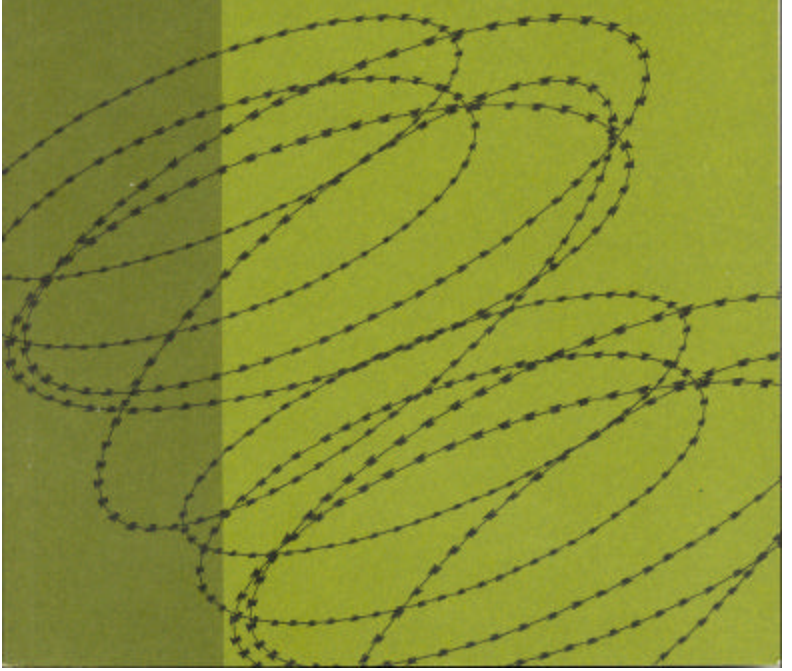
Installation Commander's

FORCE PROTECTION Handbook

July 2002



POC

Agency	Name	Phone Numbers

Foreword

JOHN N. ABRAMS
General, U.S. Army
Commanding

In the span of ninety agonizing minutes on 11 September 2001, four groups of terrorists armed with only knives and box cutters inflicted more damage and wreaked more havoc on American soil than any near-peer, conventional threat had ever done before. The sobering events of that tragic day compel American military and civilian leaders to reassess force protection programs to identify and negate vulnerabilities. The contemporary operational environment requires leaders to plan for threats across the full spectrum and to instill awareness in all members of our workforce, both civilian and military, that force protection begins with each of us.

Force protection starts at home. It must be an integral part of the way we live and train at TRADOC installations as well as a mainstay of power projection and deployed force operational considerations. This handbook is designed to provide installation commanders and their staffs some of the key tools to assess and enhance force protection readiness in and around their installations. It is not intended to be a single-source guide for techniques and procedures, but it focuses important staff functions and enhances force protection programs at TRADOC schools and centers. It provides the azimuth needed to guide proactive and comprehensive efforts to thwart terrorist operations, disrupt terrorist planning and timing, detect and defeat attacks on communications systems, and deter potential threats.

JOHN N. ABRAMS
General, U.S. Army
Commanding

Installation Commander's
Force Protection Handbook

Contents

Foreword

Chapter 1 **Introduction**

Scope 1-1
Purpose 1-1
Application 1-2
Definitions 1-2
Focus 1-2
Goal 1-3
Objectives 1-3
Spectrum 1-3
Antiterrorism Critical Tasks 1-3
Elements 1-5

Chapter 2 **Security**

Overview 2-1
Three-Ringed Security System (Operational Construct) 2-1
Installation Major Security Missions 2-4
Intelligence Gaps (Three Concentric Rings) 2-4

Chapter 3 **Antiterrorist Critical Tasks**

Task 1: Establish an Antiterrorism Program 3-1
Task 2: Collect, Analyze, and Disseminate Threat Information 3-4
Task 3: Assess and Reduce Critical Vulnerabilities (Conduct Antiterrorism Assessments) 3-7

Task 4:
Increase Antiterrorism Awareness
in Every Soldier, Civilian,
and Family Member 3-9

Task 5:
Maintain Installation Defenses
IAW Force Protection Conditions 3-10

Task 6:
Establish Civil/Military Partnership
for Weapons of Mass Destruction Crisis 3-11

Task 7:
Develop Plans for Reporting and
Responding to a Terrorist Threat/Incident 3-13

Task 8:
Conduct Exercise and
Evaluate/Assess Plans 3-14

Chapter 4 **Functions and Planning Considerations**

Introduction 4-1
Command and Control 4-1
Operations 4-1
Logistics 4-2
Health Services 4-3
Resource Management 4-4
Engineering 4-4
Contracting and Purchasing 4-5
Communications and Information Systems 4-5
Personnel 4-6
Army Community Service 4-6
Special Staff Functions 4-6

Chapter 5 **Critical Information**

Overview 5-1
Commander's Critical Information Requirements 5-1

Chapter 6 **Tiered Response Capabilities**

Overview 6-1
Internal Assets 6-1
External Assets 6-9

Chapter 7 **Installation Operations Center**
Overview 7-1
Capability 7-1
Mission 7-1
Characterists 7-2

Chapter 8 **Information Operations**
Overview 8-1
Information Assurance 8-1
Threats 8-4
Approved Information Assessment Tools 8-5
Information Operations Conditions 8-6
Installation Commander's
Information Assurance Guide 8-9

Chapter 9 **Lessons Learned**
Security 9-1
First Responders 9-3
Intelligence 9-3
Command, Control, and Communications 9-4
Bomb Threat 9-6

Appendix A **The Military**
Decision-Making Process A-1

Appendix B **Decision Support Template** B-1

Appendix C **Synchronization Matrix** C-1

Appendix D **Execution Matrix** D-1

Appendix E **Running Estimates** E-1

Appendix F **Troop-Leading Procedures** F-1

Appendix G **Warning Order** G-1

Appendix H **Risk Management** H-1

Appendix I **Training and Planning Assistance** I-1

Appendix J **Rules for the Use of Force** J-1

Appendix K **Installation Watch Card** K-1

Appendix L **Force Protection Conditions**
Measure Tracking Chart L-1

Appendix M **News Release**.....M-1
Appendix N **Suspicious Mail** N-1
Appendix O **Family Media Guide** O-1
Appendix P **Suspicious Incident Reporting Procedures**..... P-1
Glossary..... Glossary-1
Bibliography Bibliography-1

Chapter 1

Introduction

SCOPE

1-1. This handbook provides techniques and procedures governing the conduct of force protection (FP) measures at TRADOC installations. It provides a basis for understanding TRADOC policies and objectives related to FP. More importantly, this handbook provides installation commanders and their staffs some needed tools to help organize, plan, train for, and implement effective FP programs utilizing the resources at their disposal (in conjunction with available local, state, and federal support). The primary documents that provide the basis for the FP handbook (FPHB) are the draft FP operational and organizational (O&O) concept, Army Regulation (AR) 525-13, United States Army Installation Commanders' Guide (Antiterrorism and Force Protection) and United States Army Installation Commanders' Blueprint (Installation Preparedness for Weapons of Mass Destruction), and AR 380-19 (which will be replaced by AR 25-IA and DA Pam 25-IA). The FPHB is not intended to be all-inclusive, nor does it relieve commanders and their staffs from their obligation to comply with statutory and regulatory requirements.

PURPOSE

1-2. This handbook has four purposes —

- ??To explain important aspects of FP.
- ??To serve as an FP information source and quick reference for installation commanders and their staffs.
- ??To operationalize the antiterrorism (AT) tasks.
- ??To consolidate current key FP guidelines that are detailed in other references.

1-3. It is not the intent of this publication to restrict the authority of installation commanders from organizing resources or undertaking any measures deemed necessary to enhance FP program effectiveness.

APPLICATION

1-4. This handbook was compiled for TRADOC installation commanders and their staff elements. The material was extracted from regulations, guidance, and lessons learned applicable to FP. The FPHB aids TRADOC commanders in developing their FP plan and procedures to deter and defend against attackers and in establishing an effective response that saves lives and contains damage.

DEFINITIONS

1-5. JP 3-0 and FM 3-0 define FP as "actions taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place, and incorporates the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. FP does not include actions to defeat the enemy or protect against accidents, weather, or disease." AR 525-13 adds futher detail, explaining that FP is a "security program to protect soldiers, civilian employees, family members, information, equipment, and facilities in all locations and situations. This is accomplished throught the planned integration of combating terrorism (Cbt-T), physical security (PS), information operations (IO), high-risk personnel (HRP) security, and law enforcement operations; all supported by foreign intelligence, counterintelligence, and other security programs."

1-6. AR 525-13 defines Cbt-T as the combination of "all actions, including AT, counterterrorism, consequence management and intelligence support taken to oppose terrorism throughout the entire threat spectum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE)."

1-7. AR 525-13 defines AT as "defensive measures used to reduce vunerability of individuals and property to terrorist acts, to include limited response and containment by local military forces."

FOCUS

1-8. Clearly, FP is a broad subject that includes many functions outside the installation commander's span of control. The focus of this handbook is on those proactive measures that the installation commander can implement to

build an FP program. A critical element of the installation's proactive FP program includes activities to thwart terrorist operations, disrupt terrorist planning and timing, detect and defeat attacks on communications systems, and deter potential threats.

GOAL

1-9. The goal of FP is to protect soldiers, DA civilians, their family members, facilities, information, and other materiel resources from terrorism.

OBJECTIVES

1-10. DOD's FP objectives are—

??To deter incidents.

??To employ countermeasures.

??To mitigate effects.

??To recover from an incident.

SPECTRUM

1-11. The spectrum of FP includes pre-incident, incident, and post-incident tasks and activities. To achieve a comprehensive FP program requires that the full cycle of planning, preparation, execution, and continuous assessment be accomplished before, during, and after a threat event. A complete FP operation crosses the entire spectrum from pre-incident to post-incident.

ANTITERRORISM CRITICAL TASKS

1-12. AR 525-13 establishes eight AT critical tasks commanders must implement to obtain DOD's FP objectives. The eight AT critical commander's tasks are—

??Establish an AT program.

??Collect, analyze, and disseminate threat information.

??Assess and reduce critical vulnerabilities.

??Increase AT awareness in every soldier, civilian, and family member.

??Maintain installation defenses in accordance with (IAW) FP conditions (FPCON).

??Establish civil/military partnership for weapons of mass destruction (WMD) crisis.

??Plan terrorist threat/incident response.

??Conduct exercises and evaluate/assess AT plans.

1-13. Figure 1-1 provides a clear understanding of how the FP goal, objectives, spectrum, and AT critical tasks fit together. It illustrates two important points—first, the relationship between AT tasks and FP objectives and, second, it emphasizes the AT tasks across the entire spectrum of FP, from pre-incident to post-incident. One key aspect is the effect that accomplishing five of the AT tasks has on the deterrence

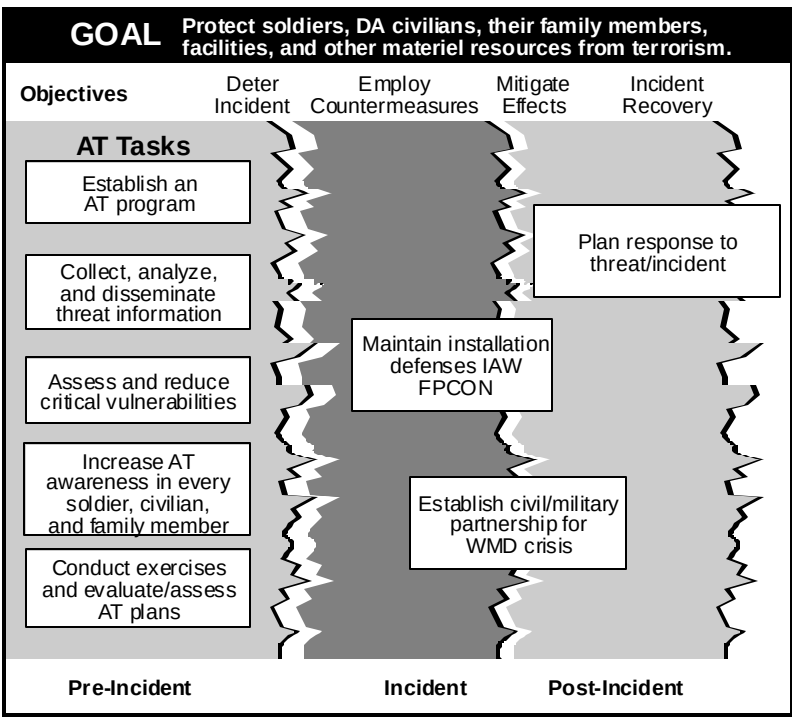


Figure 1-1. FP Goal, Objectives, Spectrum, and AT Tasks Relationships

objective. To ensure these tasks are effective requires asymmetric thinking, making sure your threat assessment is more than a mechanical process, blending a campaign quality into your FP process, achieving a reliable command and control (C^2) capability, and determining the required resources. Chapter 3 focuses on these tasks and how their integration achieves FP.

ELEMENTS

1-14. An FP program synchronizes five elements: AT, PS, HRP security, IO, and law enforcement. By integrating these components with intelligence support, the level of FP is raised thus reducing the number of vulnerabilities and the abilities of threats to plan and conduct attacks against US forces and installations. Security is the total spectrum of procedures, facilities, equipment, and personnel employed to provide a secure environment. AT is the defensive element of combating terrorism to reducing vulnerabilities and includes limited response and containment by local military forces. PS is those physical and procedural measures designed to deter, detect, and defend personnel, property, equipment, facilities, information, and material against espionage, terrorism, sabotage, damage, misuse, theft, and other criminal acts. HRP security is those additional security measures provided 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. IO encompasses those continuous military operations 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. This includes providing for the restoration of information systems by incorporating protection, detection, and reduction capabilities. The fifth element of FP is law enforcement that includes a visible deterrent to threats; the initial response to security-related incidents; investigation of incidents; a valuable resource for the collection, processing, and dissemination of criminal intelligence; and formal liaison with civilian and other military law enforcement agencies.

1-15. Figure 1-2 portrays the relationship of the AT tasks to the whole FP program. The FP goal factors (personnel, critical resources, and information) are in the center encircled by the FP elements. The outer ring of boxes is the AT tasks. When these tasks are accomplished, an effective FP program is in place to protect personnel, information, and critical resources from threat incidents.

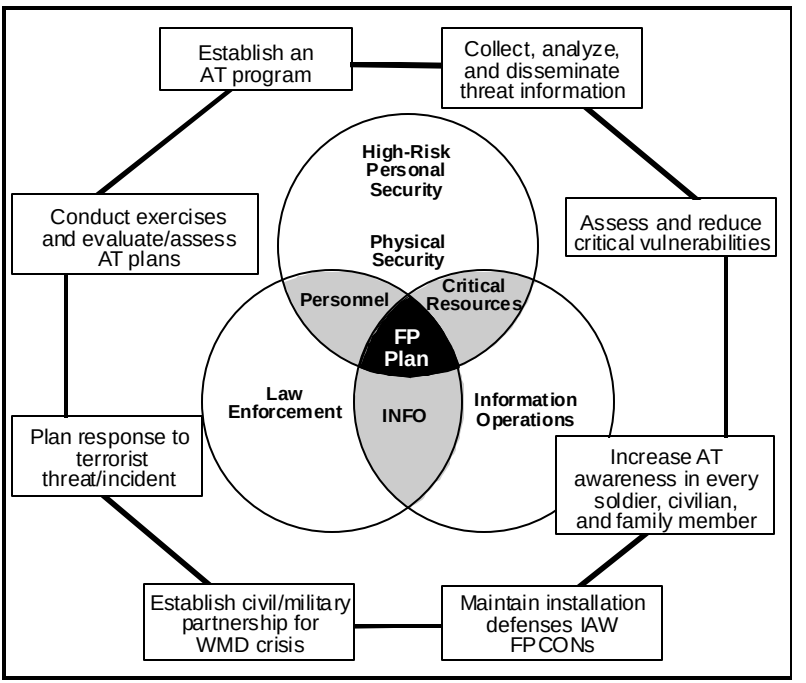


Figure 1-2. FP Goals, Elements, and AT Tasks Relationship

Chapter 2

Security

OVERVIEW

2-1. The essence of security on installations, at locations off post where military personnel reside, and during in-transit operations, is nested in the integration of policy, doctrine, personnel, materiel, training, intelligence, and planning. This integration achieves the maximum return on investment while allowing the installation commander to accept certain risks yet capitalize on optimum countermeasures. The history of shortcomings found in previous FP and PS regulatory compliance inspections has continued in the US Army Training and Doctrine Command (TRADOC) and Army FP assessments following the 11 September 2001 terrorist attacks on the World Trade Center and Pentagon. Many of these shortcomings are procedural faults, compounded by constraints on materiel and personnel resourcing priorities. Viewing installation security as a three-ringed or three-layered environment focused on major security missions improves FP by shifting the focus from physical to full-spectrum security.

THREE-RINGED SECURITY SYSTEM (OPERATIONAL CONSTRUCT)

2-2. The draft FP O&O plan introduces the concept of an installation battlespace that is analogous to the battlespace for combat operations as defined in FM 3-0 (Figure 2-1). The battlespace of an installation commander is based on his concept of the operation, accomplishing the mission, and protecting the force. A higher commander will not assign battlespace; rather, the installation commander uses experience, professional knowledge, and understanding of the situation to visualize and change his battlespace as current operations transition to future operations. The installation boundary is the area of operations (AO). The AO consists of the inner ring that must be protected, such as:

??Mission-Essential Vulnerable Areas (MEVA)—Facilities or activities within the installation that, by virtue of their function, are evaluated by the commander as vital to the successful

accomplishment of the installation, state National Guard, or major US Army Reserve command mission. This includes areas nonessential to the operational mission of the installation or facility but which, by the nature of the activity, are considered vulnerable to theft, trespass, damage, or other criminal activity.

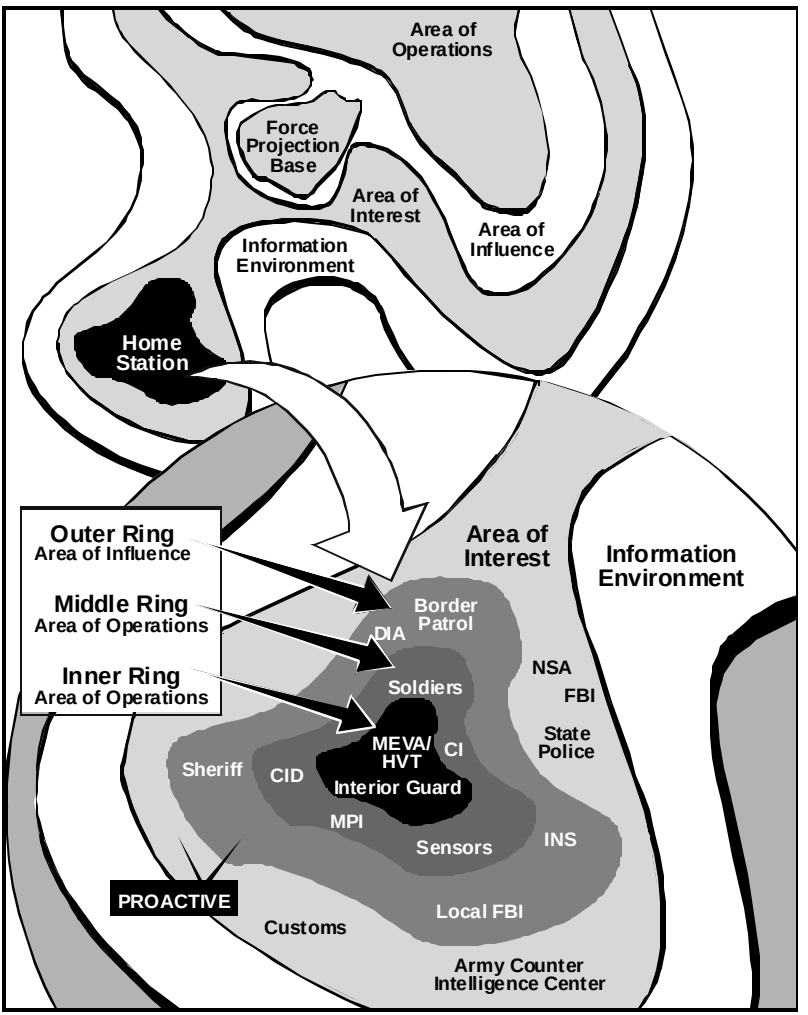


Figure 2-1. Installation Battlespace

??High-Risk Personnel (HRP)—Personnel who, by their grade, assignment, symbolic value, or relative isolation, are likely to be attractive or accessible terrorist targets.

??High-Risk Targets (HRT)—Resources/facilities considered to be at risk as potential terrorist targets because of mission sensitivity, ease of access, isolation, symbolic value, and/or potential for mass casualty.

2-3. Also part of the AO is the middle ring, which includes the rest of the installation confines such as housing, ammunition storage areas, etc. The outer ring does not have a finite boundary and must be defined by the installation commander as the area of influence. The installation area of influence includes areas that the commander can directly influence through such activities as contacts with local government officials, law enforcement agencies, emergency management agencies, and through public affairs command information channels. In addition to an area of influence, there is an area of interest. The area of interest is that area of concern to the commander that includes the area of influence, areas adjacent thereto, and areas occupied by enemy forces who could jeopardize the accomplishment of the mission.

2-4. Although this handbook does not directly address the area of interest, it may include areas distant from the installation where events may occur indicating changes in the threat to the installation. It could include facilities that provide services to the installation such as power, water, sewage, waste disposal, etc., and/or the seaports of embarkaton (SPOE)/aerial ports of embarkation (APOE) used by units deploying from the installation. It may also include contacts or information received from national and state law enforcement and intelligence or emergency management agencies relating to the area of influence or AO of the installation. All military operations take place within an information environment that is largely outside the control of military forces. The information environment is the aggregate of individuals, organizations, and systems that collect, process, store, display, and disseminate information, as well as the information itself. National, international, and non-state actors use this environment to collect, process, store, display, and disseminate information. Also the media actions could become part of a commander's area of interest. The media's use of real-time technology affects public opinion, both in the US and abroad, and alters the conduct and perceived legitimacy of military operations.

