these forces exist and have been exercised. These elements report to the Joint Chiefs of Staff (JCS), 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.

d. In response to queries regarding a possible or real terrorist or criminal threat at a particular installation or activity, the PAO may acknowledge, if appropriate, that increased security measures have been taken without going into specific details of the measures taken. For example, increased security measures such as increased guards at the gate or additional patrols, if they are obvious to the public may be acknowledged. PAOs, however, should exercise care and prudent judgment in any discussion of these and other security measures which have been or will be implemented.

APPENDIX F

DOD THREATCON System

F-1. THREATCON levels.

The terrorist threat conditions (THREATCON) system discussed here is mandated in DOD Directive 2000.12. It describes progressive levels of security measures for implementation in response to terrorist threats to U.S. Army personnel and facilities. The THREATCON system is the baseline for development of FP plans and orders; FP programs should be constructed to reflect the threat assessment system and the measures described in this appendix. The measures listed below are general in nature. When producing local plans, local commanders convert general guidance into more specific instructions in order to meet the unique requirements of the specific location.

a. There are five THREATCON levels:

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

(2) THREATCON Alpha. Applies when there is a general threat of possible terrorist activity against personnel and/or installations, the nature and extent of which is unpredictable, and circumstances do not justify full implementation of THREATCON Bravo measures. However, it may be necessary to implement certain measures from higher THREATCONs resulting from intelligence received or as a deterrent. Commands must be capable of maintaining THREATCON Alpha measures indefinitely, with only limited impact on Normal operations.

(3) THREATCON Bravo. Applies when an increased or more predictable threat of terrorist activity exists. Commanders must be capable of maintaining the measures of this THREATCON 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) THREATCON Charlie. Applies when an incident occurs or intelligence indicates that some form of terrorist action against personnel and/or facilities is imminent. Implementation of THREATCON Charlie measures for more than a short period probably will create hardships for personnel and affect the peacetime activities of units and personnel.

(5) THREATCON Delta. Implementation applies in the immediate area where a terrorist attack has occurred or when intelligence indicates that terrorist action against a specific location is likely. Implementation of THREATCON Delta Normally occurs for only limited periods of time over specific, localized areas. Commands can not sustain THREATCON Delta for extended periods without causing significant hardships for personnel and substantial reductions in capability to perform Normal peacetime missions.

b. The decision to implement a particular THREATCON is a command decision which should be based on an assessment of the terrorist 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 terrorist response. Frequently, information concerning the terrorist threat is limited to general descriptions of terrorist 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 already taken place. For this reason, the absence of specific information concerning the immediate terrorist threat should not preclude implementing a higher THREATCON and/or additional security measures when general information indicates an increased vulnerability or heightened risk to personnel and/or facilities.

c. Threat assessments are developed by intelligence staff officers and should be used as one source of information in determining the appropriate THREATCON 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 six terrorist threat factors:

(a) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

(b) Capability. The acquired, assessed or demonstrated level of capability to conduct terrorist attacks.

(c) Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity.

(d) History. Demonstrated terrorist activity over time.

(e) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.

(f) Security environment. The internal policy and security considerations that impact on the capability of terrorist elements to implement their intentions.

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

(a) Critical. Factors of existence, capability and targeting must be present. History and intentions may or may not be present.

(b) High. Factors of existence, capability, history and intentions must be present.

(c) Medium. Factors of existence, capability and history must be present. Intentions may or may not be present.

(d) Low. Existence and capability must be present. History may or may not be present.

(e) Negligible. Existence and/or capability may or may not be present.

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

d. 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 that pertain 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 FP of a combatant commander, through the combatant commanders 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 six factors in analyzing the threat level: existence of terrorist groups; capability to conduct terrorist acts; intentions to use terrorism against U.S. forces; history of terrorist activities; targeting of DOD assets; and the local/regional security environment.

(c) DOD uses a five-step scale to describe the severity of the terrorist threat. the five steps from lowest to highest are negligible, low, medium, high, and critical.

(d) DOD, through 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 either 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 determines corresponding threat levels (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, i.e. equipment, TDY personnel, funding, etc. (FP enhancements). 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 disorder, insurgency, and narco-terrorism), counterintelligence (the HUMINT threat posed by hostile intelligence services), 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 semi-annually. 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 long-term picture for planning and resource allocation (FP) 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 USG 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 that 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 shall ensure that all DOD personnel and their dependents in the country for whom he has FP 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 the following procedure be used to provide clarification: DOD, through DIA, shall 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 FP 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.

F-2. THREATCON Normal.

Local security measures designed for implementation when there is no credible threat of terrorist activity.

F-3. THREATCON 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.

(1) Ensure that law enforcement and security agencies have immediate access to building floor plans and emergency evacuation plans for MEVAs.

(2) Maintain the installation Crisis Management Force (CMF) on two hour recall.

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 one of the following measures from F-4, THREATCON Bravo:

(1) Regularly inspect all buildings, rooms, and storage areas not in regular use (Measure 15).

(2) 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 (Measure 16).

(3) Inspect all deliveries to messes, commissaries, exchanges, guest houses, clubs, libraries, schools and other locally-designated, common use facilities to identify explosive and incendiary devices. Use trained explosive ordnance detection dog (EODD) teams for some inspections, when available. Encourage family members to report suspicious packages to local law enforcement agencies, and refrain from handling such packages until cleared by appropriate authority (Measure 18).

(4) Increase both overt and covert security force surveillance of messes, commissaries, exchanges, guest houses, clubs, libraries, schools, chapels and other locally-designated soft targets to improve deterrence and build confidence among staff and family members (Measure 19).

g. Measure 7. Review all operations plans and orders, and SOPs which pertain to implementation of THREATCONs 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, intelligence and security agencies to monitor the threat to Army personnel, installations and facilities. Notify local police agencies concerning THREATCON Bravo measures that, if implemented, could impact on their operations in the local community.

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

F-4. THREATCON Bravo.

In addition to the measures required by THREATCON Alpha, the following measures will be implemented--

a. Measure 11. Increase the frequency of warnings required by Measure 1 and inform personnel of additional unclassified threat information, if available.

b. Measure 12. Retain CMF personnel on two hour recall. Periodically exercise two hour recall of the Special Reaction Team (SRT) and the CMF to ensure readiness.

c. Measure 13. Review provisions of all operations plans and orders, and SOPs associated with implementation of THREATCON Charlie.

d. Measure 14. Move automobiles and objects such as trash containers and crates at least 25 meters from MEVAs. 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 EODD teams, controlled access to parking areas, etc.).

e. Measure 15. 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 EODD 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 appropriate authority.

h. Measure 18. Inspect all deliveries to messes, exchanges, guest houses, clubs, libraries, schools and other locally-designated common use facilities to identify explosive and incendiary devices. Use trained EODD 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, guest houses, clubs, libraries, schools, chapels and other locally-designated soft targets 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. 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 installation MEVAs 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 (OCONUS). 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 counter-surveillance 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 THREATCON Charlie and Delta measures that, if implemented, could impact on their operations in the local community.

r. Measures 28. Implement Random Antiterrorism Measures Program (RAMP).

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

F-5. THREATCON Charlie.

The following measures will be implemented--

a. Measure 30. Continue all THREATCON Alpha and Bravo measures or introduce those which have not already been implemented.

b. Measure 31. Recall staff representatives and initiate 24 hour operation of the CMF. Place the SRT on 15 minute recall.

c. Measure 32. Reduce installation and MEVA 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 which 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 25 meters of MEVAs and other sensitive activities specified in local plans. 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 MEVAs, to include potential "soft" target areas such as housing areas, hospitals and schools.

h. Measure 37. Position guard force personnel in the vicinity of all 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.

F-6. THREATCON Delta.