INSTALLATION MAJOR SECURITY MISSIONS

2-5. The following are the major implied security missions that support the installation's FP mission:

??Intelligence assessment.

??Command, control, and communications.

??Access control.

??Security of MEVAs, HRTs, and HRPs.

??Securing off-post personnel and materiel in coordination with law enforcement agencies.

??Tiered response capabilities.

??In-transit security operations.

??SPOE security operations.

??APOE security operations.

??Command information and community interfaces.

INTELLIGENCE GAPS (THREE CONCENTRIC RINGS)

2-6. There are sizeable seams throughout the security posture of the United States (Figure 2-2). These gaps exist between military services, military and civilian authorities, intelligence and law enforcement organizations, various national agencies, and within the echelons of law enforcement. For installations, seams between military and civilian law enforcement, and between law enforcement and military intelligence, leave installations vulnerable to domestic and international terrorism within the United States. Liaison with the local police is the role of the installation provost marshal and the military police (MP) (paragraphs 12-9 and 12-11, FM 3-19.1). Military intelligence (MI) and MP/criminal investigation division (CID) must coordinate obtaining sensitive law enforcement information and disseminating it to commanders via an installation fusion cell.

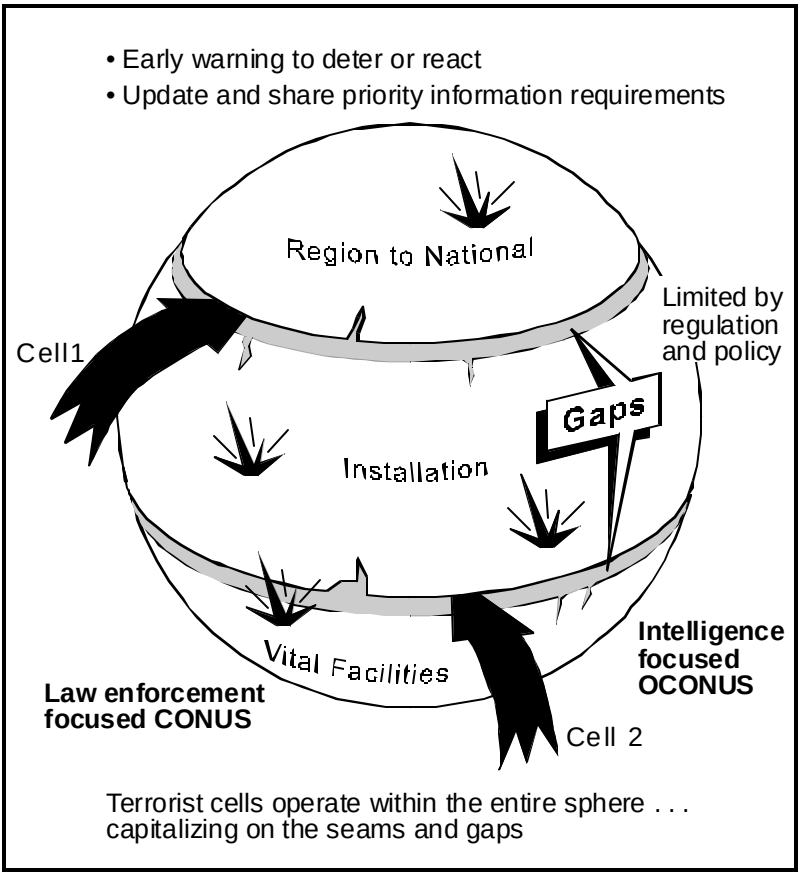


Figure 2-2. Seams in Threat Warning

2-7. Because of the current lack of coordinated plans, resources, and realistic joint training exercises, installations are vulnerable to terrorist methods. Bridging the gaps between organizations and creating analytical structures that answer the commander's tailored information needs provide a seamless flow of information that supports decision-making and appropriate FP measures. An installation commander normally has intelligence assets to assist in accomplishing these tasks. The intelligence officer and his staff perform intelligence operations in the United States in a manner that is consistent with the Constitution, applicable laws, implementing directives, and Army regulations. Specifically, the

intelligence officer and his staff must be thoroughly familiar with EO 12333, EO 12863, DOD Directive 5200.27, DOD Directive 5240.1, DOD Directive 5240.1-R, DOD Directive 5148.11, AR 381-10, AR 525-13, and applicable US legislation. Additionally, the intelligence officer and his staff must be familiar with AR 381-12 and AR 381-20 for counterintelligence (CI) activities.

2-8. A critical part of the guidelines in these publications concerns intelligence activities in relation to US persons. Contrary to popular belief, there is no absolute ban on intelligence collection on US persons. Intelligence components may collect US persons' information (through overt means) when the component has the mission (or function) to do so, and the information falls within one of the categories listed in DOD Directive 5240.1-R and AR 381-10. Two important categories are foreign intelligence and CI. Both categories include the involvement of US persons engaged in or about to engage in international terrorist activities.

2-9. The definition of *collect* within AR 381-10 differs from the common usage of the term *collect*. Within AR 381-10, collect includes the intent to use or retain the information received and to use information from cooperating sources. Procedure 2.B of AR 381-10 explains collect. The rest of this manual is written under the assumption that TRADOC installations have received the mission (function) from the proper authority and meet the criteria in Procedures 2, 3, and 4 of AR 381-10. Then the intelligence officer and his staff can collect (through overt means), retain, and disseminate intelligence that includes US persons' information. (Procedure 2.E establishes the conditions to meet to collect through other than overt means.) However, even if the intelligence officer and his section do not have the proper mission (function) to meet Procedures 2, 3, and 4, intelligence personnel can and must receive information that includes US persons' information—

??To determine its intelligence value and whether it can be collected. (See AR 381-10 for retention guidelines.)

??To deliver it to an appropriate recipient (for example the provost marshal's office) per Procedures 4 and 12, AR 381-10.

Chapter 3

Antiterrorist Critical Tasks

TASK 1: ESTABLISH AN ANTITERRORISM PROGRAM

3-1. The installation commander takes charge of his AT program by providing policies, standards, and procedures to implement the FP objectives to deter incidents, employ countermeasures, mitigate effects, and conduct incident recovery.

SUBTASKS

3-2. The installation commander—

- ??Develops throughout his command a working knowledge of AT policies.
- ??Ensures AT program includes tenets of countersurveillance, CI, and other specialized skills.
- ??Personally chairs the installation AT committee.
- ??Establishes clear operational responsibilities and assigns key staff members.
- ??Appoints an AT officer (minimum grade of 0-3 or equivalent civilian grade) to coordinate the AT program.
- ??Develops an executable plan focused on the installation's specific mission and unique environment (Appendices A-H).
- ??Develops and executes an effective training plan (Appendix I).
- ??Ensures the AT plan is exercised.
- ??Ensures daily actions are on going to improve AT. (An AT plan must be a living document that is updated and adjusted continuously as the environment and internal/external changes occur.)

??Prioritizes resource allocations.

??Ensures that an installation's military units/members and civilians understand their roles and responsibilities. Battalion units and above are required to have a Level II trained AT officer (sergeant first class or higher) who is the unit commander's AT planner, advisor, and Level I unit trainer.

??Ensures AT standards are incorporated into all aspects of deployment planning and execution. (All AT plans must be approved by the next higher command, minimum battalion commander.)

??Ensures the installation intelligence team is not overwhelmed with additional duties.

??Clearly understands how the FPCON and information operations conditions (INFOCON) are implemented, both up and down the chain of command, and who has authority to change them.

ANTITERRORISM COMMITTEE

3-3. This is the commander's team to plan, coordinate, and execute the installation commander's AT intent (Appendices A-H). The committee—

??Guides the AT program by developing strategy (Figure 3-1), conducting risk analysis, and coordinating resources.

??Integrates initiatives with other installation priorities.

??Adjusts priorities.

??Develops installation preparedness strategy for CBRNE events.

??Assesses internal hazardous material response capabilities.

??Updates and evaluates latest threat.

??Reviews memorandums of understanding (MOU) and memorandums of agreement (MOA).

??Ensures all tenant and supported reserve component units/activities are participants in the AT planning process and are included in AT plans, providing guidance and assistance as required.

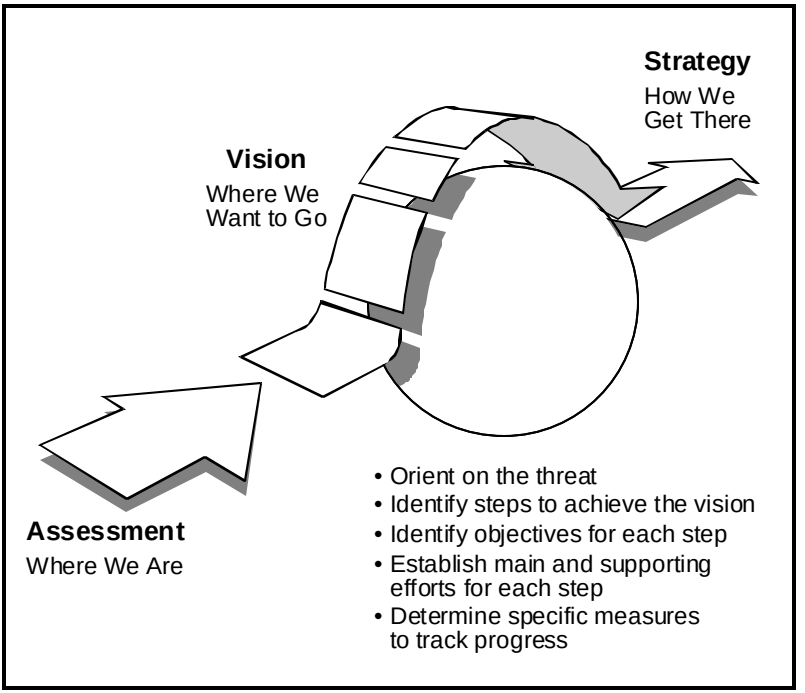


Figure 3-1. Strategy Development

3-4. Resource coordination is a critical AT committee function. Specifically, the committee—

??Determines and prioritizes installation resources for Program Objective Memorandum submission.

??Uses a holistic approach (a wide range of possibilities).

??Submits requests for management decision execution program funding. (Programs and materials having multiple uses, such as communications and medical equipment, are more competitive.)

3-5. During a regularly scheduled meeting, that is posted on both the short and long-range training calendar, the AT committee follows a set agenda. Also, identifying working groups for specific actions is a technique used effectively in AT committee meetings. Some specific working group examples are PS, threat, MEVA security, and funding working groups.

Additionally, it is important to include tenant organizations and local, state, and federal agencies participants in AT committee meetings to ensure all players and their resources are identified to implement a workable AT plan. A suggested format for a meeting includes—

??Purpose and deliverables.

??Current AT strategy phase.

??Threat assessment update.

??Brief progress report from each working group on assigned tasks. (Establish a measurement matrix for each task so that progress can be tracked.)

??Progress report on training, exercises, resources acquired, and lessons learned from after action reviews.

??Review of future events (near term, within the next six months, and long term, up to five years).

??Funding status and funding priorities.

??Commander's summary (higher headquarters guidance and priority of effort).

TASK 2: COLLECT, ANALYZE, AND DISSEMINATE THREAT INFORMATION

3-6. The second critical commander's task is to provides a system to collect, analyze, and disseminate terrorist threat information and apply the appropriate FPCON.

SUBTASKS

3-7. The commander or his designated representative—

??Designates intelligence focal point.

??Establishes an intelligence fusion cell (along with installation staff members, be sure to include local law enforcement personnel, CID, 902d MI representative, Federal Bureau of Investigation [FBI], and nearby DOD installation members).

??Determines threats.

- Integrates foreign, domestic, and crimal intelligence based on priority intelligence requirement (PIR).
- Insures timely information dissemination and incorporates current intelligence into AT training.
- Develops a threat-based information system (based on higher headquarters guidance) to raise or lower the FPCON. Subordinate commanders can raise but not lower a higher-level commander's FPCON.
- Informs and updates periodically higher headquarters of all threat attacks (Appendix J).
- Insures that any domestic intelligence activities are IAW—
  - Applicable Army regulations (AR 381-10, AR 381-13).
  - DOD Directive (DODD) 5200.27.
  - Federal law.
- Consults an intelligence-trained staff judge advocate representative to ensure domestic intelligence activities are IAW the law.

INTELLIGENCE FOCAL POINT

3-8. Designating an office as the intelligence focal point is a key aspect to an efficiently structured AT team. Recommended considerations for a successful intelligence focal point include—

- Adhering to AR 381-10 and restrictions.
- Designating a specific office (director of plans, mobilization, and security, MI or G/S-2) as the focal point.
- Not using the AT officer as the intelligence focal point (AT officer assists but should not be in charge of intelligence functions).
- Assigning the following responsibilities to the intelligence focal point—
  - Leading the intelligence functions.
  - Collecting and disseminating the intelligence data.
  - Liaisoning with local, state, and federal law and intelligence agencies.

- Assessing threat and vulnerability.
- Preparing intelligence portion of the installation AT plans.
- Providing operational impacts of changing intelligence situations.
- Making recommendations (random antiterrorism measures program [RAMP], intelligence priority changes, OPORD planning assumption changes, strategies awareness program modifications, resource allocation to the commander, etc.).

- Meeting frequently with membership of intelligence fusion cell.
- Disseminating (up, down, and laterally) information aggressively (e-mail, spot reports, secure internet, protocol router network, INTELINK, etc.).
- Seeking access to the closest classified internet source or intelligence source.
- Using threat modeling and templating to determine all available intelligence and information sources that apply to the installation.
- Using the following information sources and developing partnerships with—
  - Antiterrorism Operations and Intelligence Cell at Department of the Army, Deputy Chief of Staff for Operations, Law Enforcement Division.
  - Local, state, and federal agencies (obtain key specific information for your AO).
  - Nearby DOD installations.
  - Major command threat assessments updates.
  - Defense Intelligence Agency threat assessments.
  - State Department travel warnings.
  - Nearest CID special agent and CI agent.
  - Installation fire prevention and safety offices.

TASK 3:
ASSESS AND REDUCE CRITICAL VULNERABILITIES (CONDUCT ANTITERRORISM ASSESSMENTS)

3-9. The third critical commander's task is to assess and reduce critical vulnerabilities by continuously conducting reviews of the overall AT program, identifying physical and procedural security improvements, and analyzing unit predeployment procedures and plans. Four steps can be used in this process.

STEPS

3-10. Step one is to determine MEVAs and HRTs. (Those activities/areas on which everything depends, i.e. C^2 facilities, water systems, information systems, power generation facility, transportation network, airfield, post troop concentrations, schools, hospitals, commissaries, housing areas, mobilization center, etc. Remember, some vulnerabilities will be outside the installation.)

3-11. Step two is to identify threats and assess vulnerabilities (prioritize threats within installation functions and include terrorist use of CBRNE). The US Army Corps of Engineers *AT Planner* CD-ROM is a recommended tool to assess structural and area vulnerabilities (WGATPLAN@WES.ARMY.MIL).

3-12. Step three is to incorporate the consequences assessment tool set (CATS) into your assessment and management operations. Developed for the Defense Threat Reduction Agency, CATS is one of two Federal Emergency Management Agency (FEMA)-endorsed tool sets for man-made and natural disasters. Planners can use CATS to assess blast radii, recommend traffic/access control locations, conduct effects predictions, etc. It can be used for AT plan development, installation operations center exercises, and (using real-time weather) for actual incidents. CATS is distributed free of charge to US military organizations and can be ordered from http://cats.saic.com/ .

3-13. Step four is to mitigate risks and vulnerabilities by—

- ??Using a prioritized list of functions and their vulnerabilities to focus priority of work and reduce risk.
- ??Determining by function—
  - ✍Protection measures needed to reduce vulnerabilities.

- Resources necessary to achieve an adequate level of protection.
- Resources availability to mitigate risk.
- Location (local, state, federal) of resources.
- Coordination required.

??Coordinating actions with community officials, police, emergency responder agencies, etc.

??Developing strategy that sequences the actions and resources to achieve protection and/or mitigate impact on the installation.

??Developing a strategy timeline that achieves a preparedness end state.

??Writing a formal incident response plan.

??Implementing temporary fixes (increased site monitoring, temporary fencing, short-term adjustments to procedures, and/or increased emergency response assets) until permanent solutions are implemented.

??Continually reevaluating for effectiveness based on updated situation and/or threat. (Installation commanders must conduct, IAW Appendix C, AR 525-13, a self-assessment of their AT program within 60 days of assumption of command and annually thereafter.)

??Using external (joint staff integrated vulnerability assessment [VA], and major command teams) and internal assessments to adjust plan.

??Implementing RAMP to prevent installation security operations from becoming predictable.

UPDATE

3-14. It is important to continuously update the threat and VAs. Presidential Decision Directive 63 directs all federal agencies to implement a critical infrastructure assurance program that defines a process to assess infrastructure assets for criticality based on mission and threats, to perform assessment of these critical nodes of vulnerability, and to develop a remediation/mitigation plan to resolve deficiencies. Utilities managed by off-post companies are especially vulnerable due to the lack of military control. DOD AT construction standards provide specific guidance regarding stand off, barrier plans, access control to MEVAs, and access control-point facilities.

3-15. Installation commanders will prioritize, track, and report all vulnerabilities documented by installation and any higher headquarters VA

to TRADOC IOC within 60 days of the receipt of the VA final report. Headquarters TRADOC will track all reported installation vulnerabilities to resolution/closure. Assessment results will be retained on file for no less than three years.

TASK 4: INCREASE ANTITERRORISM AWARENESS IN EVERY SOLDIER, CIVILIAN, AND FAMILY MEMBER

3-16. The fourth critical commanders AT task is to increase AT awareness through training and a multidimensional awareness program.

TRAINING

3-17. Conducting and increasing participation in mandatory training as delineated in AR 525-13 is required. (Commanders will identify in writing the key AT positions that require formal or refresher training and ensure formal training is received at the TRADOC-designated course within 180 days of assumption of duties.) The levels of training are—

- ??Level I: Individual awareness.
- ??Level II: AT officer training.
- ??Level III: Battalion/brigade pre-command course.
- ??Level IV: Installation commander training (colonels and above who have responsibility for AT policy, planning, and execution).

AWARENESS

3-18. A multidimensional approach should be used to increase and maintain awareness consistent with the application of OPSEC measures. Suggested measures to ensure awareness are—

- ??Include AT program in newcomers' orientation briefings.
- ??Discuss at town hall meetings.
- ??Include AT measures and standards in post newspapers and post access channels on cable television, electronic bulletin boards, and command web sites.
- ??Include in quarterly training briefings.
- ??Combine AT actions with other events, i.e.100% ID/vehicle checks combined with random driving-under-the-influence screenings.

??Incorporate AT lessons learned in sergeant-time tasks, i.e. personnel/vehicle search, manning a checkpoint, emergency medical procedures, use of force rules (See Appendix J), etc.

??Combine FPCON and road conditions into a single notice at installation access points.

??Post AT awareness information at high traffic areas (post exchange, commissary, shopettes, theaters, libraries, and hospitals).

??Provide AT preparedness and response overviews to all tenant and contractor personnel.

??Review and educate tenant and senior tactical commanders on AT regulatory requirements.

??Develop AT awareness guide for family members (Appendix K).

3-19. Commanders are reminded to include the Army Air Force Exchange System; Defense Commissary Agency; morale, welfare, recreation directors; Department of Defense dependents school; and Medical Command representatives in AT planning.

TASK 5:
MAINTAIN INSTALLATION DEFENSES IAW FORCE PROTECTION CONDITIONS

3-20. The fifth critical commander's task is to maintain installation defenses IAW FPCON (See Appendix L).

TENETS

3-21. A sucessful installation FPCON has two primary tenets. Number one is achieving an increased FPCON understanding at all levels. (DOD Instruction 2000.16 mandates progressive levels of security actions in response to potential threats.) Number two is maintaining an awareness of the following FPCON system aspects:

??Each FPCON produces a detection, assessment, and response capability equal to the threat.

??Increased FPCON levels send a clear message of increased readiness.

??The AT officer and operations staff are the commander's key intelligence advisors.

- FPCON implementation considerations include—
  - After hours, weekend, and holiday notification plan.
  - Chemical, biological, and/or radiological detection equipment employment plan.
  - Pre-positioned equipment employment plan.
  - FPCON impact (notification, lodging, transportation, etc.) on HRP.
  - Effectiveness of past FPCON implementations as captured in Joint Staff, Department of the Army, major command, and internal assessments.
  - Manpower and resource requirements and sourcing options.
  - On-hand assets.
- RAMP implementation increases alertness and awareness and prevents hostile elements from predicting installation actions.
- The installation is assumed to be under hostile surveillance (learn to detect such activity).

IN-TRANSIT

3-22. Commanders of units in-transit will develop site-specific measures or actions for each FPCON which supplement those in Appendix L.

RAMP

3-23. Installation commanders will have a formally documented RAMP, under the supervision of the AT officer. The RAMP must be an integral part of the AT program and must test, at least annually, implementation of all FPCON measures.

TASK 6:
ESTABLISH CIVIL/MILITARY PARTNERSHIP FOR WEAPONS OF MASS DESTRUCTION CRISIS

3-24. The sixth critical commander's task is to create civil/military partnership to combat and defend against terrorism.

STEPS

3-25. The steps include—

- Maintaining a relationship with local community and nearby DOD installations by—
  - Establishing a civilian liaison officer position within the installation operation center (Share information IAW legal and policy guidelines).
  - Meeting and frequently interacting with external installation community officials (city mangers, law enforcement personnel, hospital directors, fire chiefs, etc.).
  - Inviting local, state, and federal law enforcement and emergency agencies to join your AT committee.
  - Using every opportunity to engage key community leaders (community orientations, installation activity days, civic meetings, festivals, celebrations, and exercises) (Appendix M).
  - Learning how civic authorities are organized and their security systems for AT.
  - Discussing and ensuring a complete understanding of how and what services (power, water, telephone repair, etc.) can be provided to your installation in the event of a WMD crises.
  - Establishing MOA and/or MOU to expand your AT tools (specialized training; communications; first responders equipment; and chemical, radiological, and biological detection and decontamination capabilities).
  - Using staff/command judge advocate to advise on legal aspects of domestic operations/support to civil authorities such as MOAs, MOUs, and status-of-forces agreements (for installations with international liaison officers and/or students), federal law enforcement jurisdiction, etc.
  - Establishing provost marshal office/CID liaisons with civil law enforcement agencies.
- Exchanging response capability (first responders: law enforcement, fire, explosive ordnance disposal [EOD], medical) information.
- Seeking and leveraging training opportunities by—

- Including surrounding community in all AT exercises and activities.
- Participating in external community emergency response exercises (airport disasters, hospital mass casualty events, domestic preparedness programs).

TASK 7:
DEVELOP PLANS FOR REPORTING AND RESPONDING TO A TERRORIST THREAT/INCIDENT

3-26. The seventh critical commander's task is to develop reactive plans that prescribe appropriate actions for reporting terrorist threat information, responding to threats/actual attacks, and reporting terrorist incidents.

IMPLEMENTATION

3-27. Ensure plans address management of the FPCON system, implementation of all FPCON measures, and include the requirement for terrorist-related reports. Commanders will conduct periodic reviews with appropriate responders of reactive plans to ensure response procedures are understood and integrated. Additionally, each installation will develop an attack warning system and use during exercises. In conjunction with the alarms exercises, commanders will drill emergency evacuation procedures, test FBI threat incident notification plans, and evaluate actions to prevent loss of life and/or mitigate property damage. Recommended actions include the following:

- Determining necessary capabilities—
  - Do as part of threat assessment.
  - Determine personnel, equipment, and functions required.
  - Evaluate post event calendar for off-post events.
  - Coordinate mutual aid agreements.
  - Determine redundant systems and effective options.
  - Develop an effective list of planning considerations unique to your installation.
- Acquiring necessary capabilities by—

- Assessing internal resources.
- Establishing local community and/or other DOD installation MOUs/MOAs.
- Achieving connectivity with state and regional federal response agencies.
- Ensuring communications compatibility and interoperability with local community, state, and federal agencies.
- Developing a long-range strategy (five-year plan).

?? Evaluating and adjusting FP capability by—

- Evaluating the status of preparedness and identifying necessary improvements.
- Coordinating to insure external agencies participate in all evaluations.
- Establishing installation mission-training plan based on AT plan needs.
- Identifying metrics to measure incident-response capability strengths and weaknesses.
- Conducting AARs and capturing what went right/wrong and specific functions needing improvement.

TASK 8: CONDUCT EXERCISE AND EVALUATE/ASSESS PLANS

3-28. The eighth critical commander's task is to conduct the exercise and evaluate and assess AT plans.

FIVE STAGES

3-29. There are five stages to exercising and evaluating the installation plan. Specific tasks include the following:

- First, determine necessary exercises and resources. (Use FM 25-101 as a guide for setting up exercises.) Accomplish the following in the exercise planning process:
  - Schedule AT scenario-driven exercises on the installation long-range calendar. (Incorporate AT planning into all major training exercises, combined training center events, and battle command training program events.)
  - Use AT committee to recommend exercise training objectives and tasks to the installation commander.
  - Use installation operations staff elements to conduct scheduling and to coordinate resource actions.
  - Include hospital mass casualty annual exercises, community events, mobilization tests, and tactical unit events in your AT exercise program. (WMD response measures and mass casualty scenarios may be sensitive to local civil authorities. Commanders will coordinate with local authorities prior to conducting such exercises if held in a location visible to the public.)
  - Include first responders early in planning phase.
  - Expand to no-notice events as confidence builds and expertise improves.
  - Consider the impact on mission, costs, and availability of personnel and resources. (Use small and concise vignette scenarios to exercise a specific part of the AT program.)
  - Take appropriate operations security measures to prevent disclosure of vulnerabilities during the planning, conducting, and evaluation of the exercise.
- Second, develop evaluation criteria for the installation functions, tenants, and local/state/federal activities participating.
- Third, execute the plan and ensure the following is incorporated:

- Stress to normal operations to duplicate confusion that occurs during crisis situations.
- The entire community to fully test the installation capability to react effectively.
- Notification to both internal and external communities/agencies before, during, and after each exercise.
- Trained external evaluators.

??Fourth, examine and evaluate the results based on—

- AT incident response plan.
- Written comments captured as exercise is conducted.

??Fifth, develop a strategy for improvements, insert adjustments into the plan, establish a timeline for completing each action item, and track each action to completion.

Chapter 4

Functions and Planning Considerations

INTRODUCTION

4-1. Although not all-inclusive, the below functions and planning considerations provide a start point for planning procedures.

COMMAND AND CONTROL

4-2. Command and control techniques to incorporate include—

??Establishing command procedures and roles.

??Structuring installation operations center (IOC) procedures.

??Standardizing reports.

??Maintaining copies of plans in the IOC.

??Designating a battle captain.

??Ensuring that sufficient primary and alternate IOC workspaces are provided.

??Instituting and publishing a succesion of command.

??Planning for redundant, compatible, and interoperable communication systems for the IOC and interfacing with first responders, the community, higher headquarters, other command elements, and residents.

??Liaisoning with civilian organizations.

OPERATIONS

4-3. Operation techniques and functions to incorporate include—

??Completing threat and VAs.

??Planning and assessing exercises (Use concise scenarios focused on specific aspects of the FP program).

??Establishing intelligence liaison support.

??Learning and drilling operations center procedures.

??Establishing agreements with tenant organizations (civilian and military).

??Developing alert notification procedures.

??Establishing reporting requirements.

??Reviewing and throroughly understanding each FPCON measure.

??Synchronizing response capabilities.

??Developing and initiating security procedures.

??Identifying and protecting critical infrastructure.

??Identifying and exercising alternate operations centers.

??Updating weather information frequently.

??Preparing a deception plan to increase deterrence.

??Developing detection and monitoring procedures.

??Coordinating for EOD capability.

??Establishing procedures for receiving and integrating, based on a specific incident, responding lead federal agency per Presidential Decision Directive 39 (CONUS).

??Tracking post and off-post events involving military personnel and/or their families.

LOGISTICS

4-4. Logistics services techniques and functions to incorporate include—

??Identifying required and available alternate life-support sources (water, food, shelter).

??Planning for mortuary, laundry, and food services.

??Stockpiling barrier and lighting equipment and material.

??Considering emergency services (transportation, environmental, utilities, locksmith, etc.) requirements.

??Planning for emergency supplies of Class I, III, IV, V, and IX.

??Stocking protective equipment.

??Determining possible heavy lift equipment requirements.

??Identifying possible facilities and staging areas for displaced operations and supporting/augmenting agencies or organizations.

??Developing materiel and baggage holding areas.

??Providing maintenance for security systems.

HEALTH SERVICES

4-5. Health services techniques and functions to incorporate include—

??Initiating MOUs/MOAs, IAW installation procedures, with local, state, and federal health service providers to support and augment unavailable or incomplete installation capability.

??Establishing an emergency preparedness plan to include ground/air lift assets.

??Maintaining necessary Class VIII stockpiled IAW US Army Medical Command (MEDCOM) policy and guidance.

??Creating an effective communications capability with the IOC, installation support team, and surrounding community hospitals.

??Identifing follow-on pharmaceutical requirements and streamlined acquisition processes IAW MEDCOM policy and guidance.

??Developing a security system for the hospital during crisis.

??Understanding that there is limited patient decontamination at the medical treatment facility (MTF) and working alternatives.

??Conducting periodic water and food checks in coordination with public health officials in the surrounding community.

??Establishing MOUs/MOAs with surrounding community hospitals to provide additional resuscitative surgical and critical care capabilities.

??Maintaining medical surveillance for unusual trends in patient complaints in conjunction with surrounding community hospitals and clinics as an early warning that a CBRN attack may have occurred.

??Estimating the surgical and critical care capabilities of the MTF and surrounding community hospitals. (Frequency of the estimates must be tailored to the FPCON. Capabilities must be stated as number of patients needing immediate resuscitative surgery that the hospital can manage over the next 12 hours and number of ventilator-dependent nonsurgical patients that the hospital can manage over the next 12 hours.)

??Planning for increased requirements for laboratory testing and handling of specimen samples and establishing MOUs and MOAs with local/state medical laboratories for specimen testing.

??Coordinating for mortuary affairs, autopsies, and storage and transport of contaminated remains as part of an emergency preparedness plan.

??Planning for veterinarian services for animal control to maintain public health.

??Publicizing an after-duty-hours phone number that military beneficiaries can dial when they have questions.

??Developing strip maps to surrounding community hospitals.

RESOURCE MANAGEMENT

4-6. Resource management techniques and functions to incorporate include—

??Coordinating with agencies for long term FP budget estimates.

??Capturing costs for reimbursement.

??Identifying funding sources.

??Preparing MOUs and MOAs.

??Coordinating funding source for deployment and mobilization orders when mobilization or deployment occurs.

??Developing and maintaining a mobilization TDA for implementation when necessary and specifying target sources for resources (manpower and equipment).

??Maintaining interservice support agreements.

ENGINEERING

4-7. Engineering techniques and functions to incorporate include—

??Developing emergency services response plans.

??Initiating MOUs/MOAs, IAW installation procedures, with local/state/federal law agencies to support and augment unavailable or incomplete installation capability.

??Assessing, procuring, and maintaining emergency assets.

??Developing a temporary housing plan.

??Identifying mass parking areas for consolidated parking plans (park and ride).

??Planning decontamination capability.

??Establishing a hazardous material (HAZMAT) and CBRNE response capability.

??Determining barrier plan design and execution requirements.

??Planning for structural evaluations.

??Planning for obstacle clearing.

??Conducting critical structures vulnerability analysis.

??Accomplishing terrain analysis to determine access vulnerabilities.

??Planning for search/rescue and rubble clearing operations.

??Determining possible environmental remediation requirements.

??Developing physical design and structure FP requirements for sensitive areas and MEVAs.

??Conducting installation shelter surveys using approved guidance from the Corps of Engineers and/or FEMA.

??Recommending shelter options.

CONTRACTING AND PURCHASING

4-8. Contracting and purchasing techniques and functions to incorporate include—

??Identifying requirements for emergency contracting (transportation, communications, protective equipment, etc).

??Preparing for emergency contracting.

??Estimating emergency costs required to fill gaps in resources.

??Identifying sources for potential contracting.

COMMUNICATIONS AND INFORMATION SYSTEMS

4-9. Communications and information systems techniques and functions to incorporate include—

??Planning and providing for communications and information systems, to include required security equipment and programs, with local community, higher headquarters, command elements, special reaction teams (SRT), and quick reaction forces (QRF).

??Establishing an information assurance program and performing VAs to determine network vulnerabilities.

??Resolving communications compatibility concerns with local community, higher headquarters, command elements, SRT, and QRF.

??Providing for and testing redundant communications.

??Developing an emergency phone directory.

??Planning and preparing for emergency reconfiguration of existing local area networks to support the IOC.

??Implementing and managing the INFOCON program IAW TRADOC Cir 25-01-1, Chapter 8.

??Determining mail screening operations and the needed resources (Appendix N).

??Establishing communication between IOC and incident commanders.

??Developing a detailed communication plan for all organizations (military and nonmilitary).

??Planning and providing for mass/public notification capability.

PERSONNEL

4-10. Personnel systems techniques and functions to incorporate include—

??Preparing a casualty assistance plan.

??Providing for civilian employee assistance.

??Participating in identification of emergency shelters.

??Providing for next-of-kin notification.

??Providing for crisis counseling.

??Identifying linguists for emergency notifications and interview requirements.

??Preparing orders IAW mobilization or deployment instructions.

??Consolidating installation personnel accountability reporting.

ARMY COMMUNITY SERVICE

4-11. An Army community service function that is important to the FP program is developing a family assistance center plan.

SPECIAL STAFF FUNCTIONS

4-12. The functions of the special staff are as follows:

CHAPLAIN

4-13. The chaplain—

??Provides crisis counseling.

??Coordinates sufficient pastoral assistance.

??Provides pastoral care.

LEGAL

4-14. The legal office—

??Advises the commander and staff on all legal matters related to FP, including, but not limited to, intelligence law, domestic operations/support to civil authorities, federal law enforcement jurisdiction, use of force, contracting, claims, environmental law, and government ethics.

??Reviews MOUs/MOAs.

??Advises the command and assists in the development, training, and certification of rules for the use of force (RUF).

??Reviews and advises the command on all intelligence-gathering efforts to ensure statutory and policy limits are complied with.

??Reviews and advises the command on all requests for support to law enforcement and civil authorities to ensure that the requested assistance falls within the limited statutory authority for allowable support.

??Ensures resolution of UCMJ jurisdiction issues over mobilized reserve component personnel.

PUBLIC AFFAIRS

4-15. The public affairs office—

??Spearheads the command information program using available assets (post newspaper, command web site, electronic bulletin boards, etc.).

??Accommodates requests for information from civilian news organizations.

??Advises the commander on all public affairs-related issues.

??Prepares and issues news releases for the command.

??Serves as the installation spokesperson.

??Develops and implements media awareness training for soldiers, civilians, and family members (Appendix O).

??Considers the establishment of an information center standing operating procedure.

PROVOST MARSHAL

4-16. The provost marshal office—

??Develops and implements installation physical security plan and barrier plan.

??Plans for installation traffic circulation.

??Protects identified individuals.

??Trains police in first-response responsibilities.

??Conducts crime scene preservation and evidence collection.

??Maintains physical security.

??Implements MEVAs protection.

??Accomplishes restricted area protection.

??CID/military police investigations coordinate with civil law enforcement departments.

??Initiates MOUs/MOAs, IAW installation procedures, with local/state/federal law enforcement agencies to support and augment unavailable or incomplete installation capability.

SAFETY

4-17. The safety office—

??Ensures commanders conduct risk and VAs for the health and welfare of affected individuals.

??Incorporates risk management techniques into first responder operations.

DOIM/DPTM

4-18. The DOIM/DPTM office—

??Establishes redundant systems for critical AOs.

??Monitors pre-incident exercises to ensure an evaluation of the interoperability capability between procedures, systems, and equipment is provided.

ENVIRONMENTAL SERVICES

4-19. Environmental services—

??Provides HAZMAT response and remediation requirements.

??Provides CBRN support to the incident commander.

INSPECTOR GENERAL

4-20. The inspector general—

??Checks and verifies correct execution of FP program per commander's guidance.

??Provides trend analysis of FP processes.

EXPLOSIVE ORDNANCE DISPOSAL TEAM

4-21. The EOD team—

??Provides expertise in proper procedures to resolve suspected package/explosive hazard incidents.

??Is the subject-matter expert in planning multiple/large scale explosive hazards procedures.

Chapter 5

Critical Information

OVERVIEW

5-1. Critical information directly affects the successful execution of operations. The commander's critical information requirements (CCIR) include information the commander requires that directly affects his decisions and dictates the successful execution of operations. The commander alone decides what information is critical and continuously reviews the CCIR during the planning process (military decision-making process [MDMP]) and adjusts them as situations change. The staff's role is to nominate information requirements for the CCIR. The CCIR generates two types of supporting information requirements:

??Friendly force information requirements (FFIR).

??PIR.

5-2. Figure 5-1 illustrates the relationship between CCIR, PIR, and FFIR. In addition to CCIR, essential elements of friendly information (EEFI) become a commander's priority when he states them. Intelligence, surveillance, and reconnaissance (ISR) are used to provide indications, warning, and predictive products to support FP and to manage PIR and request information tailored to installation needs.

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

5-3. When commanders receive a mission, they and their staffs analyze it using the MDMP (Appendix A). As part of this process, commanders visualize the battlespace and the fight. CCIR are those key elements of information commanders require to support decisions they anticipate. Information collected to answer the CCIR either confirms the commander's vision of the threat or indicates the need to issue a fragmentary order or to execute a branch or sequel. CCIR directly supports the commander's vision

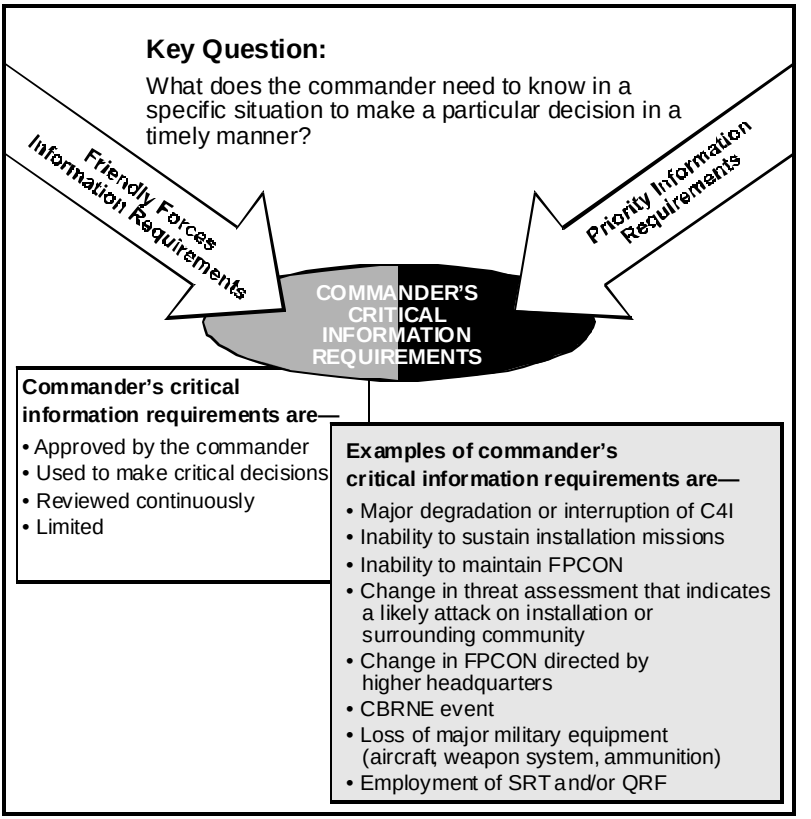


Figure 5-1. CCIR Elements

of the threat. Commanders develop them personally. The following are key characteristics of CCIR:

??Directly linked to the present and future operational situations.

??Situation dependent.

??Predicable events or activities.

??Specified by the commander for each operation (recommend limiting to 10 or less to better focus the collection effort).

??Time-sensitive information that must be immediately reported to the commander, staff, and subordinate commanders.

??Always included in operation order or operation plan.

??Transmitted by a communications system IAW standing operating procedures (SOP).

??Used to drive decisions at decision points.

??Generates FFIR and PIR.

??Focuses collection effort of units, individuals, and systems.

PIR

5-4. PIRs are those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision-making. PIRs are associated with a decision that will affect the overall success of the commander's mission. PIRs determine what the commander wants or needs to know about the threat, the enemy's purpose, capabilities, and/or operating methods (how the commander sees the threat). Figure 5-2 shows the characteristics of PIR and provides some examples of FP PIR.

A Good PIR

- Provide intelligence required to support a single decision
- Ask only one question
- Focus on specific time, place, and enemy unit

FM 34-2, Mar 94
FM 3-0, Jun 01

PIR Examples

- Is installation and/or surrounding community the target of intelligence gathering activities? Describe pattern, capability, possible intentions.
- Does threat assessment indicate that an attack is likely, imminent, or ongoing? Describe possible method of attack and objectives.
- Are there any indications of possible terrorist incidents that could cause a CBRNE event that would impact safety and continuity of installation operations?

Figure 5-2. PIR Characteristics

FFIR

5-5. FFIR is the information the commander and staff need about the forces available for the operation. This includes personnel, maintenance, supply, ammunition, and experience/leadership capabilities. FFIR allows the commander to determine the internal and external capabilities (how the commander sees his status). Figure 5-3 shows the characteristics of FFIR and provides some examples of FP FFIR.

A Good FFIR

- Information about key forces available to specific operations
- Information on forces critical to the successful accomplishment of the mission
- Limited in number

FM 101-5-1, Sep 97
FM 3-0, Jun 01

FFIR Examples

- Activity that renders part of command information plan obsolete and requires prompt release of revised information
- Training cancelled to maintain force protection levels
- Notification to expand training base to support partial mobilization
- Significant degradation in an installation's ability to perform power projection platform functions
- Prescribed FPCON level cannot be maintained
- Force protection measures that restrict ability to meet mission requirements

Figure 5-3. FFIR Characteristics

EEFI

5-6. EEFIs are not part of CCIR but are critical aspects of friendly operations that, if known by the enemy, would subsequently compromise, lead to failure, or limit success of the operation and, therefore, must be protected from enemy detection. EEFIs allow the commander to determine how to protect his resources from the threat's information-gathering systems (how the commander can prevent the threat from determining his

capabilities). Figure 5-4 shows the characteristics of EEFI and provides some examples of FP EEFI.

A Good EEFI

- Intentions, capabilities, and activities that we want hidden from enemy/threat collection
- Compromise would jeopardize the success of the operation
- Objective is to degrade the threat's situational understanding

FM 101-5-1, Sep 97
FM 3-0, Jun 01

EEFI Examples

- Location, schedule, and security of command group
- Security and configuration of the information network
- Installation plans and ability to respond to a threat
- Designation of MEVAs
- Designation of HRTs
- Measures being taken to reduce vulnerabilities and projected completion date

Figure 5-4. EEFI Characteristics

ISR

5-7. ISR is a key aspect of the intelligence-fusion process that assists in achieving information superiority. Thoroughly integrated ISR operations add many collection services. Also, ISR integration curtails functional stovepipes for planning, reporting, and processing information to produce intelligence. The mission of ISR is to provide timely, relevant, and accurate early warning and predictive intelligence products to enable proactive FPCON decisions by the commander and actions by installation entities. Twelve key ISR tasks are—

??Provide timely indications, warnings, and predictive products to support FP.