The following measures will be implemented--

a. Measure 41. Continue all THREATCON Alpha, Bravo and Charlie measures, or introduce those which have not already been implemented.

b. Measure 42. Augment guard forces to ensure absolute control over access to the installation, MEVAs, and other potential target areas.

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 MEVAs, soft targets and other sensitive areas as soon as possible.

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 areas) and parking areas. Inspections at MEVAs and in the vicinity of soft targets should be conducted by security force personnel.

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.

Appendix G
Aviation THREATCON Procedures

a. General. In addition to basic THREATCON procedures, a variety of other tasks may need to be performed at aviation facilities. This is particularly true for airbases located in areas where the threat of terrorist attacks is high.

b. THREATCONs Alpha and Bravo.

(1) Planning.

(a) Review THREATCONs Alpha and Bravo measures.

(b) Update THREATCONs Alpha and Bravo measures as required.

(2) Briefing and Liaison.

(a) Brief all personnel on the threat, especially pilots, ground support crews, and air traffic controllers.

(b) Inform local police of the threat. Coordinate plans to safeguard aircraft flight paths into and out of air stations.

(c) Ensure duty officers are always available by telephone.

(d) Prepare to activate contingency plans and issue detailed air traffic control procedures if appropriate.

(e) Be prepared to receive and direct aircraft from other stations.

(3) Precautions inside the perimeter.

(a) Perform thorough and regular inspection of areas within the perimeters from which attacks on aircraft can be made.

(b) Take action to ensure no extremists armed with surface-to-air missiles can operate against aircraft within the perimeter.

(c) Establish checkpoints at all entrances and inspect all passes and permits. Identify documents of individuals entering the area--no exceptions.

(d) Search all vehicles, briefcases, packages, etc., entering the area.

(e) Erect barriers around potential targets if at all possible.

(f) Maintain firefighting equipment and conduct practice drills.

(g) Hold practice alerts within the perimeter.

(4) Precautions outside the perimeter.

(a) Conduct, with local police, regular inspections of the perimeter - especially the area adjacent to flight paths.

(b) Advise the local police of any areas outside the perimeter where attacks could be mounted and which cannot be avoided by aircraft on takeoff or landing.

(c) Advise aircrews to report any unusual activity near approach and overshoot areas.

c. THREATCON Charlie.

(1) Planning.

(a) Review THREATCON Charlie measures.

(b) Update THREATCON Charlie measures as required.

(2) Briefing and Liaison.

(a) Brief all personnel on the increased threat.

(b) Inform local police of increased threat.

(c) Coordinate with the local police on any precautionary measures taken outside the airfield's perimeters.

(d) Implement appropriate flying countermeasures specified in SOPs when directed by air traffic controllers.

(3) Precautions inside the perimeter.

(a) Inspect all vehicles and buildings on a regular basis.

(b) Detail additional guards to be on call at short notice and consider augmenting firefighting details.

(c) Carry out random patrols within the airfield perimeter and maintain continuous observation of approach and overshoot areas.

(d) Reduce flying to essential operational flights only. Cease circuit flying if appropriate.

(e) Escort all visitors.

(f) Close relief landing grounds where appropriate.

(g) Check airfield diversion state.

(4) Precautions outside the perimeter.

(a) Be prepared to react to requests for assistance.

(b) Provide troops to assist local police in searching for terrorists on approaches outside the perimeter of military airfields.

d. THREATCON Delta.

(1) Planning.

(a) Review THREATCON Delta measures.

(b) Update THREATCON Delta measures as required.

(2) Briefings and Liaison.

(a) Brief all personnel on the very high levels of threat.

(b) Inform local police of the increased threat.

(3) Precautions inside the perimeter.

(a) Cease all flying except for specifically authorized operational sorties.

(b) Implement, if necessary, appropriate flying countermeasures.

(c) Be prepared to accept aircraft diverted from other stations.

(d) Be prepared to deploy light aircraft and helicopters for surveillance tasks or to move internal security forces.

(4) Precautions outside the perimeter.

Close military roads allowing access to the airbase.

Appendix H
TRADOC Force Protection Standards and Implementing Guidance.

H-1. General.

a. This section implements standards developed to ensure the synchronization and integration of all elements of the FP Program. Successful execution of these TRADOC FP Standards will ensure compliance with mandatory DOD Standards required by DODI 2000.16, DOD Combating Terrorism Program Standards.

b. The commander's authority to enforce security measures and responsibility to protect persons and property remains paramount. Nothing in these standards shall detract from, or conflict with, the authorities and responsibilities of commanders.

c. These are performance standards which provide commanders the necessary flexibility to undertake an assessment process of their particular situation.

d. Commanders will develop more specific standards and supplement guidance as applicable to the local situation.

e. These performance standards require commanders to apply a process to assess their specific FP capabilities and implement an approach that best accomplishes the mission. In short, performing the assessment and implementation process is the methodology for

identifying the minimum tasks necessary to meet the standards. In general the tasks require commanders to:

(1) Collect and analyze terrorist threat information and threat capability.

(2) Assess vulnerabilities to terrorist attacks, and prepare and implement procedures for enhanced antiterrorism protection.

(3) Prepare and implement procedures for responding to terrorist incidents.

f. Accomplishing these standards will provide commanders with a comprehensive FP Program.

H-2. Standard 1. TRADOC Force Protection Policy.

a. TRADOC Standard. Major subordinate commands and installation commanders will develop a full working knowledge of FP policies. Further, they will communicate the spirit and intent of these policies throughout the chain of command or line of authority.

b. Implementing Guidance.

(1) Commanders will review their specific needs and produce supplemental standards in support of the TRADOC FP Standards identified in this regulation. These supplemental standards will address, at a minimum, the following:

(a) Requirements for FP Plans and supporting plans.

(b) Specific command unique FP requirements requiring the programming of resources.

(c) New construction and modifications to existing facilities FP standards.

(2) Installation commanders will issue operations plans or orders which provide FP implementing guidance to subordinate organizations.

H-3. Standard 2. Assignment of FP Operational Responsibility.

a. TRADOC Standard. Commanders will clearly establish operational responsibility for FP for all units and individuals whether permanently or temporally assigned.

b. Implementing Guidance. When responsibilities for FP 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 MOA clearly outlining FP responsibilities. Additionally, commanders will ensure that --

(1) Procedures are in place to ensure that each individual and unit is aware of who is operationally responsible for FP.

(2) Procedures are in place to ensure those personnel operationally responsible for FP are notified upon the arrival and departure of individuals and units.

H-4. Standard 3. Program and Planning.

a. TRADOC Standard. FP programs will be based on assessments of threats and vulnerabilities. FP operational planning will identify, coordinate, allocate and employ resources to ensure FP measures are developed that provide the appropriate level of protection for all applicable threats.

b. Implementing Guidance.

(1) Commanders will develop and implement a comprehensive FP Program designed to accomplish all the standards contained in this regulation. The program will include a series of well defined plans that describe and implement the program.

(a) Commanders at all levels will ensure that FP plans, orders or other implementing guidance at a minimum address procedures to collect and analyze terrorist threat information and threat capability; assess vulnerability to threat attacks and prepare and implement procedures for enhanced FP protection; and, procedures for responding to threat incidents. These plans will also implement all applicable TRADOC FP Standards.

(b) All operations plans and orders will contain an assessment of the actual threat (or absence of threat) in the "Enemy Forces" paragraph. In addition, the "Coordinating Instructions" of such plans and orders will prescribe appropriate actions for reporting threat information, responding to a threat attack and reporting threat incidents (this requirement can be met by referencing a SOP or other document that is readily available to all units/organizations responsible for

executing the plan or order). Unit movement directives will contain instructions directing a predeployment orientation concerning the threat if the unit is deploying to a country designated by DOD as a high physical or potential threat country.

(2) Commanders will integrate threat information prepared by the intelligence community, technical information from security and engineering planners, and information from other sources to prepare their assessments. Terrorist threat assessments serve as the basis and justification for recommendations on FP enhancements and program/budget requests.

(3) Commanders will --

(a) Coordinate local FP plans and orders with the supporting FBI office and state and local law enforcement agencies. Copies of approved FP plans will be provided to those organizations, within limitations imposed by policies governing dissemination of classified information, where applicable.

(b) Immediately notify the local FBI office concerning terrorist incidents occurring on TRADOC installations, facilities and activities.

(c) If the FBI assumes jurisdiction, the Attorney General will assume primary responsibility for coordinating the Federal law enforcement response. However, commanders will take all necessary actions, as dictated by the situation, to prevent loss of life or mitigate property damage before the FBI response force arrives. In addition, the command of U.S. Army elements will remain within military channels.

(d) If the FBI declines jurisdiction over an incident occurring in an area of exclusive or concurrent federal jurisdiction, the commander will take all actions necessary to resolve the incident. The FBI may act in an advisory role in situations where they decline jurisdiction.

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

(4) When official business requires travel to, or through, DOD 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. Commanders will adhere to the following policy --

(a) DA military and civilian personnel are authorized to 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) Transportation officers who arrange travel by indirect routing or on a foreign flag carrier to avoid such areas should cite 57 Comp. Gen. 519 and 522 as the justification. The use of that citation must be documented in each case and attached to each travel voucher.

(2) This citation is not authority to disregard totally the requirement in the JFTR, volume 1, to use U.S. air carriers when available. U.S. air carriers will be utilized to the maximum extent possible, even if the flight requires transiting or change of plane in a designated high or potential physical threat country. Each command may determine if the security conditions in a designated high or potential physical threat country at the time of travel warrant justification for use of foreign flag airlines or indirect routing.

(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 service.

(b) Blanket approval and reimbursement for the use of regular-fee passports is 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 shall travel on no-fee official (red) 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 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 shall 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 prior to travel.

(3) Individuals traveling solely by military air or USAFAMC charter shall not be reimbursed for regular-fee passports unless U.S. Government transportation became available on short notice (i.e., 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 travel is not authorized.

(c) Commercial airline tickets shall 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) shall be marked, at a minimum, as FOR OFFICIAL USE ONLY and handled in accordance with command directives, when their travel takes them to, or through, DOD-designated high physical or potential threat countries. Such itineraries may be classified CONFIDENTIAL or higher, when warranted by the threat and authorized by appropriate classification authority guidelines. Security classifications should be assigned to extremely detailed itineraries (those which 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 physical or potential security threat countries.

H-5. Standard 4. Committees and Working Groups

a. TRADOC Standard. Commanders will establish FP Committees to assist in the development, integration, and management of the FP Program. Additionally, commanders will establish FP Working Groups which include representation by staff officers with FP responsibilities from operations (S3, G3, DPTMS), Provost Marshal, Intelligence, Engineer, and other staff sections dependent on the situation. FP Working Groups should meet frequently to discuss the current threat and evaluate security measures that have been planned or implemented. FP Working Groups will operate under the direction of the command's FP Officer to develop issues for presentation to the FP Committee.

b. Implementing Guidance.

(1) Commanders will establish FP Committees comprised of individuals and subject matter experts that represent all elements of FP available for use by the commander in developing, monitoring and managing the FP Program. This group will provide recommendations on FP to the commander both before and after an incident has occurred. FP Committees will --

(a) Meet periodically (a minimum of semi-annually) to discuss the threat and asset vulnerabilities; review existing FP plans and guidance; and, assign priorities to funding requests, repairs, and FP construction projects.

(b) Operate under the direction of the DPTMSEC or other individual with functional staff responsibility for FP.

(c) Include at a minimum staff principals (or designated representatives) from each of the following staff sections: Provost Marshal, intelligence, engineer, information operations, logistics, medical, budget, SJA, CID and public affairs. Other personnel, to include commanders of supporting counterintelligence and local/Federal law enforcement activities; commanders of subordinate tenant units; and supported RC/other DOD/DA activities may be invited at the discretion of the commander.

(d) Provide a written record of meetings to the commander and maintain those records on file for a period of two years.

(e) Assist the commander in the completion of the annual Commander's Assessment Tool IAW TRADOC Standard 7.

(f) FP committees should meet more frequently during periods of increased threats. The FP Committee, and supporting FP Working Group, should form the nucleus of Crisis Management Forces (CMF) constituted to direct emergency operations in response to threats and threat incidents.

(2) Commanders will establish FP Working Group to ensure the integration of all available threat information with operational requirements. FP Working Groups will--

(a) Include at a minimum representation by staff officers with FP intelligence responsibilities from Provost Marshal, intelligence, CIDC and local/Federal/host nation law enforcement offices, as appropriate.

(b) Meet frequently to discuss the current threat and evaluate security measures that have been implemented or planned for implementation to counter the threat.

(c) Operate under the direction of the command's FP Officer.

(d) Develop issues for presentation to the command's FP Committee.

(e) Serve as the linkage between operations and intelligence thereby ensuring a complete and comprehensive review of the threat within the current operating environment.

H-6. Standard 5. Exercises.

a. TRADOC Standard. Commanders will institute an exercise program which develops and refines the command's FP procedures and responses to the entire spectrum of FP threats.

b. Implementing Guidance. Commanders will conduct these exercises at least annually and maintain records until the next higher headquarters review of their FP program. The purpose of the exercise is to validate the FP plan, identify weaknesses, and prepare corrective actions. Additionally, these exercises will contain:

(1) Use and evaluation of THREATCON measures.

(2) Potential threat use of WMD.

(3) Exercise of response and consequence management capabilities.

(4) Threat attacks on AIS.

(5) Use and evaluation of risk management.

(6) Use and evaluation of attack warning systems.

H-7. Standard 6. Risk Management.

a. TRADOC Standard. The Army's five step risk management process will be integrated into all FP related planning and program execution.

b. Implementing Guidance. Commanders will ensure the effective integration of risk management throughout all aspects of the FP Program. Commanders will:

(1) Develop and promulgate to appropriate levels the policy of the risk level acceptance authority.

(2) Integrate the risk management program into all aspects of the FP Program to identify, assess, control, implement and evaluate hazards and threats.

(3) Ensure that risk management is a routine part of all mission planning and operations, and is applied by leaders at all levels.

(4) Ensure that risk management training is integrated into FP training and exercises.

H-8. Standard 7. Periodic Program Review.

a. TRADOC Standard. Installation FP programs will be reviewed by their MACOM at least once every three years.

b. Implementing Guidance. Commanders will--

(1) Review lower echelon/subordinate unit's FP programs for compliance with this regulation and the standards contained therein a minimum of every three years and report completion to HQDA.

(2) Conduct an assessment of their FP Programs annually. This assessment will be conducted utilizing the Commander's Assessment Tool at appendix C to ensure a

common baseline throughout the Army. The addition of additional tasks is authorized. Due to the multi-disciplinary aspects of the FP Program, commanders will utilize their FP committees in the preparation of this assessment. Units will maintain completed assessments until the next higher headquarters review of their FP Program.

H-9. Standard 8. Force Protection Officer.

a. TRADOC Standard. Major subordinate commands, installations, and deployable units to battalion level will designate an FP Officer.

b. Implementing Guidance.

(1) Commanders will designate these individuals in writing and ensure that they receive certifying Level II training within 180 days of assumption of these duties. Unit FP Officers must be certified and current. Initial certification, as a result of successful graduation from Level II training course or certification by first 0-6 in chain of command, constitutes being current for the first 3 year period.