??Maintain threat situational awareness and understanding throughout the area of influence.

??Manage PIR and request information tailored to installation needs.

??Prepare and execute an ISR collection plan.

??Conduct all-source analysis to support predictive assessments.

??Maintain connectivity with joint, national, combined, and service intelligence and law enforcement agencies.

??Fuse criminal information to present a seamless threat picture.

??Conduct analysis of local information to determine threat patterns.

??Collaborate with other installations and the major command.

??Conduct local liaison to gather information and ensure connectivity.

??Provide timely information to all levels to ensure common awareness.

??Disseminate intelligence to support current and future operations.

5-8. Figure 5-5 illustrates how CCIR, PIR, FFIR, EEFI, and ISR support the task of gaining and maintaining information superiority.

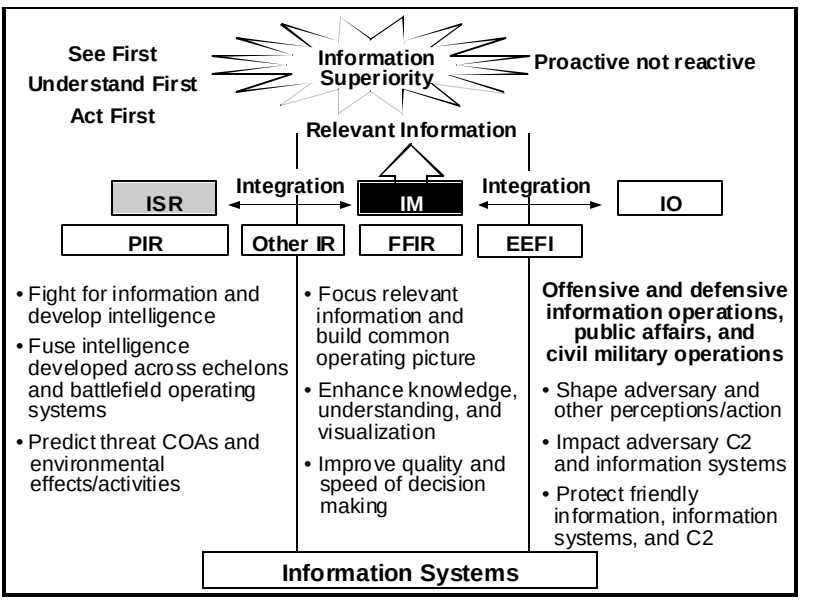


Figure 5-5. Information Superiority

Chapter 6

Tiered Response Capabilities

OVERVIEW

6-1. A tiered response to installation incidents is required to ensure an effective capability that can resolve the incident. Tiering consists of internal and external assets.

INTERNAL ASSETS

6-2. The internally resourced organizations described in this chapter are the ideal. Installations, especially small ones, will need to tailor as appropriate to meet their needs and may need to coordinate with local activities and other regional DOD installations to pool resources in order to meet the FP requirements.

FIRST RESPONDERS

6-3. First responders are those individuals and organizations that by virtue of their duty position are either on the scene when an incident occurs or are immediately available to respond to the incident without needing time to recall personnel or to obtain additional equipment.

Manning

6-4. The following are first reponders that are available on most installations:

??Guard forces.

??Emergency medical services.

??Fire department.

??Law enforcement patrols.

??Protective services detail (if an HRP is on the installation).

??Others (photographer, linguist, public affairs officer, chaplain, etc.), as required.

Missions

6-5. Working together, first responders execute the following missions:

??Respond to, contain, and resolve any incident.

??Identify and report the nature of the situation.

??Establish and seal perimeter around incident.

??Maintain observation (subjects, escape routes).

??Establish command post.

??Apprehend the perpetrators.

??Conduct investigation in conjunction with applicable agencies.

??Safeguard property and HRP.

??Submit serious incident reports.

Concepts

6-6. The following concepts guide employment of first responders:

??Provide first layer of security and response.

??Utilize basic capabilities.

??Available 24/7.

??Integrate functions (MP desk sergeant notifies post commander and IOC IAW established procedures.).

??Utilize positions of cover and concealment.

??Request as needed CID; hostage negotiators; SRT; QRF; chemical, biological, radiological, and nuclear installation support team (CBRN-IST); chemical, biological, radiological and nuclear rapid response team (CBRN-RRT); special medical augmentation response team (SMART); EOD team; and FBI.

Training

6-7. The following are the minimum training requirements for first responders:

??Certification for their unique specialty to specified standards.

??Hands-on training on all equipment to proficiency levels.

??Unit collective tasks.

??IOC interfaces.

??Communications procedures.

??Rules on the use of force.

??Cross training as specified by installation commander.

SPECIAL REACTION TEAM

6-8. The SRT is a unit of specially trained military or DOD police personnel (operating under the auspices of the provost marshal, chief of security, or chief of security police) armed and equipped to respond to and resolve special threat situations above and beyond the scope of standard or usual law enforcement capabilities.

Manning

6-9. Figure 6-1 depicts the recommended composition of the SRT. Installation commanders may need to tailor this organization based on available resources.

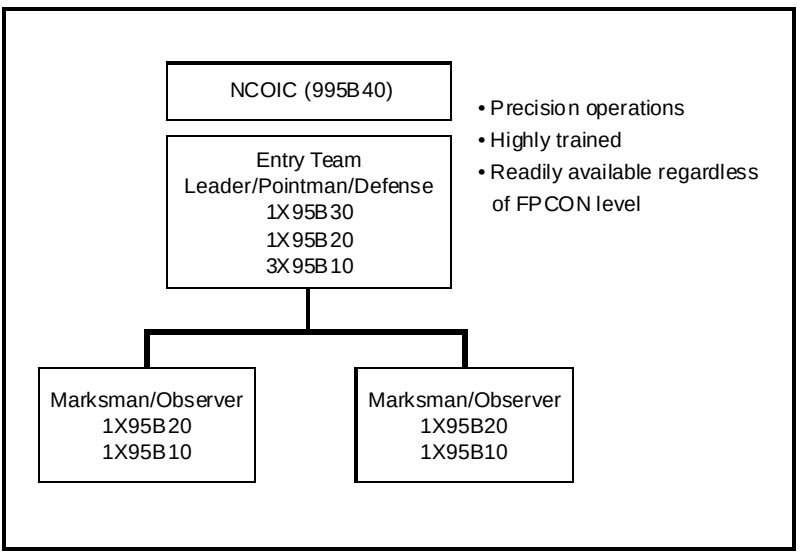


Figure 6-1. SRT Organization

Missions

6-10. The SRT is manned, trained, and equipped to perform the following missions:

??Precision high-risk entry for barricaded persons.

??Apprehend dangerous suspect.

??Counter sniper operations.

??Precision marksmanship.

Concepts

6-11. The following concepts guide employment of the SRT:

??Provides special response IAW set timeframe based on FPCON level.

??Maintains high readiness level.

??Organizes, trains, equips, and maintains an SRT by an MP unit IAW stated mission requirements.

??Requires threat analysis to identify SRT-needed level-of-response capability.

??Activates a CCIR item when employed.

??Deploys to designated forward assembly areas (FAA) upon incident/on-scene commander request.

??Provides SRT operational control to incident/on-scene commander upon assembly and ready to deploy.

Training

6-12. The following are the recommended SRT training standards:

??Train IAW FM 3-19.11, MP SRT.

??Attend two-phase SRT course at Fort Leonard Wood, MO.

??Cross train each team member in an alternate position.

??Train each team member as a combat lifesaver.

QUICK REACTION FORCE

6-13. The QRF is an uncommitted, battle-rostered organization; trained and certified on individual and collective tasks; fully equipped with individual weapons, light crew served weapons, robust secure communications, personal ballistic protection, lethal and nonlethal capabilities; and with mounted mobility.

Manning

6-14. Figure 6-2 depicts the recommended composition of the QRF. The QRF has the following characteristics:

??Recommended baseline of 31 personnel. Actual size and number of platoons determined by installation commander.

??Headquarters element (OIC, NCOIC, RTO, medic).

??Platoon (three 9-man squads).

??One combat lifesaver or medically trained equivalent per squad.

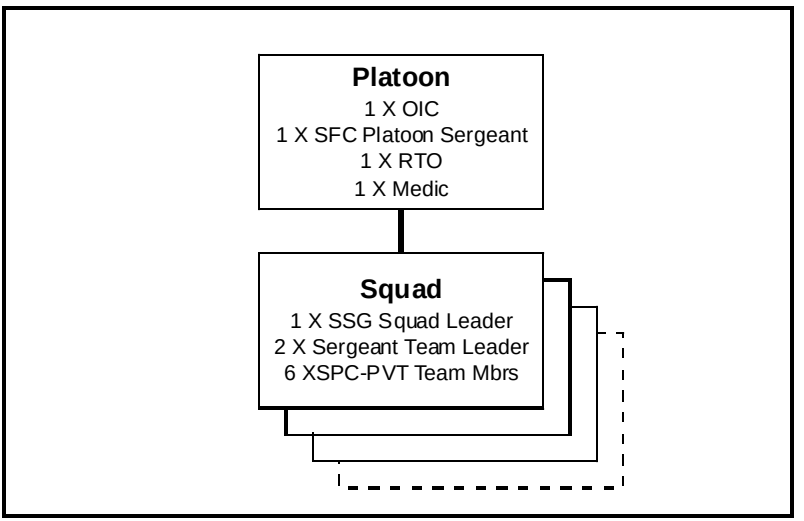


Figure 6-2. QRF Organization

Missions

6-15. The QRF is manned, trained, and equipped to perform the following missions:

??React to breaches at access control point.

??Reinforce MEVA force.

??Establish perimeter for an incident site.

??Patrol.

??Respond to very important person or other hostage situations.

??Respond to sniper incidents.

??Conduct riot-control operations.

??Clear and secure facilities.

Concepts

6-16. The following concepts guide employment of the QRF:

??Quickly generate combat power.

??Activate and employ items of CCIR.

??Tactically mobile.

??Deploy to designated FAA upon incident commander request.

??Placed under operational control of incident commander.

??Operate IAW FM 3-11xx (available May 2002), FM 3-19, and FM 7-8.

Training

6-17. The QRF is to be trained IAW training support package 191-95B-004 available from US Army Military Police School.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR INSTALLATION SUPPORT TEAM

6-18. The CBRN-IST is a matrixed organization composed of assigned, tenant, and local agency assets that provides an installation commander an organic CBRN capability. (Note: The CBRN-IST O&O plan approved, 31 January 2002, by HQ TRADOC.)

Manning

6-19. Figure 6-3 depicts the recommended composition of the CBRN-IST. Installation commanders may need to tailor this organization based on available resources.

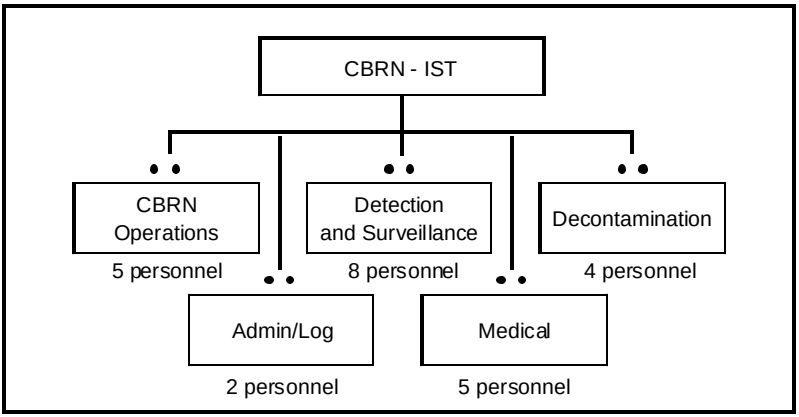


Figure 6-3. CBRN-IST Organization

Missions

6-20. The CBRN-IST is manned, trained, and equipped to perform the following missions:

??Conduct early warning using standoff and/or network-point sensors.

??Detect chemical, biological, and radiological hazards.

??Perform identification of chemical, biological, and radiological hazards.

??Locate and mark chemical, biological, and radiological hazards.

??Communicate directly with the installation commander, incident commander, and IOC via secure-voice communications.

??Calculate hazard predictions.

??Triage and emergency medical procedures.

??Coordinate evacuation of casualties.

??Coordinate administrative and logistical support.

??Coordinate security support.

??Conduct limited decontamination.

Concepts

6-21. The following concepts guide employment of the CBRN-IST:

- Activated by installation commander once indications are received that a CBRN attack may occur or once first responders suspect or determine that a CBRN incident has occurred.
- Organized as an element of the installation response capability.
- Tailored from on-call assets.
- Integrates CBRN-IST/CBRN-RRT/SMART/Chemical Corps and other government assets.
- Reports directly to the installation commander if activated prior to an incident. Once an incident occurs, reports directly to incident commander.
- Trains and exercises continuously to ensure success.
- Requires support from installation MTF, Directorate of Logistics, Directorate of Public Works, and community support agencies.
- Sustains operations for no more than 24 hours after an incident without augmentation.
- Provides support to civil authorities provided it remains within supporting distance of parent installation.
- Reinforced by CBRN-RRT.
- Activates reconnaissance and surveillance section before an incident at named areas of interest as part of collection plan.
- Performs the following tasks once hazard is detected:
  - Alert and recall (assuming CBRN-IST is not already assembled).
  - Brief IOC mission.
  - Deploy to incident site.
  - Detect and identify CBRN hazard, if not already identified.
  - Assess, decontaminate, treat, and facilitate casualty evacuations.
  - Provide hazard predication warning to IOC.
  - Determine the physical boundaries of the hazard and mark the area.

- Establish initial decontamination operation—
  - Establish initial hot line procedures.
  - Decontaminate.
  - Coordinate additional decontamination capability.
  - Provide first aid.
- Continue surveillance of the hazard.
- Conduct handover as required.
- Advise the installation commander.

Training

6-22. CBRN-IST training is based on the following concepts:

- Appropriate individual certification for duty position.
- Hands-on equipment training.
- FM 3-11xx multiservice tactics, techniques, and procedures (MTTP) for ISTs/RRTs (Chemical School working).
- Training via Chemical School mobile training teams, Fort Leonard Wood resident course, and distance learning course (all in planning stage of development).
- Medical section members attend the following courses: Basic Life Support, Advanced Trauma Life Support, Advanced Cardiac Life Support, Medical Management of Chemical and Biological Casualties.

EXTERNAL ASSETS

6-23. External response forces with regional responsibilities are available to fill gaps in the capabilities provided by internally resourced response forces or to provide reinforcing capability for the internal response forces.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR RAPID RESPONSE TEAM

6-24. The CBRN-RRT provides a full-time, dedicated capability to rapidly augment and reinforce installations following a CBRN incident. (Note: The CBRN-RRT O&O plan approved, 31 January 2002, by HQ TRADOC.)

MANNING

6-25. Figure 6-4 depicts the recommended composition of the CBRN-RRT.

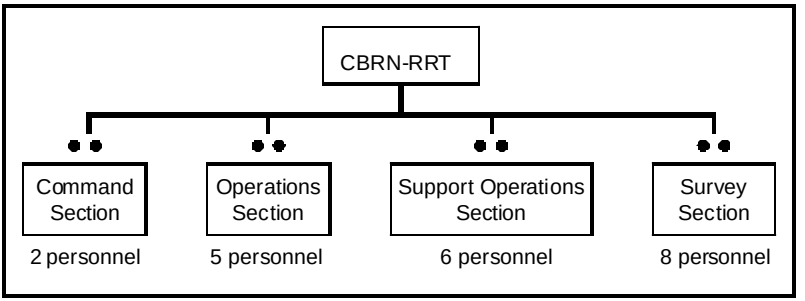


Figure 6-4. CBRN-RRT Organization

Missions

6-26. The CBRN-RRT is manned, trained, and equipped to perform the following missions:

- ??Augment and reinforce installation once a CBRN incident occurs.
- ??Pre-position and/or deploy to an incident site.
- ??Conduct en route planning.
- ??Maintain secure communications with incident site.
- ??Detect chemical, biological, and radiological hazards.
- ??Mark boundaries of a hazard.
- ??Communicate with the installation commander/incident commander/and the major command via secure means.
- ??Conduct casualty decontamination.
- ??Conduct administrative and logistical operations.
- ??Conduct coordination with MTF.
- ??Conduct limited personnel decontamination.
- ??Conduct limited equipment decontamination to sustain operations.
- ??Advise installation commander.
- ??Sustain operations for 48 hours.
- ??Collect and prepare samples for DOD and Department of Justice laboratories.

Concepts

6-27. The following concepts guide employment of the CBRN-RRT:

??Strategically locates eight teams in CONUS and Hawaii with regional responsibilities.

??Deploys to incident site, augments CBRN-IST, assesses hazards, and advises installation/incident commander.

??Integrates into CBRN-IST.

??Provides operational control to the incident commander.

??Responds no earlier than 2 hours and no later than 12 hours after notification.

??Coordinates remediation operations to restore the installation to fully mission-capable status.

??Arrives first at incident site sometimes.

??Deploys by most expedient means (air or land).

??Conducts handover to DOD, Department of Energy, or Department of Justice organization.

Training

6-28. CBRN-RRT training is based on the following concepts:

??Appropriate individual certification for duty position.

??Hands-on equipment training.

??Wear of Level A CBRN suit (self-contained breathing apparatus).

??FM 3-11xx MTTPs for ISTs/RRTs (Chemical School working).

??Team members attend two-week Fort Leonard Wood course (Chemical School working).

SPECIAL MEDICAL AUGMENTATION RESPONSE TEAM

6-29. The SMART provides short-duration medical augmentation to local, state, federal, and defense agencies for disasters, civil-military cooperative actions, humanitarian assistance, and WMD incident response. There are a total of 43 SMARTs in the Army under MEDCOM. Each SMART is configured to provide one of the following capabilities:

??Trauma/critical care.

??Nuclear/biological/chemical incident response.

??Stress management.

??Medical command, control, communication, and tele-medicine services.

??Pastoral care.

??Preventive medicine.

??Burn treatment.

??Veterinary services.

??Health systems assessment and assistance.

??Aero-medical isolation.

Manning

6-30. Manning of SMART is dependent on the capability of the individual team and may be tailored by the commander, MEDCOM, to meet the specific mission requirements.

Missions

6-31. SMARTs are manned, trained, and equipped to perform the following missions:

??Provide medical augmentation to DOD, local, state, and other federal agencies.

??Support/augment available medical capabilities.

??Provide technical advice.

??Assess incidents.

??Educate.

Concepts

6-32. The following concepts guide employment of the SMARTs:

??Task-organized based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC), and medical mission/risk analysis.

??MEDCOM tasks teams. (However, the regional medical command can respond directly to the MTF commander's request for a SMART.)

- Provide subject-matter experts.
- Deploy with in-house, off-the-shelf resources in backpacks/man-portable kits.
- Sustain themselves for up to 72 hours.
- Provide operational control to the incident commander.
- Provide short-duration medical augmentation (normally up to 72 hours).
- Alerted, assembled, and deployed within 12 hours after notification.
- Arrive at incident site, link-up, coordinate, integrate, synchronize, support, hand-off, and depart after release by incident commander.
- MEDCOM subordinate commands organize, train, equip, and deploy SMARTs.
- Deploy using DOD and non-DOD transportation assets.
- Do not compete with nor supplant federal emergency agencies and/or US Army TOE units.
- Deploy with local intra-team radios.

Training

6-33. SMART training is based on the following:

- Overall responsibility of Assistant Surgeon General, Force Projection.
- Maintain-to-standard professional credential and licensing requirements.
- Basic life support.
- Maintain compliance IAW standards in—
  - DODI 1322.24.
  - FM 8-42.
  - MEDCOM Regulation 350-4.
  - FM 100-19.
  - Certification on SMART equipment.

EXPLOSIVE ORDNANCE DISPOSAL TEAM

6-34. EOD teams support the accomplishment of the FP mission by providing for the detection, identification, on-site evaluation, rendering safe, recovery, and final disposal of unexploded explosive ordnance.

Manning

6-35. The standard light EOD team consists of a team leader (staff sergeant) and one or two assistants.

Missions

6-36. The EOD teams are manned, trained, and equipped to perform the following missions:

- Detect, identify, render safe, and dispose of—
  - Unexploded conventional munitions.
  - Improvised explosive devices (IED).
  - CBRNE.
  - Mechanical fusing (booby-trap) devices.
  - Sophisticated sensor technology (microwave, active/passive infrared accoustic, ultrasonic photo-electric, magnetic, seismic, etc.) used in devices containing CBRNE materiel.
- Provide incident commander technical advice, tools, and reach-back intelligence and technical capability.
- Provide recommendations for—
  - Protective measures.
  - Predicting effects.
  - Identifying threat materiel.
  - Render-safe options.
  - Disposition actions.
- Provide first responders, mail handlers, and leaders training for—
  - Recogniting and reporting of unexploded ordnance (UXO) and IEDs.
  - Search and evacuation procedures for bomb threats.
  - Site vulnerability assessments.
  - Reviews and validations.

Concepts

6-37. The following concepts guide employment of EOD teams:

- Commander, US Army Forces Command provides EOD support to CONUS land mass except other services' installations.
- 52nd Ordnance Group (EOD) provides C^2.
- Each EOD company is assigned a specific geographical response area.
- Installations are responsible for contacting and integrating the supporting EOD company into their FP program.
- Installations not assigned an EOD company must contact the EOD Ordnance Group for support.
- Teams are detached from an EOD company to handle most conventional ordnance incidents and can operate independently up to 72 hours.
- Several light response teams can be grouped to work large multi-UXO, large IED, and/ or WMD.
- A heavy response team with special and/or one-of-a-kind tools and equipment can augment light teams.
- For nuclear incidents, the team leader must be an EOD-qualified officer.
- 100% mobile and equipped with organic equipment.
- Normal sequence of events to handle a suspect device/package—
  - Evacuate the area.
  - Report incident to MP.
  - Activate the alert procedures (MP desk sergeant) (normally includes IOC, security team, medical facility, fire department, engineers, EOD team, and public affairs officer).
  - Dispatch EOD response team which reports to incident commander.
  - Brief all responders (incident commander).
  - IAW EOD procedures, develop a plan (detonation and mitigation procedures included) and coordinate support with incident commander.

- Begin EOD operations (render-safe procedures or item moved to remote area).
- Once device rendered safe, continue actions by the responsible law enforcement agency.

??In Army emergencies, the closest Army EOD unit responds with the understanding that the responsible Service retains operational control in their areas of responsibility (Responsibilities: Army-their installations, land-mass areas except Navy, Marine Corps, or Air Force installations; Navy-their installations, oceans, canals, enclosed bodies of water and up to high-water mark of sea coasts, inlets, bays, and harbors; Marine Corps-their installations; Air Force-their installations).

6-38. Figure 6-5 lists 24-hour EOD contact telephone numbers.

EOD 24-Hour Contact Headquarters Telephone Numbers		
Department of the Army Operations Center	(703) 697-0218/0219	DSN 227
Forces Command Operations Center	(404) 464-5222	DSN 367
52d Ordnance Group	(404) 469-3333	DSN 797
3d Ordnance Battalion, Fort Lewis, WA	(253) 937-1971	DSN 357
63d Ordnance Battalion, Fort Dix, NJ	(609) 562-5940	DSN 944
79th Ordnance Battalion, Fort Sam Houston, TX	(210) 221-1308	DSN 944
184th Ordnance Battalion, Fort Gillem, GA	(404) 469-5225	DSN 797

Figure 6-5. EOD 24-Hour Contact Headquarters Telephone Numbers

Training

6-39. EOD teams are trained on the following, with recurring refresher training for teams and individuals:

??EOD procedures, tools, and equipment.

??Performance of EOD tasks in CBRN environments.

??Basic EOD diagnostic procedures.

??EOD access techniques.

??Safety policies for ammunition and explosives.

Chapter 7

Installation Operations Center

OVERVIEW

7-1. The C^2 functions are performed through an arrangement of personnel, equipment, commnications, facilities, and procedures. The IOC is a key component of the FP C^2 structure. Through the IOC, the commander is assisted in integrating all the FP functions and systems toward the common goal of FP mission accomplishment. Listed below are the aspects to consider in establishing an IOC.

CAPABILITY

7-2. The IOC must be able—

- ??To identify and be proactive to changing situations.
- ??To provide a continuous, interactive process of reciprocal influence between the commander, the staff, and available support personnel and teams.
- ??To mitigate chaos and reduce uncertainty.
- ??To maintain an accurate and reliable common operating picture (COP) commensurate with FPCON.

MISSION

7-3. The missions include—

- ??Monitoring the security status based on the FP plan.
- ??Reacting to internal and external crises by providing information and issuing guidance to subordinate elements, agencies, higher headquarters, and civilian agencies.
- ??Issuing operation orders and fragmentary orders based on command guidance.
- ??Serving as the tasking office (director of plans, training, and mobilization [DPTM] may do this function externally to the IOC).

- Receiving and disseminating specific information requirements, spot reports, and operational reports (Appendix P).
- Maintaining force tracking of all units/organizations on post.
- Tracking the task organization for different levels of FP and mobilization.
- Identifying and tracking participation in disaster relief operations.

CHARACTERISTICS

7-4. In the current operating environment, the following characteristics should be incorporated:

- Maintaining accountability and positive control of personnel.
- Operating the IOC like a tactical operations center with a 24/7 cycle.
- Determining additional manning based on FPCON.
- Manning with installation staff representatives, non-DOD agencies, and liaison officers with decision-making ability. Include the following agencies:
  - DPTM.
  - Public affairs office.
  - Provost marshal office.
  - Director of information management.
  - Department of public works.
  - Director of logistics.
  - CID.
  - MI.
  - Staff judge advocate.
  - Medical department activity/dental activity (MEDDAC/DENTAC).
  - Adjutant general.
  - Chaplain.
  - Non-DOD agencies—
    - FBI.
    - State Emergency Management Agency or equivalent.
    - FEMA.

- Local law enforcement.
- Others as situation dictates.

- Liaison officers—
- Tenant organizations.
- Tactical units.

- Resourcing adequately for 24/7 operations.
- Incorporating battle hand-off procedures.
- Incorporating a chain of command.
- Organizing along functional staff lines to include (Figure 7-1):
  - Operations officer.
  - Battle captains.
  - Battle trackers.
  - Communications cell.
  - CBRNE cell.
  - Fusion cell (MI/CID).

Title	Number	Grade	Duty Period
IOC Operations Chief	1	GS 11	Duty Day
Battle Captain	5 (24/365 ops)	GS 9	8-Hour Shift
Battle Staff	5 (24/365 ops)	GS 7	8-Hour Shift
COMM/ELEC Monitors	5 (24/365 ops)	GS 5	8-Hour Shift
CBRN Specialist*	2	E7/03	Duty Day
Intelligence Supervisor**	1	GS 13	Duty Day
Intelligence Analyst**	5 (24/365 ops)	GS 11	8-Hour Shift
CID Analyst**	5 (24/365 ops)	E6/W02	8-Hour Shift
Total Personnel	29		

*Part of CBRN-IST
**Fusion cell

Figure 7-1. Recommended IOC Manning

Note: Actual IOC manning subject to TDA resourcing limitations.

- Organizing the area to include—
  - Brief area.
  - Work area.
  - Communications area.
- Using battle tracking tools. For example:
  - Event log.
  - Installation security plan overlay.
- Tracking visually the mission, personnel, equipment, incidents, and taskings with status boards.
- Establishing an effective and user friendly IOC plan/SOP.
- Ensuring facilities have a redundant power source, secure location, and a secure alternate location.
- Communications and information capabilities (Figure 7-2) must be—
  - Multi-modal with redundancy and flexibility.
  - Secure.
  - Able to provide an on-post emergency services net.
  - Expandable.
  - Interoperable with non-DOD communications and information systems.
  - Minimized to reduce operations security requirements.
- Incorporating an after action report process.

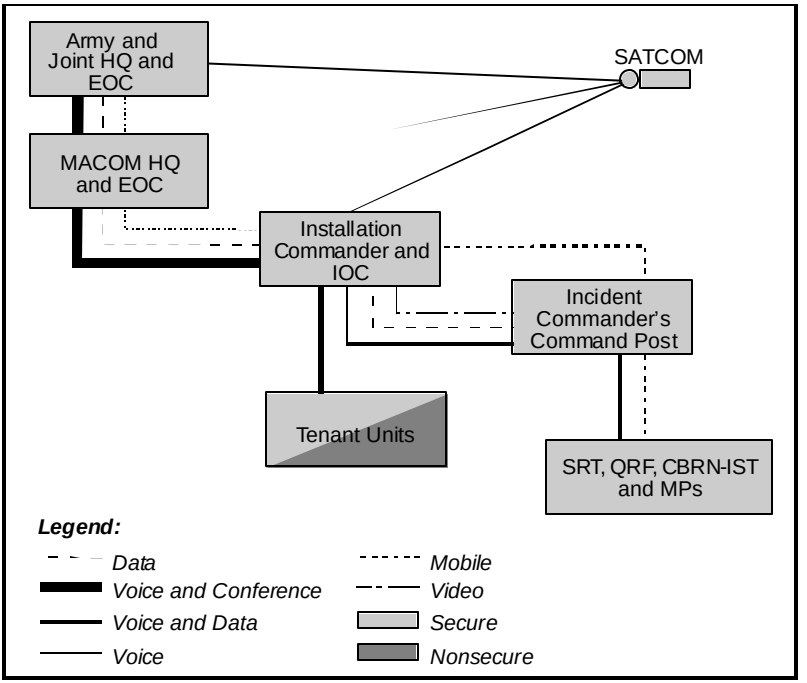


Figure 7-2. FP C^4 Operational Architecture

Chapter 8

Information Operations

OVERVIEW

8-1. Commanders conduct IO to apply the information element of combat power. IO comprises two components, offensive IO and defensive IO, also known as information assurance (IA). The goal of IO is to gain and maintain information superiority, a condition that allows commanders to seize, retain, and exploit the initiative. It facilitates more effective decision-making and faster execution. IO involves a constant effort to deny adversaries the ability to detect and respond to friendly operations, while simultaneously retaining and enhancing friendly force freedom of action.

8-2. IO in support of FP at the installation level centers on IA, specifically network and information system security, as installations lack the resources to conduct offensive IO. This chapter provides a brief description of IA (network security, TRADOC IA program, risk management, and vulnerability assessments), threats, approved IA software tools, INFOCON, and a network security checklist to assist installation commanders in protecting the installation network infrastructure.

INFORMATION ASSURANCE

8-3. IA is the defensive component of IO to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of information and information systems. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

NETWORK SECURITY

8-4. Installation commanders have the responsibility of ensuring that all networks and information systems are protected. Implementation of IA countermeasures is through the IA personnel structure from the installation IA manager (IAM) to the TRADOC IA program manager (IAPM) IAW AR 380-19.

8-5. Network security is the process of preventing and detecting unauthorized users on the network. Prevention measures help stop unauthorized users (intruders) from accessing any part of your network infrastructure. Network security involves—

??Protection. Protect the information network from malicious threats, such as computer viruses or software programs that compromise or damage data and systems, and unauthorized users.

??Detection. Use network security tools to detect security policy violations, intrusion attempts, events or occurrences (such as numerous log-in attempts within a specified period).

??Reaction. React accordingly to correct the problem. Operate during periods of degraded operations due to hostile attacks. Report and restore destroyed and/or compromised data.

INFORMATION ASSURANCE MANAGER COUNTERMEASURES

8-6. The IAM is responsible for implementing network security countermeasures to prevent unauthorized entry or denial of service of the network. The following are essential in network protection: regularly scheduled self-assessments to determine network vulnerabilities, firewalls to block unauthorized intruders, current virus definitions on installation-controlled devices, access control list to restrict access to networked devices, implementing information assurance vulnerability alert (IAVA) countermeasures, and incident reporting procedures IAW AR 380-19. Directors of information management (DOIM) support the intrusion detection systems (IDS) managed by the CONUS-Theater Network Operations and Security Center.

USER COUNTERMEASURES

8-7. The user may implement countermeasures to prevent an intrusion or report an intrusion/incident to the information assurance security officer (IASO) or supervisor. Typical, and critical, user countermeasures include password control (i.e., not sharing passwords, ensuring passwords meet AR 380-19 format standards, and changing passwords at least every 6 months for unclassified systems), locking workstations when not in use for 10 or more minutes, reporting system anomalies and data corruption to the IASO, using only government-authorized tools and system services (no modems, no unauthorized software, scanning disks for viruses, etc). Annual

information awareness training is an important tool to meet and maintain user certification. User countermeasures are effective when users (military, civilians, and government contractors) assume an active IA role and are properly trained and certified.

INFORMATION ASSURANCE MANAGER RESPONSIBILITIES

8-8. The IAM is responsible, to the installation commander, for ensuring all systems (networked and stand-alone) have current software change packages and fixes, have current antivirus definitions, and are IAVA compliant. In addition, the IAM is responsible for verifying DOIM and tenant devices have applied all IAVAs; checking and ensuring no unauthorized modems are in use; conducting vulnerability self-assessments; maintaining audit log files on all critical devices (DOIM- and tenant-controlled devices); ensuring all systems have met security certification and accreditation requirements; supporting vulnerability assessments requested by the installation commander, DCSIM TRADOC, or the Army Computer Emergency Response Team (ACERT), or regional computer emergency response team (RCERT); and using only Department of the Army-approved IA software tools.

ARMY INFORMATION ASSURANCE PROGRAM

8-9. Installation commanders are responsible for implementing the Army information assurance program (AIAP). The AIAP is focused on securing information and its associated systems and resources. The AIAP will ensure availability, confidentiality, and integrity of the networks. AIAP will—

- ??Provide a unified approach to protecting classified and sensitive but unclassified information.
- ??Provide a risk analysis approach for identifying vulnerabilities and providing the appropriate safeguards.
- ??Identify vulnerabilities that occur as a result of the lack of security or ineffective safeguards.
- ??Ensure networks receive protection by implementing AIAP.

RISK MANAGEMENT

8-10. Organizational and operational dynamics demand a continuous review of the risk management program for effectiveness. Commanders must be

assured that network security controls are providing the desired results. A risk management assessment will—

??Ensure documented security techniques have not created a more serious vulnerability or risk.

??Ensure collective effectiveness of applied countermeasures for future security actions.

??Identify problem areas and additional security requirements.

VULNERABILITY ASSESSMENTS

8-11. An installation commander may request a VA be conducted on their installation network under the computer defense assessment program (CDAP). Commanders must submit a formal request through the TRADOC IAPM to Department of the Army DCSOPS for approval indicating intent, scope, and requested assessment dates. The CDAP is conducted by the ACERT or applicable RCERT. In addition, the ACERT has initiated the do-it-yourself vulnerability assessment program (DITY VAP). DITY VAP decentralizes the assessment process and provides a library of tools, technical support, training, and other forms of assistance to requesting commands and activities desiring to conduct their own VAs. The goal of DITY VAP is to provide unit- and command-level systems administrators and network managers an organic capability to perform self-assessments. Before the installation or tenant representative conducts a DITY VAP, he must first receive DITY VAP certification training through RCERT-CONUS. DITY VAPs provide a detailed level of security awareness down to an appropriate organizational level. Access to state-of-the-art VA tools and techniques and other technical support will be provided from the ACERT-CDAB (computer defense assistance branch) as the central authority and from the RCERT-CONUS, as needed. To request a CDAP assessment, or for more information on the DITY VAP, see the Land Information Warfare Activity ACERT NIPRNET web site at https://www.acert.belvoir.army.mil/cdap/.

THREATS

8-12. Threats to systems and networks can be generalized into the following categories:

??Intentional/deliberate.

✍Attacks on a computer system's ability to process or on its resources (software and data).

- Theft (e.g., cryptographic keys, userids and/or passwords).
- Corruption of databases, control programs, and physical destruction of information systems.

- Unintentional. Not malicious. Accidental loss of confidentiality, availability, passwords, or integrity of information and systems.
- Structural. Flaws in the construction of the physical environment, the physical configuration, or the system or application software.
- Natural. Natural threats such as earthquakes, flood, dust, temperature, and humidity vary greatly between locations and must be considered.
- Physical. Destruction and damage of components.

APPROVED INFORMATION ASSESSMENT TOOLS

8-13. The IA tools list is developed and maintained by the Department of the Army chief information officer/G6. IA tools include CIO/G6-approved security software and products. The Communications Security Logistics Activity (CSLA) is the Army's executive agent for procuring communications security (COMSEC) and information security IA products (network security tools). CSLA has established 10 blanket purchase agreements (BPA) for procuring IA products/tools. The CLSA BPAs include firewalls, intrusion detection systems, network vulnerability scanners, high assurance guard, purge tools, and DOD information technology security certification and accreditation process (DITSCAP) tool. More information on IA-approved tools can be found at http://www.us.army.mil. The following IA tools are national information assurance partnership tested and approved by Director of Information Systems for Command, Control, Communications, and Computers (DISC4):

- Firewalls.
  - Raptor/VelociRaptor E-ppliance.
  - Cisco PIX.
  - Lucent-managed firewall.
  - Gauntlet/WebShied E-ppliance.
  - Sidewinder.
  - Sunscreen.
  - Firewall-1.

??IDS.

- Intruder Alert (host-based IDS).
- RealSecure Engine (network-based IDS).
- Cybercop Monitor (host-based IDS).

??Network Vulnerability Scanners.

- Security test and analysis tool (STAT).
- STAT with the government IAVA key.
- Internet security systems scanner.
- Cybercop scanner.

??High Assurance Guard.

- Defense Message System/Defense Information Infrastructure Guard.

??Purge Tools.

- Shred (Uniplexed Information and Computing System (UNIX)-file tool–BETA).
- Unishred Pro (UNIX-hard drive tool).
- No*Trace (Windows 95/98, 2000, NT hard drive tool).

?? DITSCAP tool.

- Web certification and accreditation.

INFORMATION OPERATIONS CONDITIONS

8-14. The INFOCON system is implemented by the Secretary of Defense and administered through the Director for Operations, Joint Staff (J-3). Subordinate and operational unit commanders will use the INFOCON procedures developed by their higher headquarters (e.g., combatant commands or Services). Existing policy and procedures on COMSEC may be integrated into local INFOCON procedures at the commander's discretion. TRADOC Cir 25-01-1 contains TRADOC implementation procedures and countermeasures for each INFOCON level. The DCSIM TRADOC determines the TRADOC INFOCON level. Installation commanders may raise their INFOCON level to a higher level, as needed, to protect against threats directed towards a specific installation.

8-15. The purpose of INFOCON is to recommend actions to uniformly heighten or reduce defensive posture, defend against computer network attacks, and to mitigate sustained damage to the TRADOC information infrastructure, including computer and telecommunications networks and systems. The INFOCON system impacts all personnel who use DOD and Army information systems, protects systems while supporting mission accomplishments, and coordinates the overall defensive effort through adherence to standards.

8-16. INFOCON presents a structured, coordinated approach to defend against and react to adversarial attacks on TRADOC computer and telecommunication networks and systems.

8-17. There are five levels within INFOCON, with each level reflecting a defensive posture based on the risk of impact to military operations. INFOCON levels are—

??Normal.

??Alpha.

??Bravo.

??Charlie.

??Delta.

INFOCON NORMAL (NORMAL ACTIVITY)

8-18. This day-to-day condition warrants established routine security procedures. Typical threat IO activity at this level includes random probes on TRADOC's information infrastructure as detected by network automated IDS. Vu lnerabilities are assumed to be consistent with those documented in the systems security documentation for each computer network or in previous assessments of other communications systems. At this level, daily information systems security measures apply.

INFOCON ALPHA
(INCREASED RISK OF ATTACK)

8-19. This condition is declared when an increased risk of attack on TRADOC information systems exists. Typical threat IO activity at this level includes computer network scans, probes, or mapping. INFOCON ALPHA

is also established when military operations, contingencies, or exercises require—

??Increased security of information systems.

??Response to indications and warning or intelligence indicators identifying increased surveillance or reconnaissance against TRADOC's information infrastructure.

??Response to special alerts or advisories that have been received from DOD agencies indicating a general threat or new vulnerabilities may be existent.

INFOCON ALPHA measures must be capable of being maintained indefinitely.

INFOCON BRAVO
(SPECIFIC RISK OF ATTACK)

8-20. This condition is declared when a specific risk of attack against TRADOC information systems exists. This condition may be prompted by an information warfare threat warning assessment indicating specific adversary capabilities with evidence of intent. Typical threat IO activity at this level includes limited computer network attacks with minor operational impact. Other indicators may include—

??A significant increase in detected viruses.

??Limited denial of service attacks.

At this level, new or existing vulnerabilities must be identified and actions taken to mitigate them. These measures should be maintained for several weeks without undue personal hardships or degrading TRADOC's ability to operate.

INFOCON CHARLIE
(LIMITED ATTACK)

8-21. This condition applies when an actual information attack occurs or when intelligence indicates the possibility of an imminent information attack that could result in a significant operational impact. Typical threat IO activity at this level includes—

??Actual or threatened attempts to gain access to TRADOC computer network systems for the purpose of massive data destruction, false data creation, wide denial of service, or gaining control of critical systems.

??The injection across several networks of malicious code, viruses, Trojan horses, and e-mail bombs all fall into this INFOCON.

Response measures at this INFOCON are focused at protecting critical systems. When implemented for even short periods of time, response measures at this INFOCON could create personal hardship, affect peacetime capabilities, and have the potential for increased operational costs.

INFOCON DELTA
(GENERAL ATTACK)

8-22. This condition applies when general attacks against TRADOC information systems and networks significantly degrade readiness and operations. This condition may be prompted when extensive coordinated regional and global information attacks by entities with hostile intent toward/against the US and its allies are expected. Response measures at this INFOCON are focused on maintaining or restoring TRADOC's ability to operate its minimum critical systems. As with INFOCON CHARLIE, the response measures will likely result in personal hardships, increased operational costs (both time and dollars), and a degradation in peacetime capabilities.

8-23. Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions and are contained in TRADOC Cir 25-01-1.

INSTALLATION COMMANDER'S INFORMATION ASSURANCE GUIDE

8-24. Ultimately, the commander of the installation is responsible to ensure adequate resources are applied to the IA program and that it is successful. The commander's IA checklist is as follows:

??IA training certification is in compliance with CIO/G6 guidance on IA certification for all levels (users [contractors, military, civilian, and approved foreign nationals], system administrators, network managers, and IA personnel).

??Software security controls are in place to protect system software from compromise; only authorized licensed software is in use; disks are scanned for viruses before installing on government devices; existing, new and upgraded have completed security certification and

accreditation documentation; and only CIO/G6-approved IA security software is used.

??Security objectives and safeguards are maintained for classified electronic media IAW AR 380-5.

??Network security includes the correct configuration of firewalls, routers, switches, servers (to include web and proxy servers), workstations, and related devices.

??Antivirus definitions are current and are only from DOD or ACERT.

??Network self-assessments are conducted periodically IAW Chapter 1-7(e), AR 380-19.

??IAVA reporting process is in place that documents all corrective actions accomplished, and IAM conducts periodic random checks to verify compliance.

??Information systems security monitoring certification notification is applied to all electronic devices (to include computer warning banners), DD Form 2056 is on all telephones (except tactical telephones), and telephone or communications directory notice is IAW AR 380-53. Also, commanders will ensure confirmation of compliance with AR 380-53, paragraphs 2-4 and 2-5, not later than 1 July of each odd-numbered year to DCSIM TRADOC.

Chapter 9

Lessons Learned

SECURITY

9-1. Installation security policies and procedures historically have been oriented on crime prevention. In the future, they must also be threat-based.