(2) To maintain a current status, FP Officers must take part in a comprehensive FP exercise, or attend FP training IAW DODI 2000.14 "DOD Combating Terrorism Program Procedures," a minimum of every 3 years. Documentation of currency requires signature of the first 0-5 in the chain of command.

(3) Level II training serves two purposes: it prepares an individual to manage a unit FP Program and provide subject matter expertise to the unit commander, and it trains an individual who can then provide Level I training at the unit level.

H-10. Standard 9. Development of Local THREATCON Levels.

a. TRADOC Standard. Commanders will develop a process based on terrorist threat information and/or guidance from higher headquarters to raise or lower THREATCON levels. THREATCON transition procedures and measures will be disseminated and implemented by all subordinate and tenant commanders.

b. Implementing Guidance. This process will be IAW appendix F, written and maintained in applicable FP plans. All commanders can set a local THREATCON. Subordinate commanders can raise but not lower a higher level commander's THREATCON. Additionally, commanders will ensure that--

(1) These procedures are incorporated and evaluated as part of annual FP exercises.

(2) These procedures are evaluated whenever implemented.

(3) These procedures contain provisions for after duty-hours notifications.

(4) These procedures contain provisions to notify all organic, tenant and supported RC units.

(5) There are sufficient assets to implement all THREATCON measures on-hand or available from local assets.

(6) There is a process to continuously review the effectiveness of daily physical security measures under THREATCON Normal.

(7) Successful threat operations, like military operations, rely on intelligence gathering prior to execution. Employing random security measures (Random Antiterrorism Measures Program, or RAMP) makes the threat group's task of gathering information more difficult. RAMP involves implementing multiple security measures in a totally random fashion to change the appearance of an installation/facility security program. RAMP introduces an element of uncertainty in the overall security program -- uncertainty that defeats surveillance attempts and makes effective operational planning by threat groups difficult, if not impossible.

(a) RAMP will be developed for all Army installations and facilities that have the structures, equipment, personnel and authority to control access.

(b) RAMP measures will include a selection of different types of vehicle searches (trunk, undercarriage, total), document inspections and observable security procedures designed to vary the look of the security program.

(c) RAMP will be implemented utilizing THREATCON measures located in appendix F.

(d) RAMP will be thoroughly planned to ensure measures are implemented randomly

(not in predictable patterns). Commanders will vary the types of measures along with schedules for employment of measures.

H-11. Standard 10. Weapons of Mass Destruction Planning.

a. TRADOC Standard. FP Plans, orders, SOPs, threat assessments, and coordination measures will address potential terrorist WMD threats. Commanders will assess the vulnerability of installations, facilities, and personnel within their 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.

b. Implementing Guidance. Commanders will--

(1) Develop estimates for potential terrorist use of Weapons of Mass Destruction (WMD) in their AOR. Reports throughout chain of command and line of authority will be processed immediately when significant information is obtained identifying organizations with WMD capabilities operating in their AOR. Commanders will task appropriate level units for support, ensuring all supported organic, tenant and supported RC units are considered and receive copies. Units lacking organic assets will coordinate with supporting installations or higher headquarters.

(2) Assess the vulnerability of installations, facilities, and personnel within their AOR to terrorist use of WMD. Such assessments will address potential use of chemical, biological or radiological agents.

(3) Task appropriate level units for support, ensuring all supported organic, tenant and supported RC units are considered and receive copies. Units lacking organic assets will coordinate with supporting installations or higher headquarters.

(4) Take appropriate measures to notify and protect DOD personnel and reduce the vulnerability to terrorist use of WMD. Commanders will exercise applicable measures and attack warning systems as part of their FP Exercise Program.

(a) Plans, orders, SOPs, threat assessments, and coordination measures will address the WMD threat. Units and individuals will be made aware of the WMD threat and have practiced response procedures. Clear command, control, and communication lines will be established between local, state and federal emergency assistance agencies, first responders, criminal investigation teams, and follow-on forces.

(b) All individuals and teams will be trained on the proper use and maintenance of their chemical defense equipment (CDE). CDE must be sufficient to provide immediate protection for first-responders, security forces and follow-on support, and shortfalls and additional requirements must be forwarded through command channels for resolution.

(c) Training readiness is achieved once all assigned and attached personnel, units and organizations, and family members are aware of the WMD threat, trained to identify and respond to those threats, and have exercised contingency plans which include the WMD threat.

H-12. Standard 11. First Response and Consequence Management.

a. TRADOC Standard. First responders will be officially identified, trained, and equipped to respond to both conventional and WMD attack. Detailed response plans will include: casualty triage, decontamination, evacuation, and tracking; site security, evidence preservation, and contamination control measures; and detailed interagency support and coordination measures. Annual FP exercises will test medical response and consequence management procedures, including WMD response measures.

b. Implementing Guidance: Commanders will ensure that the Medical Response and Consequence Management Program is integrated into the command's FP Program. Additionally, commanders will ensure that--

(1) Medical Response and Consequence Management exercises are conducted regularly to test the plan and assess the command's ability to respond to the threat entity use of WMD, directed energy weapons, and conventional munitions.

(2) The medical community utilizes the risk management process to assist them in assessing and controlling the risks associated with medical operations.

(3) First responders are officially designated.

(4) First responders have adequate protective equipment, including Chemical Defense Equipment.

(5) Adequate hospital support, capable of treating mass casualties to include WMD casualties, is available.

(6) Medical MASCAL and WMD scenarios are included in the FP Exercise Program.

(7) Adequate resources to support the emergency response plan are available.

(8) Response plans address mass casualty scenarios in high density population areas.

H-13. Standard 12. Command Information Program.

a. TRADOC Standard. Commanders will incorporate FP into their Command Information Programs.

b. Implementing Guidance. The PAO at each level of command will serve as the sole spokesperson for the commander on matters pertaining to FP to ensure that all official information concerning the FP program originates from a single source. Commanders will also develop an awareness program to ensure visibility to the FP 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.

(1) The PAO remains the sole spokesperson for the command until responsibility for FP is transferred to another federal agency (for example, the FBI or DOS).

(2) When responsibility is transferred to another Federal agency, the TRADOC PAO will assist that agency in the transfer. The TRADOC PAO will also continue to serve as the release authority for information concerning TRADOC involvement in the incident.

(3) PA planning and execution of FP efforts are governed by the following procedures:

(a) Army officials, commanders, senior leaders and knowledgeable individuals may be interviewed by the media about FP matters pertaining to those areas for which they are responsible. FP 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 FP programs, the following reply is appropriate: "Army policy prohibits discussing specific defensive measures in our Force Protection Program. Such disclosure could adversely affect the success of the program."

(c) The Office of the Assistant Secretary of Defense for Public Affairs (OASD(PA)) must approve all media requests to film, videotape, or photograph FP training. PAOs receiving such media requests will submit them through MACOM public affairs channels to HQDA (SAPA-MR), WASH, DC 20310. HQDA (SAPA-MR) will coordinate requests with OASD (PA) and ODCSOPS, HQDA.

(d) Prior to releasing Army-produced FP training photos, videotapes, films, or slides to the media, PAOs must obtain OASD (PA) and ODCSOPS, HQDA 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 concerning those measures. 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 360-5, chapter 3. If the terrorist act creates a chemical or nuclear accident or incident, AR 360-5, chapter 10, will govern PA actions.

(h) PAOs will immediately report all terrorist incidents through channels to HQDA (SAPA-PP) WASH 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) and ODCSOPS, HQDA approval.

(1) PAOs, after coordinating proposed releases with their local Crisis Management Force, will forward the proposal through the appropriate MACOM to HQDA (SAPA-PP). HQDA (SAPA-PP) will coordinate release with OASD (PA) and ODCSOPS, HQDA.