9-2. Friction between security and convenience will always be an issue.

9-3. High standards at access control points must be maintained. Soldiers must—

??Remain alert.

??Maintain appearance and bearing.

??Not establish a routine.

??Be briefed on any information regarding potential threats.

??Receive initial and sustainment training on RUF.

9-4. Personnel are trained to recognize fake or altered ID cards and drivers licenses. Information is available at http://www.driverslicenseguide.com/ and http://www.counterfeitlibrary.com/cl/articles/barbook.asp.

Note: The appearance of commercial web sites does not constitute endorsement by the US Army or the information, products, or services contained therein. The US Army does not exercise any editorial control over the information found at these locations. Such commercial web sites are provided consistent with the stated purpose of this handbook.

9-5. Develop procedures for screening packages and other deliveries to the installation. Consider procedures for potential large-scale vehicle entry (e.g., moving vans during the summer PCS season, railroad access to and/or upwind of the installation).

9-6. Focus security resources on protecting military capability, not the installation (develop acceptable risks).

9-7. Perform personal security vulnerability assessments on all HRP. Remove all personal data (home address, name of school attended by children, etc.) from official biographies appearing in open-source material.

9-8. Assign both a criticality (importance, effect, and responsibility) and vulnerability (accessibility, recoverability, and construction) score for each

installation critical capability to help develop a prioritized protective areas list (part of threat and vulnerability assessment).

9-9. Do not let the threat use the installation web site as a source of sensitive information. Maps and pictures of the installation and its facilities, personal information on key staff, detailed information on housing units, and listings of special events and activities are examples of the types of information that should not be made available to anyone with Internet access. Potential solutions include security awareness training for personnel responsible for maintaining web sites, placing access controls on web sites, such as placing password restrictions on certain pages or recognizing access only from authorized *mil* servers, and creating an installation-exclusive intranet.

9-10. View the installation from the enemy's perspective.

9-11. Ensure tactics, techniques, and procedures are focused on countering future threats, not just past terrorist attacks (bottom line: threat-based).

9-12. Poorly secured vehicles make convenient weapons platforms for terrorists.

9-13. Review contract privileges for vendors. Never allow the use of post facilities for overnight parking or storage.

9-14. Gymnasium activities and sporting events are attractive targets.

9-15. As you progress to higher FPCON levels, consider requiring installation employees and contractors to bus to the main gate, thus decreasing access-point manpower requirements, delays, and possible concealed car bombs.

9-16. Establish specific procedural inspection standards for contract fuel and water trucks.

9-17. Give careful consideration to FPCON changes during a hostage situation. The terrorist will undoubtedly be monitoring TV and radio broadcasts. The garrison commander should consider restricting the movement of military and dependents on the installation during hostage situations.

FIRST RESPONDERS

9-18. Increase protection for first responders.

9-19. Ensure responders (QRF)—

??Are highly qualified personnel.

??Are provided detailed and quality guidance for each potential threat.

??Have effective capabilities (communications, transportation, personal protective gear, etc.).

??Have an embedded medical capability (combat life saver training and medics).

??Exercise regularly with realistic scenarios.

??Receive initial and sustainment training on RUF.

9-20. Change installation TDA to include authorization for necessary personnel and equipment to support responders.

INTELLIGENCE

9-21. Intelligence manpower assets within garrisons are extremely limited. Subsequently, installation threat assessment management groups lack the organic capability to produce strong, full-spectrum threat assessments. Potential sources of additional expertise include—

??Individual mobilization augmentees.

??Borrowed military manpower from tenant organizations.

??Requested TDA increases.

9-22. Intelligence assets assigned to the IOC become the nexus for the fusion cell.

??Work to eliminate intelligence sharing gaps between—

✍Military and civil law enforcement.

✍Law enforcement and MI.

✍MI and CID.

✍Military and civilian agencies.

??Using—

✍Exchange of liaison officers.

✍Compatible communications systems.

✍Regular updates.

✍Joint participation in exercises.

✍Establishment of MOUs/MOAs.

??Create an intelligence fusion cell—

✍Include military, federal, state, and local agencies.

✍Solicit input from private businesses on criminal behavior and critical infrastructure.

✍Share the CCIR and PIR within the fusion cell to enable all agencies to collect needed information.

✍Establish a single all-source intelligence product (maximizes interagency coordination while reducing duplication of effort).

✍As a standing entity, not one that has to be recreated every time the FPCON is raised above normal.

COMMAND, CONTROL, AND COMMUNICATIONS

9-23. Make the antiterrorism officer (ATO) a priority position (recommend the same level as the IOC operations officer) with clearly defined responsibilities. The MP School at Fort Leonard Wood offers a two-week ATO course.

9-24. Structure FP response as a military operation.

9-25. IOC SOP must be periodically reviewed, revised, and rehearsed to remain functional and relevant.

- Ensure IOC SOPs have an operational focus.
- Borrow tactical SOP ideas, adapt to the installation's needs, and continue to revise as required.
- Create an IOC SOP annex for each staff section with procedures describing how the staff section operates in an increased FPCON situation, to include continuous operations (24/7) for an indefinite period, and procedures and tools for tracking information. Ensure SOPs include procedures for conducting both internal and external coordination Ask the question, Who else needs to know?
- Conduct periodic, rigorous training exercises for IOCs and installation staff using their SOPs. Integrate federal, state, and local agencies into the training.
- Develop and implement a plan for regular and continuous updating of IOC SOPs based on experience, lessons learned, and new information. Examples of events that could trigger IOC SOP updates are—
  - Change in type of threat.
  - Change in laws.
  - Change in technology.
  - Change in mission.
  - Change in surrounding community.
  - Change in external agency mission/capabilities.

9-26. Installations are not resourced adequately to man IOC positions 24/7. To run continuous operations over extended periods requires five assigned personnel for each IOC position. Options available to installation commanders in the near-term are to have assigned personnel work extra shifts, which leads to burnout, or to task tenant organizations to provide the additional manpower required. Manpower borrowed from tenant organizations needs to be trained and verified before working in the IOC. In the long-term, the baseline IOC manning identified in the FP O&O must be added to installation TDAs and resourced.

9-27. IOC communications systems are ineffective, insufficient, and vulnerable to single point failures.

- ??Cell phones should be considered as backup/alternate means of radio communications.
- ??SIPRNET/NIPRNET should be provided with redundant, independent circuits.

9-28. The C^2 relationship and communications between the QRF and the chain of command at MEVA sites are not well defined. If there are multiple events, the QRF will be rendered useless quickly. MEVA guard forces will be the first QRF until the backup QRF arrives.

- ??Establish a clear chain of command for each MEVA site and for the QRF in the garrison SOPs.
- ??Ensure the QRF can reliably communicate with the chain of command at each MEVA.
- ??Establish a mission folder for each MEVA site.

9-29. Visibility of senior leaders checking their command, demonstrating calm, resolute leadership, and interacting with personnel at all levels is a key element that reinforces leader development and sustains morale.

9-30. Failure to get the word out in a crisis situation leads to the proliferation of rumors and increases stress and anxiety among soldiers, civilians, and their families.

- ??Frequent senior leader visits are key. They should—
  - ✍Target small groups.
  - ✍Inform and allow people to ask questions.
  - ✍Listen to the concerns of the soldiers and parents.
  - ✍Use a question-and-answer format to get the message across.
- ??Employ chain of command to get the word out.
- ??Utilize family readiness groups.

BOMB THREAT

9-31. Understand capability of the EOD team.

9-32. Incident commander, and his tasks, needs to be clearly identified in FP plans for each possible threat scenario.

9-33. Ensure EOD team can communicate with forward command post.

9-34. Be careful not to create a larger target by consolidating the forward command post in the vicinity of the bomb.

9-35. MOUs/MOAs need to support communication requirements with local law enforcement. Specify type of incidents about which they will be notified and the possible impact of the incident on the local community.

9-36. Ensure facilities in the vicinity of the incident area are checked for bombs.

9-37. Determine who helps the garrison commander to develop courses of action at the forward command post. Consider using your AT officer who, in turn, needs to use the FP program as a play book.

Appendix A

The Military Decision-Making Process

OVERVIEW

A-1. The MDMP provides a common framework for the IOC staff to do parallel planning. It provides a logical sequence of decisions and interactions between the commander and the staff. Figure A-1 depicts the definition, the sequential seven-step analytical process, and characteristics of this tool.

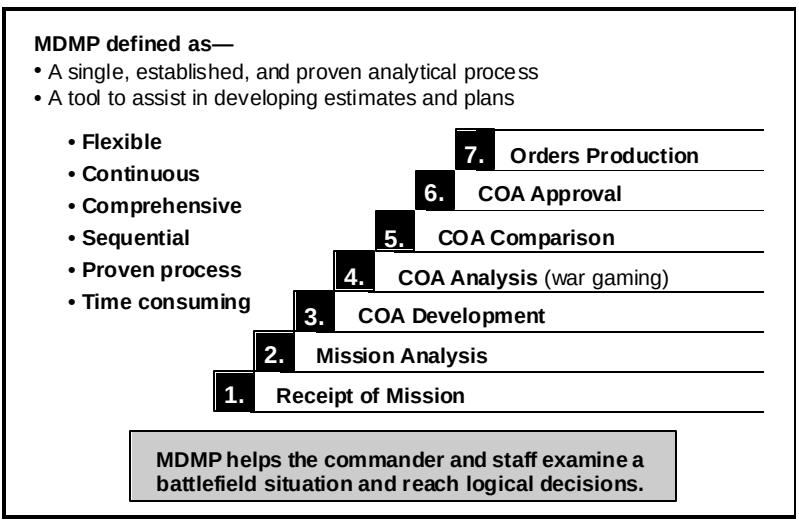


Figure A-1. MDMP

STEP 1
MISSION RECEIPT

A-2. The MDMP begins when a mission is received by higher headquarters or is deduced by the commander/staff.

STEP 2
MISSION ANALYSIS

A-3. The following are components of mission analysis (IAW AR 381-10 and AR 525-13):

??Analyze higher order.

??Complete intelligence preparation of the battlefield (IPB) by—

- Defining the installation AO (three concentric circles).
- Describing incident effects.
- Evaluating the threat (AR 381-10 considerations).
- Developing threat courses of action.

??Identify specified, implied, and essential tasks.

??Review available assets.

??Determine constraints.

??Identify critical facts and assumptions.

??Conduct risk assessment.

??Determine initial CCIR: PIR and FFIR.

??Determine, as required, EEFI.

??Prepare initial reconnaissance annex (inner, middle, and outer rings).

??Plan use of available time.

??Write the restated mission.

??Do mission analysis brief.

??Obtain restated mission approval.

??Obtain commander's intent.

??Obtain commander's guidance.

??Issue warning order (Appendix G).

??Review facts and assumptions.

A-4. Briefing format—

??Mission and intent two levels up.

??Mission, intent, and concept of higher.

??Commander's guidance.

??IPB products.

??Specified, implied, and essential tasks.

??Constraints.

??Forces available.

??Hazards and their risks.

??Recommended initial CCIR.

??Recommended timeline.

??Proposed restated mission.

A-5. Products (IAW AR 381-10 and AR 525-13)—

??Situation template (SITEMP) and event template.

??Restated mission.

??Commander's intent.

??Commander's guidance—

✍Friendly/enemy courses of action.

✍CCIR.

✍Reconnaissance guidance and deception.

✍Combat support/combat service support priorities.

✍Timeline and type order/rehearsal.

✍Warning order (Appendix G).

STEP 3
COURSE OF ACTION DEVELOPMENT

A-6. The components (IAW AR 381-10 and AR 525-13) for course of action (COA) development are—

??Analyze relative combat power.

??Generate options (suitable, feasible, acceptable, distinguishable, and complete).

??Array forces (first responders, SRT, QRF, CBRN-IST).

??Develop scheme of maneuver—

✍Purpose.

✍Risk.

✍Critical events.

✍Purpose of main effort.

- Purpose of secondary effort.
- Purpose of reserve (CBRN-RRT, SMART, EOD team, others).
- Inner, middle, outer installation rings.
- Responsibilities, graphics.

??Assign headquarters.

??Prepare COA statement and sketch.

A-7. Briefing format—

??IPB update.

??SITEMPs.

??Restated mission.

??Mission and intent two levels up.

??COA statement and sketches.

??COA rationale.

A-8. Products (IAW AR 381-10 and AR 525-13)—

??COA statements and sketches.

??SITEMPSs.

STEP 4
COURSE OF ACTION ANALYSIS

A-9. The components (IAW AR 381-10 and AR 525-13) are—

??Gather the tools.

??List friendly forces.

??Make assumptions.

??Develop critical events and decision points.

??Evaluate criteria.

??Select wargame method (zone, areas, perimeters).

??Select recording method (narrative, sketch, synchronization matrix, execution checklist).

??Wargame.

??Assess results.

A-10. Briefing format—

??Higher headquarters mission, intent, and deception.

??Updated IPB.

??COAs wargamed.

??Assumptions.

??Techniques used.

??For each COA identify—

✍Critical events.

✍Actions/reactions.

✍Pros and cons.

A-11. Products (IAW AR 381-10 and AR 525-13)—

??Refined/detailed COA and synchronization matrix.

??Location and timing of combat power at decisive point.

??Detailed task organization.

??Refined event template.

??CCIR and collation plan.

??Concept for reaction teams, engineer, and support.

??Subordinate tasks.

??Risk assessment (Appendix H).

STEP 5
COURSE OF ACTION COMPARISON

A-12. Components (IAW AR 381-10 and AR 525-13) are—

??Post criteria matrix.

??Weight criteria.

??Evaluate COA strengths and weaknesses.

??Consider each staff estimate.

A-13. Briefing format—

??Higher headquarters mission and intent two levels up.

??Restated mission.

??Status of forces.

??Updated IPB.

??For each COA list—

✍Assumptions.

✍Effects on staff estimates.

- Advantages/disadvantages.
- Risk (Appendix H).

??Recommended COA.

A-14. Products (IAW AR-381-10 and AR 525-13) are completed staff estimates.

STEP 6
COURSE OF ACTION APPROVAL

A-15. Products (IAW AR 381-10 and AR 525-13) are—

??Approved COA.

??Commander's guidance.

??Warning order (Appendix G).

STEP 7
PRODUCE ORDERS

A-16. Five paragraph orders format includes—

??Situation—

- Enemy forces.
- Friendly force.
- Attachments/detachments.
- Assumptions.

??Mission.

??Execution with the commander's intent for the following:

- Concept of operations (maneuver and reaction teams).
- Tasks to response teams.
- Tasks to support units.
- Coordinating instructions.

??Service support.

??Command and signal.

MILITARY DECISION-MAKING PROCESS OPERATIONALIZED

A-17. Figure A-2 operationalizes the FP MDMP processes by highlighting the integration of FP actions in the MDMP model. Also, using the MDMP system provides an efficient framework for planning, preparing, and executing the FP operational missions. Lastly, using MDMP simplifies the translation of the commander's FP vision through planning guidance and intent into plans and orders.

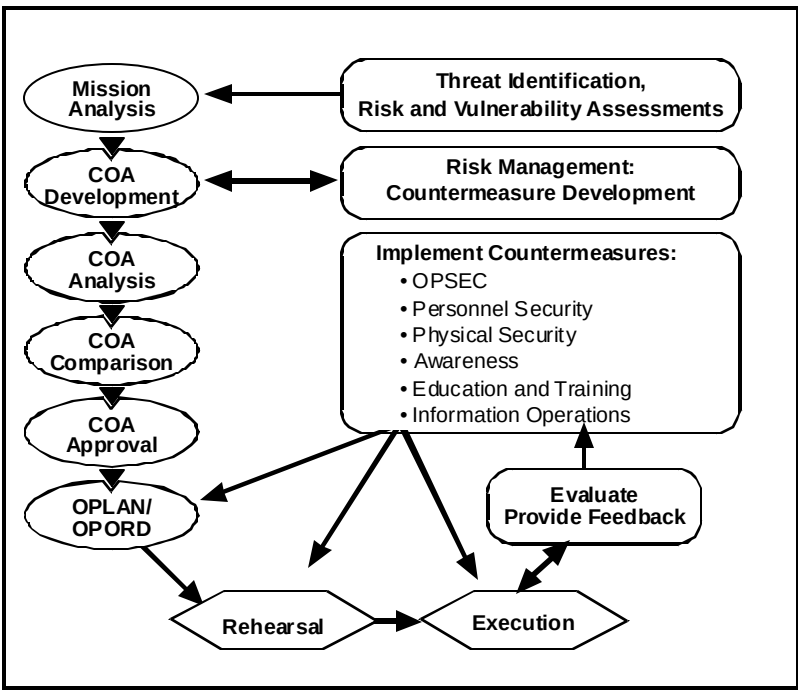


Figure A-2. MDMP Operationalized

Appendix B

DECISION SUPPORT TEMPLATE

OVERVIEW

B-1. A decision support template (DST) graphically represents the projected situation and identifies where a decision must be made to initiate a specific activity or event. It does not dictate decisions, but indicates when and where the need for a decision is most likely to occur.

B-2. DST graphically integrates—

??Time-phased lines and threat events, activities, and targets.

??Friendly events, activities, schemes of maneuver, and control measures from the synchronization matrix and the operation overlay.

??CCIR.

??Time estimates (calculations of times required to implement decisions).

B-3. FM 34-1 and FM 34-130 explain the elements of the DST. The process as explained in these references is designed for use by units operating in a field environment and must be modified when used to support installation FP planning.

OPERATIONALIZED FOR FORCE PROTECTION

B-4. The following six DST steps are used to support installation FP planning:

??Develop access control obstacle/avenue of approach (AA) overlay.

??Develop enemy situation event template.

??Develop event template.

??Develop target areas of interest (TAIs).

??Develop friendly course of action.

??Develop decision points (DPs) and critical events.

STEP 1
DEVELOP ACCESS CONTROL OBSTACLE/AVENUE OF APPROACH OVERLAY

B-5. The access control obstacle overlay/AA overlay helps the commander to visualize the enemy's means to gain access to the installation and how obstacles can be employed to deter or defeat the enemy's attempts. Obstacles can be physical (e.g., barriers), electronic (e.g., firewalls), or procedural (e.g., ID checks). Actions needed to develop the overlay include—

??Determine AAs.

- Ground–pedestrian, privately owned vehicles, public transportation, delivery services (rail, postal, package services, etc.).
- Air.
- Electronic.

??Determine resources available.

??Determine possible obstacle locations and types that minimize impact on mission. Also locate obstacles a sufficient distant from MEVAs/HRTs to prevent enemy from attacking without having to breach the obstacle.

STEP 2
DEVELOP ENEMY SITUATION EVENT TEMPLATE

B-6. The enemy situation event template is used to develop possible enemy COAs. As a minimum, the template should depict the most probable and most dangerous enemy COAs. Each COA must include the following:

??Who–enemy.

??What–type of operation.

??When–time action expected.

??Where–sector, zone, AA, enemy objectives.

??How–method enemy will employ assets.

??Enemy high-value targets.

STEP 3
DEVELOP EVENT TEMPLATE

B-7. The event template is a description of the indicators and activity expected to occur in each named area of interest (NAI). It normally cross-references each NAI and indicator with the times they are expected to occur and the COAs they will confirm or deny. The event template is used to—

??Wargame enemy COAs.

??Identify where enemy activity in each COA distinguishes it from other COAs.

??Establish NAIs.

??Focus on NAIs that help detemine and identify which COA the enemy selects.

??Guide development of ISR collection plan.

??Determine when and where to collect information.

STEP 4
DEVELOP TARGET AREAS OF INTEREST

B-8. TAIs depict engagement points or areas where interdiction of an enemy force will reduce or eliminate particular enemy capabilities or cause him to abandon, modify, or adopt another COA.

STEP 5
DEVELOP FRIENDLY COURSES OF ACTION

B-9. Based on the installation mission and the enemy situation event template, the staff develops friendly COAs. Each COA must be suitable (accomplish the mission), feasible (within the installation's capabilities), acceptable (in terms of resources, especially casualties), distinguishable (from other COAs), and complete. The steps for friendly COA development are—

??Assess available forces.

??Generate options.

??Array initial forces.

??Develop scheme of maneuver.

??Select control measures.

??Assign headquarters.

??Prepare COA statements and sketches.

STEP 6
DEVELOP DECISION POINTS AND CRITICAL EVENTS

B-10. A DP is the point in space and time where the commander or staff anticipates making a decision concerning a specific friendly COA. Critical events are those that directly influence mission accomplishment. DPs relate to identified critical events and are linked to NAIs and TAIs. Wargaming the enemy and friendly COAs identify DPs and critical events. For the selected friendly COA, the event template and the identified TAIs become the DST.

Appendix C

SYNCHRONIZATION MATRIX

OVERVIEW

C-1. A synchronization matrix provides a visible, clear method for ensuring the staff addresses all operating systems as they develop and record COAs. The matrix shows relationships between activities, units, support functions, and key events.

EXAMPLE

C-2. Figure C-1 illustrates an FP synchronization matrix. The tasks in the left column are the major tasks of an FP program. The FPCON (Alpha through Delta) are the conditions that are dealt with during the planning process and execution of the FP program. The numbers are the FP measures from AR 525-13 (see Appendix L for list), which are the minimum standards. As the FP guidance process migrates from an operation plan to an operation order and is then changed with fragmentary orders, the synchronization matrix must be updated. Also based on METT-TC, changes will need to be incorporated into the matrix.