(2) The use of periodic, scheduled news briefings is one method to ensure that essential, factual and cleared information is provided the press during the course of an incident.

(3) In cases where the PAO releases information to the media prior to obtaining OASD (PA) approval, that information should be provided by the most expeditious means to HQDA (SAPA-MR). The intent is to ensure that information released to the public by all levels of the Army is consistent. HQDA (SAPA-MR) will provide copies of such materials to ODCSOPS, HQDA.

(j) When commands have declared a THREATCON 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 should also 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.

(l) Policy governing counterterrorism (CT) forces.

1. 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 have also said that 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."

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

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

4. All public media requests to interview or film special operations forces (SOF) personnel and training must be coordinated with the Commander, USASOC, ATTN: AOPA. Requests that deal with CT issues will be forwarded by USASOC through USASOCOM to OASD (PA) for approval. HQDA (SAPS-MR) will be an information addressee on all such requests.

H-14. Standard 13. Collection of Force Protection Intelligence Information.

a. TRADOC Standard. Commanders will have a fully integrated FP intelligence program focused and based on priority intelligence requirements (PIR) that provides the appropriate threat information to protect personnel, family members, facilities, and material in all locations and situations. The commander will ensure that production and analysis requirements are focused and based on the commander's PIR.

b. Implementing Guidance.

1. Commanders at all levels will use the DOD Terrorist Threat Level classification system to identify the terrorist threat in a specific overseas country. Army commanders will use this threat analysis as the basis for developing FP plans. Threat levels are estimates, with no direct relationship to specific THREATCON. An explanation of the THREATCON and DOD Terrorist Threat Level Classification System is located at appendix F.

2. Commanders will task the appropriate organizations under their command to collect, analyze, and disseminate terrorist threat

information as appropriate. Additionally, commanders will ensure that--

(a) Collection operations are being conducted consistent with the provisions and limitations of AR 381-10.

(b) The command has connectivity to receive threat related information from all available sources (e.g., FBI, local law enforcement, and Intell Link).

H-15. Standard 14. Threat and Vulnerability Assessments.

a. TRADOC Standard. Commanders will prepare a threat assessment for their AOR. Where the threat assessment indicates a general threat, and prior to any deployment, commanders will prepare a vulnerability assessment.

b. Implementing Guidance. Developing a comprehensive threat assessment plan is the first step in this process. From here, threat analysis is continually conducted, resulting in a threat assessment. Where the threat analysis identifies a general or specific threat, this is coupled with a vulnerability analysis of the targeted facility to produce the threat and vulnerability assessment. Specifically, commanders will--

(1) Integrate threat information prepared by the intelligence community, law enforcement community, local/host nation sources of intelligence, technical information from security and engineering planners, and other sources as deemed appropriate to the local situation to prepare these assessments. Additionally, commanders will ensure that:

(a) The entire spectrum of threats, to include terrorist use of WMD, is part of the threat and vulnerability assessment.

(b) The results of threat and vulnerability assessments are disseminated to all affected organizations (e.g., organic, tenant and supported Reserve Component units).

(c) Where specific vulnerabilities are identified that they are reviewed for appropriate classification.

(2) Utilize these threat and vulnerability assessments as the basis and justification for FP enhancements, program/budget requests, and the establishment of THREATCONs.

H-16. Standard 15. Dissemination of Force Protection Intelligence Information.

a. TRADOC Standard. Commanders will ensure FP intelligence information is disseminated in a timely manner. Current intelligence will be integrated into the FP training program.

b. Implementing Guidance. Due to the political and strategic implications of terrorist attacks on U.S. Army personnel and facilities, HQDA must be informed of terrorist threats and terrorist attacks and updated periodically during the course of such incidents. Timely and accurate reporting serves two purposes: it permits HQDA to provide appropriate support to threatened commands and it permits DOD and HQDA, in conjunction with the local PAO, to provide consistent, accurate information to the public concerning the situation. Additionally, commanders will ensure that--

(1) All information pertaining to terrorist threats, or acts of terrorism involving DOD personnel or assets in their AOR, is forwarded throughout the chain of command or line of authority as appropriate.

(2) Production and analysis requirements are focused and based on the commander's priority intelligence requirements (PIR)/contingency plans so as to support the commander's ability to assess the risk when designating THREATCON for operational planning.

(3) Written procedures are established for disseminating time sensitive threat information during duty and non-duty hours, and that subordinate commanders, through company (or equivalent) level, have developed supporting procedures.

(4) Threat information is coordinated with other staff elements involved in the FP Program through the FP Committee and FP Working Group.

(5) The "no double standard policy" (threat information distributed to military, civilian, and contractor workforce) is followed/understood when disseminating threat information.

H-17. Standard 16. Individual Training.

a. TRADOC Standard. Commanders will ensure that all military and DA Civilian personnel in their command receive the appropriate training for individual antiterrorism awareness prior to deploying or traveling outside the United States and/or territories. The individual's records will be updated in accordance with local policy. Family members will receive similar training prior to traveling outside the United States and territories on official government orders.

b. Implementing Guidance. The minimum training requirement is as follows:

(1) Level I: Individual awareness training. Level I training provides individual AT awareness training to soldiers, DA civilians, and family members deploying or traveling on government orders outside the 50 united states, its territories, and possessions. Level I training must be accomplished within six months prior to deployment/travel. Level I consists of two categories: (1) training required for deployment to negligible/low threat areas; and, (2) training required for medium or high threat areas.

(2) Level I minimum training standards for deployment to negligible/low threat areas are as follows:

(a) View the Army's AT/FP Level I training videos.

(b) Issuance of JS Guide 5260 "Service Member's Personal Protection Guide: A Self-Help Handbook to Combating Terrorism" or Service equivalent; and GTA 21-3-11, a folding card entitled "Individual Protective Measures".

(c) Recent Area of Responsibility (AOR) update for area of travel. Commanders will establish procedures to ensure access and appropriate dissemination of AOR specific guidance via the Army Message Handling System, Global Command and Communications System, Home Pages (HQDA Home Page provides access to CINC/other FP Home Pages), or Intel Link. Organizations such as RC units and Reserve Officers Training Corps (ROTC) detachments lacking organic capability are responsible for coordinating with supporting installations, higher headquarters, or other Services in the local area for this support.

(d) Level I (negligible/low threat area) training does not require a Level II qualified instructor to present the required training.

(3) Level I minimum training standards for deployment to medium or higher threat areas are as follows:

(a) Same requirements as Level I negligible/low threat areas (videos, guide and folding card, AOR update).

(b) Instruction by a qualified instructor using an approved TRADOC lesson plans. A qualified instructor is an individual who has completed Level II training or, an individual who has received formal training in AT individual protection. The first O-6 level commander in the chain of command is the lowest level authorized to designate qualified instructors of those who have not completed formal Level II training.

(4) Commanders will ensure that all personnel under their command receive Level I training prior to deploying or traveling outside the 50 United States, its territories, and possessions, and document training in the individual's training files IAW local policy. Commanders will also ensure that family members traveling outside the United States, its territories and possessions on official business (i.e., on official orders) receive Level I training. Level I training must occur within six months prior to deployment or travel.

(5) This training will not take the place of the biennial SAEDA training requirement (AR 381-12).

H-18. Standard 17. Leader Training.

a. TRADOC Standard. Individuals identified as having significant responsibilities for the command FP program will receive adequate training that provides them with the ability to train others, as well as advise the commander.

b. Implementing Guidance. Commanders will identify those key positions which require formal or refresher FP training, to include risk management, prior to assumption of duties. Such positions include, but are not limited to, installation/garrison/unit commanders; commanders/directors of stand alone facilities; operations officers (or equivalent) who are responsible for FP; unit FP Officers; medical unit commanders; and, installation staff principles responsible for supporting the FP

Program. Requirements will be forwarded through MACOMs to ODCSPER who will ensure that assignment orders clearly delineate special instructions for training prior to assignment to the gaining theater/command. For personnel not in transient, MACOM commanders will review and forecast training needs through established training channels.

(1) Training will be IAW DODI 2000.14.

(2) In addition to formal training identified in DODI 2000.14, key personnel will also receive the following training:

(a) Level II. Training for FP Officers will be IAW TRADOC Standard 8.

(b) Level III. Level III training targets 0-5 and 0-6 students in precommand (PCC) training courses. Instruction is designed to provide commanders with knowledge, skills, and abilities necessary to apply FP components to ensure unit combat power preservation.

(c) Level IV. Level IV is an executive level seminar providing focused updates, detailed briefings, and panel discussions. Seminar will include a tabletop FP wargame focusing on antiterrorism, intelligence, THREATCON management and implementation of FP actions. Target audience is 0-6 to 0-8 commanders/ personnel, nominated by MACOM commanders, who have responsibilities for FP policy, planning, and execution. Training announced by HQDA message traffic.

H-19. Standard 18. Hostage Training.

a. TRADOC Standard. Personnel assigned to Medium or High Terrorist Threat Level areas, will receive guidance at least annually on appropriate conduct in the event they are taken hostage or kidnapped.

b. Implementing Guidance. Commanders will ensure DOD personnel and dependents assigned to Medium and High Threat locations are given guidance, at least annually, on appropriate conduct in the event they are taken hostage or kidnapped. Commanders will ensure that Level II certified/current instructor is utilized for establishing this program. Training can be accomplished via the commands information program and appropriate service videotapes, or during scheduled Level I training.

H-20. Standard 19. Training in Support of High Risk Personnel.

a. TRADOC Standard. Commanders will ensure that HRP and their family members are made aware of risks and trained in personal protective measures. Additionally, support staff such as drivers, aides, and protective services details will be trained and equipped.

b. Implementing Guidance. Commanders will ensure personnel designated as personnel at high risk to terrorist attack and personnel assigned to high risk billets receive appropriate training prior to assuming duties. Training will be accomplished utilizing recognized courses identified in DODI 2000.14.

H-21. Standard 20. Resource Management.

a. TRADOC Standard. FP requirements will be prioritized by the Commander (with assistance by the FP Committee) based on the threat, documented vulnerabilities, regulatory requirements, and/or command directives. Funds supporting the FP program will be tracked and accounted for.

b. Implementing Guidance. Commanders will ensure that--

(1) The proper people are involved in requirements generation, and are familiar with the FP program in order to identify those projects (within their programs) that belong in the FP Program.

(2) An acceptable standard is applied to justify and prioritize FP projects, and the justification is based upon a documented threat, regulatory guidance; or, in the absence of a quantifiable threat, potential future threats.

(3) The MACOM proponent identifies funding requirements during the Program Objective Memorandum (POM) budget development cycle. When critical requirements are not funded in the POM, the MACOM functional proponent will conduct an analysis and inform the commander of associated risks. The status of funding support will be an agenda item at each FP Committee meeting.

(4) Unforeseeable requirements which are generated due to a rapid change in the threat environment, or threat capabilities, are

reviewed for local reprogramming actions prior to submission to the next higher headquarters. Those projects which become unfunded due to FP reprogramming may then be reported as unfinanced requirements (UFRs) in the Normal budgetary process.

(5) Operations and Maintenance, Army (OMA) funding provided to the MACOMs is used for the purchase of equipment that does not exceed the $100k ceiling. For purchases that exceed this amount, Other Procurement, Army (OPA)-3 funds are required. These limited funds are managed by DAMO-ODL and requirements are to be submitted on a yearly basis for prioritization and potential funding.

H-22. Standard 21. Information Operations Integration.

a. TRADOC Standard. Commanders will ensure that Information Operations is integrated into all FP planning and program execution. Commanders will ensure integration of relevant laws and regulations pertaining to security monitoring of the command's network information infrastructure.

b. Implementing Guidance. Commanders will ensure that--

(1) Provisions of AR 380-19, Information Systems Security (ISS), are integrated into the command's FP Program.

(2) All elements of IO (e.g., OPSEC, Public Affairs, and COMSEC monitoring) are integrated into the FP Program.

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

(4) Incident reporting procedures are published for system administrators IAW the C2 Protect Implementation Plan.

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

(6) Provisions of AR 530-1, Operations Security, are integrated into all elements of the command's FP Program (e.g., physical security, law enforcement and operations).

(7) IO, C2 Protect, and ISS are included in threat briefings and assessments provided to the command.

H-23. Standard 22. Information Operations Threat and Vulnerability Assessments.

a. TRADOC Standard. Commanders will ensure friendly information systems are included in threat and vulnerability assessments. Commanders will ensure C2 Protect procedures and techniques are developed to detect and deny unauthorized intrusion to the communication network.

b. Implementing Guidance. Commanders will ensure that --

(1) An annual vulnerability assessment of their information systems is conducted.

(2) A methodology is in place to protect, detect, and react to computer intrusions. Commanders will utilize the C2 Protect Implementation Plan 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 has identified specific requirements for tools.

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

(5) Ensure that the OPSEC process is applied in determining threats and vulnerabilities to the command's communications infrastructure.

(6) Countermeasures are routinely tested (e.g., user IDs, passwords, and audit trails).

(7) All security incidents/violations (e.g., viruses, unauthorized entries or attempts, and password compromises) are analyzed, reviewed, investigated and reported.

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

(9) Identification and authentication (i.e., user id and password) is required for access to all systems.

(10) The OPSEC process is applied in developing countermeasures for the communication infrastructures.

H-24. Standard 23. Information Operations Training.

a. TRADOC Standard. Commanders will develop information security and awareness training and will develop management methodologies to evaluate risks associated with operations of information networks.

b. Implementing Guidance. Commanders will ensure formal assignment of responsibilities for the execution of the Command and Control Protect (C2P) Program. The program must establish a professional career program for experts in the C2 protect field, to include those in such specialties or subspecialties as C4 Security CI, active and passive technical countermeasures, and investigative and analytical fields. Commanders will ensure--

(1) Designation of a MACOM Information Systems Security Program Manager.

(2) Designation below MACOM, and at DA Staff and field operating agencies, of an Information System Security Manager (ISSM), at all appropriate levels.

(3) Designation of an Information System Security Officer (ISSO) for each AIS.

(4) Designation of a Network Security Officer (NSO) for each identified network.

(5) Designation of a Terminal Area Security Officer (TASO) for each terminal or group of terminals not under the control of a ISSO or NSO.

(6) Development of formal training requirements, to include resource identification, based upon local need.

(7) That where both system security and network maintenance functions are performed by the same person, that the requirements of AR 380-19 and the C2 Implementation Plan are met.

H-25. Standard 24. Security Engineering.

a. TRADOC Standard. FP will be considered in standard Army design practice with security measures that are based on risk and threat analysis.

b. Implementing Guidance. Commanders will ensure that--

(1) FP design considerations have been considered and included in the command's construction program IAW AR 415-15.

(2) Recommended protective measures are based on risk and threat analysis.

(3) Risk analysis for all new construction projects and renovations of MEVAs are performed IAW the procedures outlined in DA PAM 190-51.