FPCON				
Conditions / Task	A	B	C	D
Intelligence	9	28 (OPSEC Part)		
C3	2, 3, 7	12, 13, 20, 21, 28	30, 31	41, 47, 49
Security/ Response Forces	4	19, 26	35	42
Access Control	5	17, 18, 22, 23	32, 38, 39	44, 45, 46, 50
MEVA/HRP/HRT Security	6, 8	14, 15, 16, 25	33, 34, 36, 37	43, 48
CMD/CMTY Information Operations	1	11, 24, 27		

Figure C-1. Synchronization Matrix

Appendix D

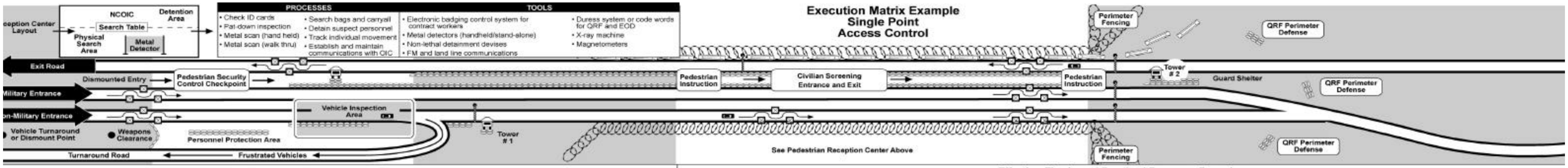
Execution Matrix

OVERVIEW

An execution matrix is a visual and sequential representation of the critical tasks and responsible organizations by phase of an FP operation used as a staff tool. It depicts when and where specific supporting actions must occur. FMs 71-123 and 101-5 provide a more detailed explanation.

EXAMPLE

Figure D-1 is a sample execution matrix for an installation access control point.



Layered System of Barriers that Delay Intruders Area

	Exterior Security Zone	Inspection Zone	Security Zone	Transit Zone	Interior Security Zone
	Processes/Tasks/Responsibilities				
mal	• Initial vehicle screen (spot check) • ID check (spot check) **2x guards** • Clear weapons (all) • Control non-mission vehicles	• Random inspection of vehicles (use bunkered inspection area) • Random inspection of vehicle occupants **1x guard** • Direct pedestrians to screening shack **1x inspector 1x NCOIC**	• Control flow of vehicles and pedestrians with a roving guard • Monitor/observe vehicles and report vehicles entering transit zone • Establish and maintain communications with HQs via FM and land line **1x roving guard and 1x tower guard**	• Establish speed limit in this zone and strictly enforce • Ensure visual of this zone with towers #1 and #2 • Establish the maximum number of vehicles in exit and entrance lanes at any one time	• Establish access point HQs • Establish base station for giant voice • Focal point for QRF • Monitor/observe vehicles exiting transit zone • Monitor flow of vehicles and pedestrians in/out with static and drop-arm barrier guards • Establish and maintain communications with tower #1, HQs via FM and land line **1x offic 1x NCO 2x RTO/ADM 3x guar 1x tower gua**
ne	• ID check (all) • Reduce flow of non-mission vehicles • Conduct random patrol (QRF) • Dog (MWD) Presence	• Increase inspection of vehicles (use bunkered inspection area) • Increase inspection of vehicle occupants **1x guard** • Begin dog (MWD) presence **1x MWD 1x Hander**	• Restrict flow of vehicles through drop-arm barrier • Monitor and record vehicles and report vehicles entering transit zone • Man the personnel alerting system in tower • Increase security in tower **1x Tower Guard**	• Roving guard in pedestrian walkway • Restricted zone for movement, speed limit and time limit for transit **1x roving guard**	• Control flow of vehicles in and out of zone • Establish protective and defensive positions to maintain perimeter • Maintain log and emergency numbers and frequencies • Place automatic weapon in tower • Establish casualty collection point and decon point • Establish pedestrian detention and security plan • Establish exterior warning plan for military and civilian organizations **1x gunner auto weapons in tow**
ro	• No non-mission vehicles inside base • Conduct routine patrols **1x MWD** • Use dogs (MWD) random **1x hander**	• Inspect all non-military vehicles (contractors) • Inspect all vehicle occupants • Use dogs (MWD) random	• Limit flow of transit zone to one vehicle at a time • Increase tower security with automatic weapon **1x Tower Guard** • Record all vehicles entering post **1x NCOIC**	• Reduce number of vehicles in zone at one time • Pre-position obstacle materials in this zone (cover or shelter from weather)	• Rehearse and control QRF (ID alert status) • Rehearse evacuation plan for guards forward of the zone • Establish field of fires and fire support plan • Rehearse casualty collection point and decon point • Rehearse pedestrian detention and security plan • Rehearse exterior warning plan for military and civilian organization
rile	• Dog (MWD) routine • Drill evacuation drill • Limit use of parking lot	• No random non-military vehicles on base (require preplanned arrivals only) • Use dogs full time	• Test evacuation plan • Test perimeter defense plan **1x MWD** • Test personnel protection plan (forward of perimeter) **1x hander**	• Restrict the use of the pedestrian walkway • Restrict the use of entrance land **1x squad 6-9 PAX**	• Clear all vehicles entering and exiting the perimeter with HQs • Upgrade QRF alert status • Log all vehicles entering or exiting perimeter • Position mounted weapon systems in zone for penetration pursuit • Increase active patrolling inside perimeter **1x squ 6-9 PA**
a	• Close parking lot • Close access, limit hours • Move overwatch weapons systems to vicinity tower #1	• Withdraw inspection team to interior perimeter only open for planned arrivals	• Maintain forward perimeter and position MWD to this zone • Clear all vehicle movement with HQs • First line of defense-prepared to pull into interperimeter/close obstacles	• Close lane with moveable and portable barriers • Control obstacles with detail	• Close vehicle and pedestrian lanes with moveable and portable barriers • Deny access and departure of perimeter • Be prepared to support exit and reception of external patrols • Increase lighting or go total black out (situational dependant) • Deploy QRF in zone **1x Pl (25-60 PAX) 2-3 Vehicl**
l Personnel	2x guards, 1x MWD & handler	2x guards, 1x NCOIC, 1x MWD & handler (same MWD teams)	4x guards, 1x NCOIC, 1x MWD & handler (same MWD teams)	1x guard, and 1x squad (9PAX)	1x officer, 1x NCOIC, 2 RTO/ADMIN, 5 guards, 1x squad (9 PAX), 1x QRF (25-40 PAX), and 2-3 combat vehic
	Supporting Technologies and Tools				
mal	• Signs • Temporary barriers Painted lines, rope, colored tape Sandbags, sawhorses, empty oil drums, and jersey walls	• Night observation devises • Loud speakers • Floodlights • FM and hardwire COMMO to HQs • Solid road surface to facilitate turnaround point • Inspection kit (pliers, screwdriver, hammer, flashlight, gloves etc.) • Detention kit (quick cuffs and surgical gloves)	• Organic communications equipment • Signs for movement and speed limit • Drop-arm barrier • Exterior lighting • Tower is platform for mass notification systems • Safe area for civilians (weather) • Electric power, bull horn • Flashlights (spotlights from tower)	• Haskin barriers (divide and protect walkways) • Lighting • Protective cover for pedestrians • Concertina wire • Sandbags • Speed signs	• Organic communications assets • Medics and aid bag • Haskin barriers • Drop-arm barriers • Second tower • Personnel alerting system on tower • External and internal lighting (power needed) • Generator • Concertina wire
ne	• Speed bumps • Extmal perimeter lighting • Construct protection bunkers	• Vehicle screening mirrors • Blast blankets • Blast mitigation containers • Duress system for guards and QRP • Vehicle inspection card • Protective positions for guards (bunker and sandbags) • Non-lethal weapons • Sawhorses for internal control • Handheld metal detectors	• Body armor for guards • Personnel alerting system • Personal duress • Non-lethal weapons • Additional detention kit • Automatic weapon for overwatching inspection point	• Body armor for patrols	• Automatic weapon(s) in tower • Body armor for guards • Saber 203 laser system
ro	• Security television systems • Ground sensors • Personnel alerting systems (speakers)	• Bomb swipe kits • 3meter telescoping mirror • Density meter • Body armor • Sonar vehicle Inspectors • Black Scatters • Under carriage inspectors	• CCTV • Bollards to protect tower • Thermal imagery • Laser range finder • Tire shredders • Nail boards • Saber 203 laser light		• Protective positions for guards • Fighting positions for QRF • Vehicle tracking tools
rile	• Fence sensors • Fence protection systems • Portable line sensors	• CCTV • Personnel alerting speakers • Individual duress systems • Flexible fiber scope (light) for fuel tanks • Video capture systems to aid EOD • Blast mitigation containers	• Conventional obstacles • Mines • Wire		• Wire and fence protections systems • Thermal imagery • Mobile barriers
a	• Intrusion detection systems • Thermal imagers	• Additional barriers • Conventional mines • Platoon early warning devices II	• CCTV monitors • Pre-positioned obstacle equipment • Obstacle marking kits		

Figure D-1. Access Control Point Execution Matrix

Appendix E

Running Estimates

OVERVIEW

E-1. The MDMP (Appendix A) is based on estimates that must be continually updated. The process of continuous updating of estimates is commonly referred to as maintaining *running* estimates.

EXAMPLE

E-2. As Figure E-1 illustrates, the elements of the MDMP are dependent upon one another. For example, a change in countermeasures will have an impact on threat capabilities, which in turn will affect the vulnerability of installation assets, which may in turn require new countermeasures. For this reason, the commander and his staff must continuously update their estimates of those variables upon which the MDMP is based.

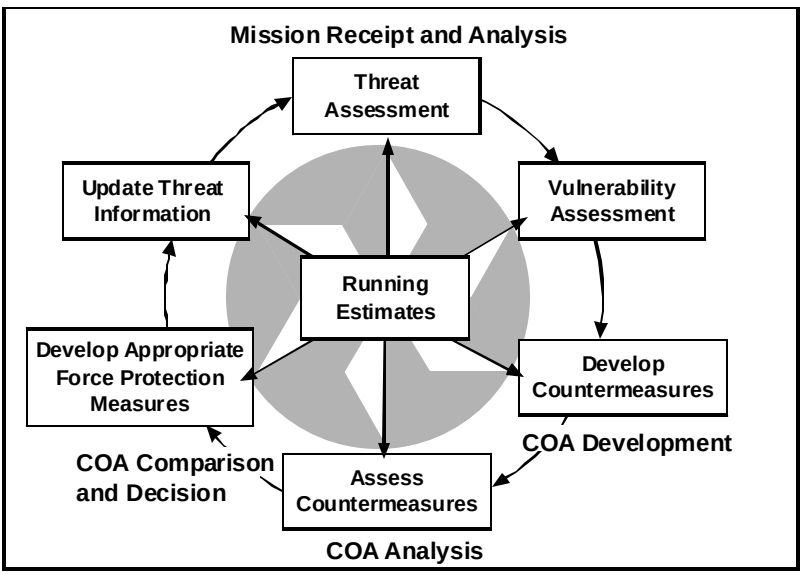


Figure E-1. Running Estimate

Appendix F

Troop-Leading Procedures
(Reaction Team Example)

OVERVIEW

F-1. Troop leading is the process a leader goes through to prepare his reaction team to accomplish an FP mission. It begins when he is alerted for a mission. It starts again when he receives a change or a new mission. The troop-leading procedure comprises the steps listed below. Many of them may be accomplished concurrently. During FP events, rarely will leaders have enough time to go through each step in detail. Leaders must use the procedure as outlined, if only in abbreviated form, to ensure that nothing is left out of planning and preparation, and that their team members understand the mission and prepare adequately. They continuously update their estimates throughout the preparation phase and adjust their plans as appropriate.

EIGHT STEPS

F-2. Step 1. Begin planning—

- ??Estimate the situation and analyze the mission.
- ??Plan the use of available time and issue warning order.
- ??Continue estimate of the situation—
  - ✍✍Analyze terrain maps, installation sketch, and/or aerial photograph of all three concentric rings of the installation AO for observation and field of fire, cover and concealment, obstacles, key terrain features, and avenues of approach.
  - ✍✍Analyze enemy strength, possible locations, dispositions, and capabilities.
  - ✍✍Develop, analyze, and compare COAs.
- ??Make preliminary plan

F-3. Step 2. Arrange for—

??Movement of team (where, when, how).

??Reconnaissance (select route, persons to take along, use of subordinates).

??Issuance of order (notify subordinate leaders of time and place).

??Coordination (adjacent and supporting units, agencies, and other DOD installations).

F-4. Step 3. Make reconnaissance (complete analysis of threat and terrain).

F-5. Step 4. Complete plan (confirm preliminary plan/estimate).

F-6. Step 5. Issue order.

F-7. Step 6. Supervise activities.

F-8. Step 7. Execute the mission.

F-9. Step 8. Debrief and turn in equipment.

Appendix G

WARNING ORDER
(REACTION TEAM EXAMPLE)

OVERVIEW

G-1. The team leader provides initial instructions in a warning order. The warning order contains enough information to begin preparation as soon as possible. Reaction team standing operating instructions should prescribe who will attend all warning orders and the actions they must take upon receipt: for example, drawing ammunition, rations, and water, and checking communications equipment. The warning order has no specific format. One technique is to use the format below. The leader issues the warning order with all the information available at the time. Updates are provided as often as necessary.

WARNING ORDER FORMAT

G-2. Brief statement of the situation.

G-3. Mission of the team.

G-4. General instructions—

??General and special organization.

??Uniform and equipment common to all.

??Weapons, ammunition, and equipment.

??Chain of command.

??Time schedule for the team's guidance.

??Time, place, uniform, and equipment for receiving the order.

??Times and places for inspections and rehearsals.

G-5. Specific instructions—

??To subordinate leaders.

??To special purpose components in the team and/or key individuals.

??RUF.

Appendix H

Risk Management

DEFINITIONS

H-1. FM 3-100.12 (formerly FM 100-14) defines risk management as "a process that assists decision makers in reducing or offsetting risk (by systematically identifying, assessing, and controlling risk arising from operational factors) and making decisions that weigh risks against mission benefits."

BENEFITS

H-2. Risk management assists the commander or leader by—

??Enhancing operational mission accomplishment.

??Supporting well-informed decision making to implement a COA.

??Providing assessment tools to support operations.

??Enhancing decision-making skills based on a reasoned and repeatable process.

??Providing improved confidence in unit capabilities. Adequate risk analysis provides a clearer picture of unit readiness.

??Preserving and protecting personnel, facilities, critical systems, and related support equipment while avoiding unnecessary risk.

??Providing an adaptive process for continuous feedback through the planning, preparation, and execution phases of military operations.

??Identifying feasible and effective control measures where specific standards do not exist.

PROCESS

H-3. FM 3-100.12 provides a cyclical five-step conceptual framework for risk management. The five steps are—

??Identify the threat.

??Assess the threat.

??Develop controls and make risk decision.

??Implement controls.

??Supervise and evaluate.

H-4. Subsequent cycles of the risk management process augment and refine the control measures in order to reduce risk to acceptable levels.

H-5. Figure H-1 depicts the five-step risk management process.

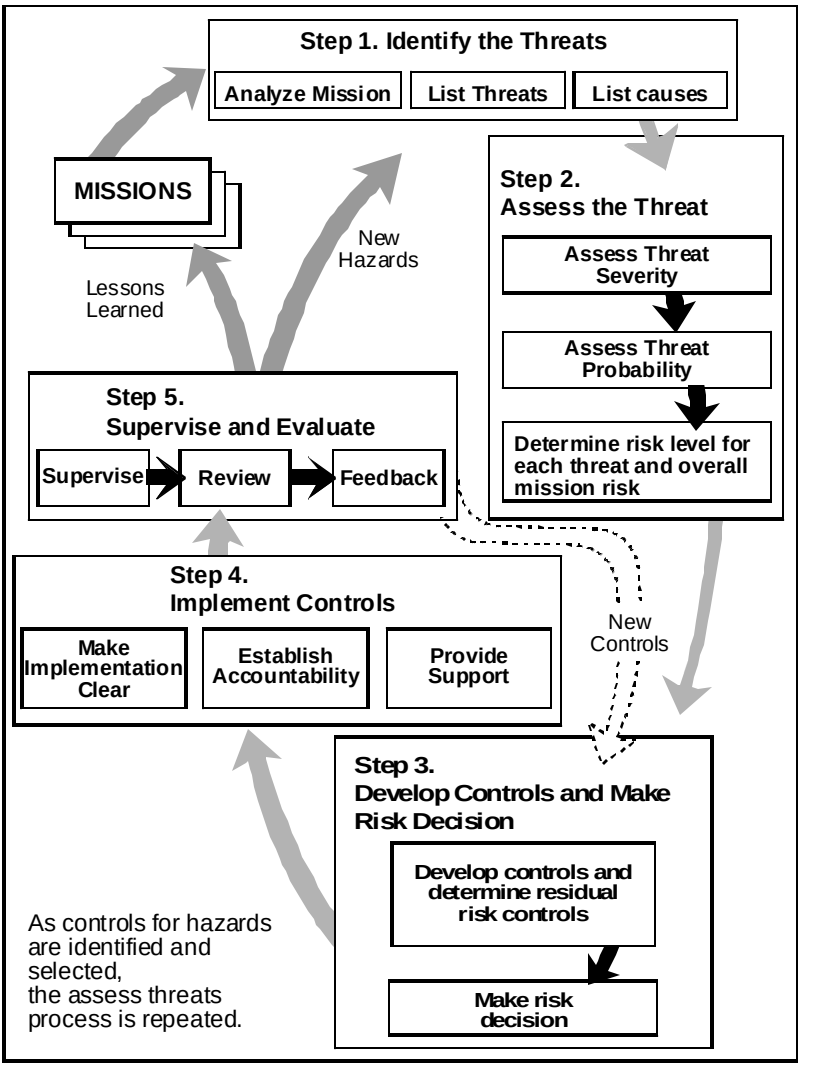


Figure H-1. Risk Management Process

TOOLS

H-6. DA Pam 190-51 provides guidance for conducting and documenting risk analyses for critical installation assets using a risk-level worksheet (DA Form 7278-R). The procedures (six steps) for completing the worksheet contained in DA Pam 190-51 provide a practical means of accomplishing step two (assess the threat) of the risk management process. The six steps for completing the worksheet are—

??Identify organization or unit that is responsible for the critical asset.

??Identify specific asset needing protection and appropriate asset category. For example:

✍A-Aviation aircraft, facilities, and components.

✍B-Vehicles, carriage, or towed weapons and motor pools.

✍M-Critical or high-risk personnel.

✍N-Military/civilian population.

??See Paragraph 2-3, DA Pam 190-51, for complete list.

??Determine asset value IAW Chapter 3, DA Pam 190-51.

??Determine likelihood of aggression IAW Chapter 4, DA Pam 190-51.

??Determine the risk levels for the asset IAW Table 2-2, Chapter 2, DA Pam 190-51.

??Determine required protection measures IAW AR 190-51 and AR 190-11.

H-7. Figure H-2 is an example of a completed risk-level worksheet.

Unit or Organization: B Co, 3/47 Inf. Date: 09 / 01 / 01

Inspectable Area: Motor Pool Analyst: SFC Smith

Asset Category	Value Rating Factors: Army Mission Criticality (Table 3-1)	Unit Mission Criticality (Table 3-1)	Replaceability (Table 3-1)	Relative Value (Table 3-1)	Sum of Value Rating Factors	Value Rating (Tables 3-2/3)	potential (✓)	Aggressors	Likelihood Rating Factors: Asset Profile (Table 4-3)	Usefulness (Table 1-1 — 1-6)	Asset Availability (Table 1-7)	Local Incidents (Past) (Table 1-8)	Nearby Incidents (Past) (Table 1-9)	Potential Threats (Table 4-16)	Accessibility (Table 4-11)	Law Enforcement Effectiveness (Table 1-17)	Deterrence (Table 4-18)	Sum of Likelihood Rating Factors	Likelihood Rating (Table 1-20)	Risk Levels (Table 2-2): Criminals/Vandals	Terrorists/Extremist Protest Groups
B	1	4	4	3	12	M	✓	Unsophisticated Criminals	4	3	3	1	1	2	8	4	4	30	M		
Description:							✓	Sophisticated Criminals	4	5	3	1	1	2	8	4	4	32	M		
Tactical vehicles including HMMWVs and 2-1/2 ton trucks.								Organized Criminal Groups													
							✓	Vandals/Activists	4	4	3	1	1	2	8	4	2	29	L		
														Highest Likelihood					M	II	
Combat vehicles including Bradley Infantry Fighting Vehicles.							✓	Extremist Protest Groups	4	2	3	1	1	1	8	2	6	28	L		
							✓	CONUS Terrorists	4	2	3	1	1	1	8	2	6	28	L		
								OCONUS Terrorists													
								Paramilitary OCONUS Terrorists													
														Highest Likelihood					L		II

DA FORM 7278-R, AUG 93 RISK LEVEL WORKSHEET

Figure H-2. Risk-Level Worksheet (Motor Pool Example)

H-8. This process does not apply for sensitive or classified information and nuclear and chemical materials.

Appendix I

Training and Planning Assistance

OVERVIEW

I-1. The Department of Defense has mandated FP training requirements for all military personnel, DOD civilians, and their family members under specific circumstances. Appendix F of AR 525-13 outlines AT awareness training, training for AT officers, AT pre-command training, and AT executive-level training. The following paragraphs list training and planning tools to assist in accomplishing training and planning requirements.

WEAPONS OF MASS DESTRUCTION-CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR (WMD-CBRN)

I-2. The United States Army Chemical School (Fort Leonard Wood, MO) provides Basic Capability and Operator CBRN Training to DOD military and civilian students serving in installation CBRNE first responder, CBRNE planner, Operations Center, Emergency Disaster Planning Officer, Emergency Response Working Group, or incident command positions.

I-3. The WMD-CBRN Installation Planners Course (40 hours) includes familiarization on:

??Federal regulations and DoD policies.

??Federal Response Plan.

??Military support to civilian authorities.

??Basic concepts of terrorism.

??Recognition, detection, and identification of CBRN agents and other hazardous materials.

??Personal protective equipment.

I-4. The Weapons of Mass Destruction Chemical, Biological, Radiological, and Nuclear (WMD-CBRN) Installation Emergency Responders Training Course (WMD-IERTC) (40 hours) includes familiarization on:

??Basic first responder techniques.

??Federal regulations.

??Recognition, detection, and identification of CBRN agents and other hazardous materials.