H-26. Standard 25. Security Planning.

a. TRADOC Standard. Commanders at all levels will plan, based on risk analysis, for security of assets entrusted to them. Plans will be affordable, effective, and attainable. Plans will tie security measures together and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. Planning must ensure that requirements at each THREATCON have been addressed.

b. TRADOC Implementing Guidance. Commanders must plan for security of assets entrusted to them. Plans must be affordable, effective and attainable. Plans will tie security measures together and integrate security efforts by assigning responsibilities, establishing procedures, and ensuring subordinate plans complement each other. Planning must ensure that requirements at each THREATCON have been addressed, to include, responsibility assigned for execution of measures, adequate local implementation guidance, and assurance that adequate resources are available. Additionally, commanders will--

(1) Incorporate installation physical security initiatives into the Installation Master Plan. These initiatives should:

(a) Reduce installation/facility vulnerabilities in a manner that deters threat attack.

(b) Reduce physical security program costs.

(c) Inspire an appropriate level of confidence in the commander's ability to protect personnel and assets.

(2) Ensure that the FP Plan must be tailored to meet local needs based upon the principles of risk management. Security

measures will be tailored to counter the assessed threat.

H-27. Standard 26. Physical Security Threat Assessment.

a. TRADOC Standard. PS programs will be based on local threat and vulnerability assessments which are updated at least annually.

b. Implementing Guidance. These assessments will consider the range of identified and projected threats against a specific location or installation personnel, facilities and other assets. The assessment will address vulnerabilities and solutions for enhanced protection of personnel and resources. All assessments will be reviewed at least annually, and updated as appropriate.

H-28. Standard 27. Mission Essential/Vulnerable Areas.

a. TRADOC Standard. MEVAs, areas which are critical to mission accomplishment or are vulnerable to theft/damage/ attack, will be identified in order to focus security efforts.

b. Implementing Guidance. Commanders will ensure that--

(1) All MEVAs are identified, prioritized, and approved by the commander IAW AR 190-13.

(2) Periodic reviews are conducted IAW AR 190-13 to update areas designated as MEVAs.

H-29. Standard 28. Restricted Areas.

a. TRADOC Standard. Areas which are considered critical or sensitive will be identified and formally designated as "Restricted Areas" in order to give commanders legal authority to impose special access controls.

b. Implementing Guidance. Commanders will ensure that--

(1) Restricted areas are identified and designated IAW AR 190-13.

(2) Restricted areas are correctly posted.

H-30. Standard 29. Inspections and Surveys.

a. TRADOC Standard. Periodic formal reviews by security specialists will be conducted in order to assess physical security programs and to ensure compliance with security standards for protection of MEVA.

b. Implementing Guidance. Commanders will ensure that--

(1) Installation surveys conducted at least every three years to assess installation physical security posture.

(2) Physical security inspections of MEVAs conducted every 18 months for arms, ammunition and explosives storage facilities and every two years for others types of MEVA.

H-31. Standard 30. Employment of Security Measures.

a. TRADOC Standard. Appropriate physical and procedural measures will be employed which provide integrated deterrence, detection and defense capabilities in order to safeguard all personnel and material assets.

b. Implementing Guidance. Commanders will ensure that--

(1) Detection and assessment measures are integrated with defense (delay) measures to protect personnel and material assets.

(2) Security engineering surveys are conducted when planning new facilities or renovating existing facilities.

(3) Risk and threat analysis is utilized in the development of any protective measures beyond those specifically requiring employment by regulation.

(4) TM 5-853-1 is used in the development and employment of security measures.

H-32. Standard 31. Antiterrorism.

a. TRADOC Standard. Commanders will develop AT programs that provide standards, policies and procedures to reduce the vulnerabilities of all personnel including DOD

military, civilians, and family members from terrorist attack. AT programs will include installation-wide terrorist response plans which include procedures for determining the nature and scope of terrorist incidents, post incident response and reconstitution.

b. Implementing Guidance. Commanders will--

(1) Prepare installation-wide terrorist incident response plans. These plans will include procedures for determining the nature and scope of post-incidence response measures, and plans to reconstitute the installation's ability to perform AT/FP measures. Response plans will also include provisions to address the following:

(a) THREATCON measures.

(b) Threat use of WMD.

(c) Medical response and consequence management capabilities.

(d) Threat AIS attacks.

(2) Ensure Terrorist Incident Response plans contain current residential location information for all DOD personnel and their dependents assigned to Medium and High Terrorist Threat Level areas. Such plans will provide for enhanced security measures and/or possible evacuation of DOD personnel and their dependents. Commanders will develop procedures to ensure periodic review, update and coordination of these plans with appropriate responders.

(3) Develop an attack warning system utilizing a set of recognizable alarms and reactions for potential emergencies, as determined by the threat and vulnerability assessment. Commanders will ensure personnel are trained in recognition and exercise the attack warning system as part of their FP Exercise Program.

H-33. Standard 32. Residential Security Assessment for Off-Post Housing.

a. TRADOC Standard. Commanders in Medium or High Terrorist Threat Level areas will conduct physical security assessments of off-post residences for permanently assigned and TDY personnel. Based on the assessment results, commanders will provide antiterrorism recommendations to the residents and facility owners. Personnel assigned to Medium or High Terrorist Threat Level areas and not provided on-installation or other government quarters, will be furnished guidance on the selection of private residences to mitigate risk of terrorist attack.

b. Implementing Guidance.

(1) Commanders will ensure DOD personnel assigned to Medium or High Terrorist Threat Level areas, and not provided on-installation or other government quarters, are furnished guidance on the selection of private residences to mitigate risk of terrorist attack. Commanders will utilize the guidance contained within the DOD Handbook and supplement with local threat considerations, as appropriate.

(2) 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 the same terrorist threat, terrorist risk and vulnerability criteria as that used to assess the safety and security of other facilities or installations housing Army personnel on installations within the AOR.

H-34. Standard 33. Facility and Site Evaluation/Selection Criteria.

a. TRADOC Standard. Commanders will develop a prioritized list of FP factors for site selection teams. These criteria will be used to determine if facilities, either currently occupied or under consideration for occupancy, can adequately protect occupants against terrorist attack.

b. Implementing Guidance. Commanders will develop lists targeted to address the appropriate level terrorist threat and vulnerability assessment, and be based upon guidance contained within the DOD Handbook.

H-35. Standard 34. Law Enforcement Operations.

a. TRADOC Standard. Law enforcement operations will support installation FP requirements through the commander's authority to enforce federal law and Army regulations. In the event of acts of terrorism on installations, military and DOD police will take immediate action to resolve the incident and prevent loss of life. Terrorist incident response plans will include the use of law enforcement as first responders and provide

procedures for employing police resources effectively.

b. Implementing Guidance. Commanders will ensure that--

(1) Adequate law enforcement contingency plans for emergency situations (e.g., bomb threats, hostage taking, base closures and increased THREATCON levels) are developed and exercised.

(2) Exercise results are provided to the Commander through the FP Committee.

(3) Each command/activity supporting these plans been given the opportunity to participate in the creation of the plan and are in receipt of a copy of the plan.

(4) Plans address backfill of law enforcement personnel during deployments.

H-36. Standard 35. Law Enforcement Liaison.

a. TRADOC Standard. PM will conduct effective liaison with federal, state, local and host nation agencies, as appropriate, to ensure criminal intelligence is shared and that plans and operations supporting FP are coordinated.

b. Implementing Guidance. Commanders will ensure that--

(1) Coordination of security plans includes applicable federal, state, local and host nation officials outlining movement, security, and jurisdictional responsibilities.

(2) Liaison is conducted to ensure criminal intelligence, to include U.S. domestic threat information, is properly gathered, processed, and passed.

(3) This information is coordinated through the FP Committee and FP Working Group.

(4) Law enforcement operations are coordinated with the appropriate federal, state, local and host nation agencies.

H-37. Standard 36. Identification and Designation of High Risk Personnel.

a. TRADOC Standard. Commanders will ensure that 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 in order to make them eligible for special control/security measures.

b. Implementing Guidance.

(1) Personnel may be designated high risk based on assignment to a high-risk billet (HRB) or based on personal factors, regardless of position. Examples of the former include senior general officers serving in prominent positions who could serve as symbolic targets for terrorist attack and U.S. military personnel of all ranks operating in areas where there is an active insurgency or frequent anti-U.S. violence. Examples of the latter include personnel who have established worldwide or regional prominence that transcends position.

(2) Within 90 days of publication of this regulation, commanders will report to HQ TRADOC (ATBO-J) all personnel designated as Level I HRP within their geographical areas of responsibility. Subsequent to that initial report, commanders will submit an annual report to HQ TRADOC (ATBO-J), listing all Level I HRP within their geographical areas of responsibility effective on 1 October of each year. Such reports will reach HQ TRADOC not later than 1 November. Changes to Level I HRP lists will be reported within 14 days to HQ TRADOC (ATBO-J). All reports will include the position of HRP (if designation is based on HRB), incumbent's name (or name of individual whose designation is not based on a HRB), and location (installation, military community, or city).

H-38. Standard 37. Protective Measures for Safeguarding High Risk Personnel.

a. TRADOC Standard. Commanders will take appropriate measures to provide enhanced protection to HRP.

b. Implementing Guidance.

(1) HRP will be designated and protected IAW AR 190-58. Additionally, commanders will ensure that--

(a) Reviews of supplemental security needs are undertaken within 72 hours of a change in THREATCON assigned to an AOR containing high risk billets or to which HRP

have been assigned, and immediately upon receipt of specific targeting information.

(b) Heavy Armored Vehicles (HAVs) will only be used to protect personnel designated by MACOM commanders as HRP IAW AR 190-58.

(c) Personnel performing protective services duties for HRP-1 are selected using criteria in AR 190-58. Additionally, Protective Service Details (PSD) will be trained, organized and equipped IAW AR 190-58.

(2) A PSVA will be performed by the supporting USACIDC office for HRP when requested or directed. A PSVA is intended to identify security weaknesses in the individual's living and working environments, travel between those locations, and the HRP's personal activities, and identify measures to correct those weaknesses.

GLOSSARY

Section I
Abbreviations

AA&E
Arms, Ammunition, and Explosives

ACIC
Army Counterintelligence Center

AIS
Automated Information Systems

AOC
Army Operations Center

AOR
Area of Responsibility

AT
antiterrorism

ATOIC
Antiterrorism Operations and Intelligence Cell

C2
command and control

C4
command, control, communications, and computer systems

CAC
Combined Arms Center

CALL
Center for Army Lessons Learned

CASCOM
Combines Arms Support Center

CDE
chemical defense equipment

CFSO
counterintelligence force protection source operations

CI
counterintelligence

CMF
Crisis Management Force

COA
course of action

COE
chief of engineers

CONUS
continental United States

CPA
Chief of Public Affairs

CT
counterterrorism

DA
Department of the Army

DOD
Department of Defense

DODD
Department of Defense Directive

DODI
Department of Defense Instruction

EAC
echelon above corps

FBI
Federal Bureau of Investigation

FP
Force Protection

FPC
Force Protection Committee

FPO
Force Protection Officer

FPP
Force Protection Program

HRB
high risk billet

HRP
high risk personnel

HUMINT
human resource intelligence

IAW
in accordance with

INFOSEC
information security

IO
information operations

ISSM
information system security manager

ISSO
information system security officer

MACOM
Major Army Command

MCA
military construction, Army

MDEP
management decision package

MEVA
mission essential vulnerable area

MWD
military working dogs

NSO
network security officer

OCONUS
outside continental United States

PA
public affairs

PAO
public affairs officer

PAG
public affairs guidance

PCS
permanent change of station

PM
provost marshal

PS
physical security

PSVA
personal security vulnerability assessment

PSD
protective service detail

RAMP
random antiterrorism measures program

SAEDA
Subversion and Espionage Directed Against US Army

SJA
Staff Judge Advocate

SOP
standing operating procedures

SRT
special reaction team

TASO
terminal area security officer

TDY
temporary duty

THREATCON
threat condition

TIG
The Inspector General

TRADOC
United States Army Training and Doctrine Command

WMD
weapons of mass destruction

USACE
United States Army Corps of Engineers

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. Also called AT.

AT Awareness
Fundamental knowledge of the terrorist threat and measures to reduce personal vulnerability to terrorist acts.

AT Resident Training
Formal classroom instruction in designated DOD courses that provide specialized instruction on specific combating terrorism topics; i.e., personal protection, terrorism analysis, regional interest, and AT planning.

Combating terrorism
Actions, including antiterrorism and counterterrorism taken to oppose terrorism throughout the entire threat spectrum.

Counterintelligence
Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs.

Counterterrorism
Offensive measures taken to prevent, deter, and respond to terrorism. Also called CT.

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

Crisis Management Force (CMF)
An installation's assets capable of reacting to an incident.

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.

Force protection
Security program developed to protect soldiers, civilian employees, family members, facilities and equipment, in all locations and situations. This is accomplished through the planned integration of combating terrorism (AT/CT), physical security, information operations, personal services and law enforcement operations, all supported by the synchronization of operations, intelligence, training and doctrine, policy and resources.

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
U.S. material resources and facilities, because of mission sensitivity, ease of access, isolation, and symbolic value may be an especially attractive or accessible terrorist target.

Information operations (IO)
As one of the components of FP, encompass those continuous military operations within the military information environment (MIE) that enable, enhance and protect the friendly force's ability to collect, process and act on information to achieve an advantage across the full spectrum of military operations. IO include interacting with the global information environment (GIE) and exploiting or denying an adversary's information and decision-making capabilities.

Installation
A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base.

Installation commander
The individual responsible for all operations performed by an installation.

International (or transnational) terrorism
Terrorism in which planning and execution of the terrorist act transcends national boundaries. In defining international terrorism, the purpose of the act, the nationalities of the victims, or the resolution of the incident are considered. Those acts are usually planned to attract widespread publicity and are designed to focus attention on the existence, cause, or demands of the terrorists.

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

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine indicators hostile 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. Also called OPSEC.

Physical security
That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

Prevention
The security procedures undertaken by the public and private sector in order to discourage terrorist acts. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Risk management
Process of identifying and controlling hazards to protect the force and increase the chance of mission accomplishment. Applicable to any mission and environment. Five steps are: Identify hazards; Assess hazards; Develop controls measures and make risk decisions; Implement controls; and Supervise and evaluate.

Special reaction team
A unit of specially trained military or DOD police personnel operating under the auspices of the PM, the Chief of Security, or the Chief of Security Police, armed and equipped to respond to and to resolve special threat situations above and beyond the scope of standard or usual law enforcement capabilities.

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. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Terrorist
An individual who uses violence, terror, and intimidation to achieve a result. (Approved for inclusion in the next edition of Joint Pub 1-02.)

Terrorist threat conditions
A Chairman, Joint Chief of Staff (CJCS) approved program standardizing the military services' identification of and recommended responses to terrorist threats against U.S. personnel and facilities. Also called THREATCONs, this program facilitates inter-service coordination and support for AT activities.

Threat analysis
In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment.

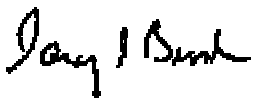
Threat and vulnerability assessment
In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis.

Weapons of mass destruction (WMD)
Weapons that are capable 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, and radiological weapons, but excludes the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon.

FOR THE COMMANDER:

OFFICIAL:

JAMES J. CRAVENS, JR.
Major General, GS
Chief of Staff



GARY E. BUSHOVER
Deputy Chief of Staff
for Information Management