??Clandestine lab awareness.

??Toxicology.

I-5. The Joint Senior Leaders Course (20 hours) includes the following activities:

??Classified threat brief.

??Presentations featuring keynote speakers.

??Full dress-up exercise with live chemical agent training at the Chemical Defense Training Facility.

??CBRN wargame.

I-6. Registration information for the WMD-CBRN Installation Planners Course and the WMD-IERTC can be found at the following website: http://www.wood.army.mil/84chem/HHC/TTD/WMD/wmd.htm. Personnel interested in attending the Joint Senior Leaders Course should contact the Office of the Course Director at DSN 676-8076 or Commercial: 573-396-0131 ext 38076.

WEAPONS OF MASS DESTRUCTION INSTALLATION PREPAREDNESS PROGRAM SERVICES

I-7. US Army Soldier and Biological Chemical Command (SBCCOM) assists installations in developing WMD preparedness programs. The SBCCOM program is tailored to military installations, special facilities, and public or private venues. Mobile teams provide on-site delivery of the assistance. Products available through this program include the following:

??Command and staff workshop.

??Baseline assessment.

??Customized training program courses—

- Employee Awareness – 30-minute video.
- Responder Awareness – 4 hours.
- Responder Operations – 4 hours.
- Technician–HAZMAT – 16 hours.
- Technician–EMS – 8 hours.
- Hospital Provider – 8 hours.
- Incident Command – 8 hours.
- Command Workshop – 4 hours.

??Planning workshops.

??Chemical tabletop exercises.

??Biological tabletop exercises.

??Chemical weapons field exercises.

I-8. For more information on this program, contact the SBCCOM Homeland Defense Business Unit Leader at (403) 436-3674 or visit the SBCCOM website www2.sbccom.army.mil/hld/.

ADVANCED PHYSICAL SECURITY TRAINING PROGRAM

I-9. The Federal Law Enforcement Training Center (FLETC) provides training tailored to individuals requiring an in-depth knowledge of physical security. The training is conducted at its facility in Glynco, GA. Depending on individual needs, the training can be focused on any combination of the following subjects:

??Conceptual security considerations.

??Vulnerability assessment.

??Crime prevention theory and application.

??Risk assessment.

??Information and computer security.

??Bomb threat procedures.

??Facility security profiles.

??Security information and resources.

??Perimeter protection.

??Contingency planning.

??Legal issues.

??Guard force management.

??Security design.

??Intrusion detection systems.

I-10. The training may also include practical exercises.

I-11. For more information on this program, contact the Program Manager, FLETC, (812) 267-2354, or visit the FLETC website http://63.117.243.216/ssd/ssd_home.htm.

INSTALLATION ANTITERRORISM PROGRAM AND PLANNING TOOL

I-12. J34's Deputy Directorate for Operations (Combating Terrorism) maintains an installation planning template that provides formats for key aspects of an FP plan IAW DODI 2000.16. The template is available on CD ROM by contacting J-34 (DSN 223-7562, x104).

BATTLE COMMAND TRAINING PROGRAM

I-13. The battle command training program (BCTP) at Fort Leavenworth, KS, has a three-phase training program that is available by contacting the BCTP staff at (913) 684-5918 (DSN 552-5918). Proponency for this program will transfer to CASCOM. Future plans are for the Army Management Staff College to develop a single course for the staff of an installation operation center, a garrison chief of staff course, and to expand the current pre-command courses to include an FP simulation exercise.) The current three-phased BCTP for installations includes—

??Phase I. FP leader training conducted at Fort Leavenworth, KS, for two days. The audience is the garrison commander and key staff members.

??Phase II. Crisis decision making conducted at the installation for two days. The audience is the garrison staff, installation staff, virtual staff, and local civilian agencies.

??Phase III. Crisis response conducted at the installation for two days. The audience is the garrison staff, IOC staff, installation staff, and virtual staff.

US ARMY CORPS OF ENGINEERS

I-14. IAW AR 190-13, the Corps of Engineers maintains centers of expertise for protective design and intrusion detection systems. The centers may assist installations in developing solutions to FP vulnerabilities. Additionally, the Joint Program Office for Special Technology Countermeasures manages DOD critical infrastructure protection plans and may provide installation vulnerability studies. To use their services, contact one of the following:

??Army Engineering District, Omaha (402) 221-3817.

??Huntsville Engineering Support Center (256) 895-1756.

??Joint Program Office for Special Technology Countermeasures (450) 653-8589.

FORCE PROTECTION MODELING

I-15. The Technology Development Division serves as the field agent for FP for the Chairman of the Joint Chiefs of Staff. The agency develops software for FP modeling. For additional information, contact http://www.dtra.mil/td/td_index.html.

Appendix J

Rules for the Use of Force

OVERVIEW

J-1. RUF are different from the more familiar rules of engagement (ROE). RUF are escalating rules for US-based military personnel performing security duties when dealing with US citizens. ROE are directives delineating the circumstances and limitations for military forces to initiate or continue combat engagement with other forces. AR 190-14 prescribes RUF and any RUF published must be informed by its contents. It is recommended that the staff judge advocate review RUF prior to publishing.

EXAMPLE

J-2. An example of a RUF follows:

- A soldier has the inherent right of self-defense and the defense of others.
- Minimum force necessary and proportional to the threat is used.
- Deadly force is used only as a last resort—
  - For immediate threat of death or serious bodily injury to self or others.
  - For defense of persons under protection.
  - To prevent theft, damage, destruction of firearms, ammunition, explosives, or property designated vital to national security.
- When the situation permits, security personnel will utilize escalating degrees of force. These degrees are defined as—
  - SHOUT–verbal warnings to halt.
  - SHOVE–nonlethal physical force.
  - SHOW–intent to use weapon.
  - SHOOT–deliberately aimed shots until threat no longer exists.
  - Warning shots are not permitted.

Appendix K

Installation Watch Card
(For Soldiers and Families)

OVERVIEW

K-1. IAW AR 525-13 commanders will develop an awareness program to ensure visibility of the AT program and enhance awareness of all personnel. The more awareness a commander can inculcate in all personnel, the stronger the FP program will become. A multidimensional approach is essential. One technique to use is to develop an installation watch card for installation personnel.

EXAMPLE

K-2. The installation watch card shown in Figure K-1 illustrates one effective technique to increase AT awareness.

Installation Watch Card

Awareness is key! Everyone is a sensor.

Do: Observe and Report—

Unusual or suspicious activity or suspected surveillance.
Unusual questions or requests for information relating to capabilities, limitations, or operational information.
Unusual vehicles operating in or around the installation.
Unusual phone calls, messages, or e-mails.
Unusual contacts on or off post.
Unusual aerial activity near or around installation.
Any possible compromise of sensitive information.

Do Not—

Discuss any aspect of military operations or planning.
Discuss military capabilities or limitations.
Discuss FP measures, capabilities, or posture.
Disclose any information related to unit deployments.

Report any suspicious activity immediately to your chain of command or to the military police.

Your call may save lives!

Figure K-1. Installation Watch Card

Appendix L

Force Protection Conditions Measure Tracking Chart

OVERVIEW

L-1. There are five FPCON levels, Normal and ALPHA through DELTA, and each has individual security measures established by AR 525-13. Staff elements, tenant organizations, and building managers will report completion of each measure to the IOC IAW installation SOPs. Authority to increase FPCON level above command-directed level rests with the installation commander. Changes to FPCON level will be reported to TRADOC Operations Center via OPREP.

FPCON MEASURES TABLES

L-2. The specific measures by FPCON for installation commanders, installation staff, and tenant organizations to complete are listed in the following tables.

Table L-1. Individual Measures within FPCON Normal

AR 525-13 Requirements	Sample Implementing Guidance
Routine security measures designed to defeat the criminal threat.	??C^2 on call. ??MP patrols. ??Vulnerability and risk assessments. ??Security checks. ??SRT on call.

Table L-2. Individual Measures within FPCON ALPHA

AR 525-13 Requirements	Sample Implementing Guidance
1. At regular intervals, remind all personnel, including family members, to report the following to appropriate law enforcement or security agencies — (1) Suspicious personnel. (2) Unidentified vehicles. (3) Abandoned parcels or suitcases. (4) Any other activity considered suspicious.	**Notes:** (1) Pay particular attention to personnel carrying suitcases or other containers or those observing, photographing, or asking questions about military operations or security measures. (2) Emphasis on vehicles parked or operated in a suspicious manner.
2. (1) Personnel with access to building plans as well as the plans for area evacuations must be available at all times. (2) Key personnel should be able to seal off an area immediately. (3) Key personnel required to implement security plans should be on call and readily available.	**Note:** Ensure that law enforcement and security agencies have immediate access to building floor plans and emergency evacuation plans for HRT.
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.	
4. Increase unannounced security spot checks.	**Note:** Inspection of personal identification; vehicle registration; and the contents of vehicles, suitcases, briefcases, and other containers at access control points for US installations
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.	

Table L-2. Individual Measures within FPCON ALPHA (continued)

AR 525-13 Requirements	Sample Implementing Guidance
6. As a deterrent, randomly apply measures from 14, 15, 17, or 18 in Table L-3, either individually or in combination with each other.	
7. Review all operation plans and orders and SOPs, which pertain to implementation of FPCONs BRAVO through DELTA.	
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).	
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 FPCON BRAVO measures that, if implemented, could impact on their operations in the local community.	
10. Spare for MACOM or installation use.	

Table L-3. Individual Measures within FPCON BRAVO

AR 525-13 Requirement	Sample Implementing Guidance
In addition to the measures required by ALPHA, the following measures will be implemented:	
11. Increase the frequency of warnings required by Measure 1 in Table L-2.	**Note:** Also inform personnel of additional threat information, as appropriate.
12. Keep all personnel involved in implementing AT-related contingency plans on call.	QRF on 4-hour recall. Capability to provide augmentation force. Committee and FP working groups.
13. Review provisions of all documents associated with implementation of CHARLIE.	
14. Move automobiles and objects, such as trash containers and crates, away from HRT and selected MEVAs.	**Note:** If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures in accordance with local plans (frequent inspection by explosive detector dog [EDD] teams, centralized parking, controlled access to parking areas, etc.).
15. Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.	
16. Inspect the interior and exterior of buildings in regular use for suspicious activity or packages, for signs of tampering, or for indications of unauthorized entry.	**Note:** At the beginning and end of each workday and at frequent intervals.

Table L-3. Individual Measures within FPCON BRAVO (continued)

AR 525-13 Requirement	Sample Implementing Guidance
17. (1) Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. (2) 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.	**Note:** If available, use trained EDD teams for inspection of suspicious items and to conduct periodic screening of mail.
18. (1) Inspect all deliveries to common-use facilities to identify explosive and incendiary devices. (2) Encourage family members to report suspicious packages to local law enforcement agencies and refrain from handling them until cleared by appropriate authority.	**Notes**: Some common-use facilities are messes, exchanges, guesthouses, clubs, libraries, schools, and others as locally designated. Use trained EDD teams for some inspections, when available.
19. Increase both overt and covert security force surveillance.	**Notes**: Surveillance at facilities such as messes, commissaries, exchanges, guesthouses, clubs, libraries, schools, chapel, and HRT to improve deterrence and build confidence among staff and family members.
20. Inform soldiers, civilian employees, and family members of the general threat situation to stop rumors and prevent unnecessary alarm. Periodically update all personnel as the situation changes.	

Table L-3. Individual Measures within FPCON BRAVO (continued)

AR 525-13 Requirement	Sample Implementing Guidance
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.	
22. Verify the identity of all personnel entering the installation, HRTs, and other sensitive activities specified in local plans (inspect identification cards or grant access based on visual recognition). Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (trunk, undercarriage, glove boxes, etc.) and the frequency of inspections of suitcases, briefcases, and other containers.	100% ID check at access control points and HRTs.
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.	Liberal use of random measures.
24. Increase security provided to off-post personnel in conjunction with local law enforcement agencies, where required and /or practicable, or transport off-post personnel to protected areas IAW local contingency plans. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.	

Table L-3. Individual Measures within FPCON BRAVO (continued)

AR 525-13 Requirement	Sample Implementing Guidance
25. Implement additional security measures for HRP.	**Notes:** For example, conduct of countersurveillance operations in accordance with existing plans. Consider providing 24-hour protective services protection for Level I HRP, if not already provided.
26. (1) Brief security personnel concerning the threat and policies governing use of force/ROE. (2) Repeat this briefing on a periodic basis.	**Note:** Security personnel include all law enforcement personnel, guards, and security augmentation force personnel.
27. (1) Increase liaison with local police, intelligence, and security agencies to monitor the threat to Army personnel, installations, and facilities. (2) Notify local police agencies concerning FPCON CHARLIE and DELTA measures that, if implemented, could impact on their operations in the local community.	Interface regularly with external agencies.
28. Test attack warning system and supporting evacuation plans, ensuring proficiency and appropriate OPSEC.	
29. Spare for MACOM or installation use.	

Table L-4. Individual Measures within FPCON CHARLIE

AR 525-13 Requirement	Sample Implementing Guidance
30. Continue all ALPHA and BRAVO measures.	
31. Keep all personnel responsible for implementing AT plans at their place of duty.	
32. Reduce installation and HRT access points to the absolute minimum necessary for continued operation.	
33. (1) Verify the identity of all personnel entering installations, facilities, and activities. (2) Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. (3) Increase the frequency of detailed vehicle inspections.	
34. (1) Remove vehicles parked within or near HRTs and MEVAs. (2) Implement centralized parking.	
35. (1) Issue weapons. (2) Ensure that all personnel are briefed on use of force/ROE. (3) Ensure that ammunition is available.	**Notes:** Applies to all law enforcement personnel, security guards, and guard force augmentation personnel, if not already accomplished. Particular criteria for use of deadly force. For immediate issue (for those personnel not already issued ammunition) and ensure that supervisory personnel are familiar with policies governing issuance of ammunition.

Table L-4. Individual Measures within FPCON CHARLIE (continued)

AR 525-13 Requirement	Sample Implementing Guidance
36. Increase security patrol activity to the maximum level sustainable, weigh the effort toward HRTs.	
37. Position guard force personnel in the vicinity of all HRTs and MEVAs.	
38. Erect barriers to protect against vehicle bomb attacks.	**Note:** Required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.
39. Consult local authorities about closing roads and facilities.	**Note:** Focus on those that might make sites more vulnerable to terrorist attacks.
40. Spare for MACOM or installation use.	

Table L-5. Individual Measures within FPCON DELTA

AR 525-13 Requirements	Sample Implementing Guidance
41. Continue all ALPHA, BRAVO, and CHARLIE measures or introduce those which have not already been implemented.	Response forces alerted and prepared to execute mission on order.
42. Augment guard forces to ensure absolute control over access to the installation, MEVAs, and HRTs.	
43. Identify the owners of all vehicles already on the installation and OCONUS owners in the vicinity of soft targets off installations.	**Note:** In those cases where the presence of a vehicle cannot be explained (owner is not present and has no obvious military affiliation), inspect the vehicle for explosive or incendiary devices, or other dangerous items, and remove the vehicle from the vicinity of HRTs as soon as possible.

Table L-5. Individual Measures within FPCON DELTA (continued)

AR 525-13 Requirements	Sample Implementing Guidance
44. Inspect all vehicles entering the installation, facility, or activity.	**Note:** 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, suitcases, boxes, and other containers in vehicles should also be inspected.
45. Limit access to installations, facilities, and activities to those personnel with a legitimate and verifiable need to enter.	Installation lockdown.
46. Inspect all baggage, such as suitcases, packages, and briefcases brought on the installation.	**Note:** Check for presence of explosive or incendiary devices or other dangerous items.
47. Take measures to control access to all areas under the jurisdiction of the US command or agency.	
48. Implement frequent inspections of the exterior of buildings (to include roof and subterranean areas) and parking areas.	**Note:** Security force personnel should conduct inspections at HRTs and MEVAs.
49. Cancel or delay all administrative movement that is not mission essential.	
50. Request 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.	**Note:** Facilities in the vicinity of military installations, facilities, and activities.
51. Spare for MACOM or installation use.	

Appendix M

News Release

The following is an example of a news release.

Alert Army Members Contribute to Effective Force Protection

FORT MONROE, Va. -- Soldiers, civilian employees, and family members can make valuable contributions to force protection measures throughout Training and Doctrine Command.

"The Army, along with the nation's other military services, will become the world's dominant antiterrorism and counterterrorism forces," said General XXXXXX, commander.

"Our military installations at home and overseas will be targets for terrorists seeking revenge for our success in Operation Enduring Freedom," he said. "Our security forces are taking measures to protect installations and our forces.

"Families and employees can help by being alert, looking out for individuals in places they don't belong or who are asking for information they shouldn't have. They should report these incidents to their provost marshals.

"Force protection measures will allow TRADOC to continue its mission of training new soldiers and developing leaders," XXXXXXX said.

"The Army's role in responding to the terrorist attacks of 9-11 will be a long-term effort," the general said. "President Bush has told the country not to expect a quick fix to the fight against terrorist organizations.

"The Army family must support each other so we can stay focused on the mission."

Installation commanders will try to allow life to continue as normal on installations, while still taking effective force protection measures, according to XXXXXX. People will see vendors allowed on post to support dining facilities; exchanges; commissaries; and morale, welfare, and recreation facilities.

"That does not mean that military operations are business as usual," he said. "We will have security measures that ensure force protection, operational security, and the mission that are consistent with the threat assessment.

"Cooperation and assistance from the Army family will make our force protection measures even more effective," XXXXXX said.

Appendix N

Suspicious Mail

INTRODUCTION

N-1. Mail historically has been used as an avenue of approach by our enemies with the common practice of sending explosive devices through the mail system. Installation personnel now face a more widespread harm of biologically contaminated mail in the United States Postal System. The actions recommended below are provided to help mitigate the impact of this expanded threat. An in-depth discussion of the mail FP measures is provided in TRADOC Cir 25-01-02.

N-2. Some indicators of a suspicious envelope or package are—

??Threatening message.

??Loose shifting material.

??Excessive postage.

??Handwritten or poorly typed address.

??Stains.

??Odors.

??No return address.

??Protruding wires.

??Lopsided or uneven envelope.

??Excessive weight.

??Unidentified powdery substances.

??Leaking fluids.

HANDLING

N-3. The following are actions recommended for addressees, mail handlers, and leader/supervisors.

ADDRESSEE

N-4. If received at work, the addressee will—

??Instruct others in the room to leave immediately.

??Slowly set the package down on a stable surface and not handle it any more.

??Not cover the package, even if leaking. Air movement from covering it could spread contamination. Also, covering the package makes it impossible to assess from a distance.

??Call coworkers/supervisor, if available. Explain the situation, ask if the sender can be verified, or whether the package was expected.

??Turn off fans and air conditioners in the room. If the room is served by a central air system, turn off the system if you can. Close windows and doors into the room as you leave.

??Go directly to the restroom and wash hands thoroughly with soap and water.

??Initiate emergency response by notifying MP/provost marshal.

??Clear the offices and restrooms in the immediate area of the room.

??Proceed to the evacuation rally point and direct departing personnel to the designated rally point.

??Make a list of personnel that were in the room and evacuated.

??Remain at evacuation rally point to provide information and for possible medical follow-up until released by incident command.

??Prevent reentry of unauthorized personnel into the immediate area.

N-5. If received at home, the addressee will—

??Instruct others in the room to leave immediately.

??Not shake or empty contents.

??Slowly set the package down on a stable surface and not handle it any more.

??Not cover the package, even if leaking. Air movement from covering it could spread contamination. Covering the package makes it impossible to assess from a distance.

??Call leader/supervisor, if available, and explain situation.

??Turn off fans and air conditioners in the quarters. Close windows and doors into the room as you leave.

??Go directly to restroom and wash hands thoroughly with soap and water. Remove clothes and shower if any contents were spilled on yourself or children.

??If you have a central heating/cooling air system, turn it off.

??Get everyone out of the quarters and keep people from coming back in.

??Initiate emergency response by notifying MP/provost marshal.

??Leave quarters, but remain on the scene to provide information and to receive possible medical follow-up until released by incident command.

MAIL HANDLER

N-6. The mail handler will—

??Instruct others in the room to leave immediately.

??Not shake or empty contents.

??Slowly set the package down on a stable surface and not handle it any more.

??Call coworkers, if available. Explain the situation, ask if the sender can be verified, or if a package is expected. If in doubt, assume it is suspicious.

??Call leader/supervisor, if available, and explain situation.

??Turn off fans and air conditioners in the room Close windows and doors into the room as you leave.

??Go directly to restroom and wash hands thoroughly with soap and water.

??Initiate leader actions if leader/supervisor not available.

??Evacuate facility to designated rally point.

LEADER/SUPERVISOR

N-7. If the mail is suspicious, the leader or supervisor will—

??Initiate emergency response by notifying MP/provost marshal.

??Disable ventilation systems or notify department of public works to shutdown ventilation systems.

??Assign monitors to manage clearing the immediate area. Instruct the monitors—

✍To clear the offices and restrooms in the immediate area of the room.

✍To direct departing personnel to the designated rally point.

✍To prevent reentry of unauthorized personnel into the immediate area.

✍To direct employees in the room to go directly to the restroom, wash their hands, evacuate, and await instructions.

??Hold all personel at evacuation rally point to provide information until released by incident command.

??Make a list of all personnel in the area that were evacuated.

??Notify the installation leadership of the situation.

N-8. Response preparation activities—

??Identify controls for ventilation systems and how to disable, if possible, by user.

??Identify evacuation routes and rally points and ensure all personnel are aware of them.

??Rehearse evacuation plan.

OPEN/LEAKING PACKAGE

N-9. Upon receipt of an opened or leaking envelope or package with an unidentifiable liquid, powder, or solid substance (as opposed to readily identifiable contents—soup mix, salad dressing, coffee creamer, etc.), treat the package as suspicious.

MAIL HANDLER

N-10. If a suspicious opened or leaking envelope or package is received, the mail handler will—

??Instruct others in the room to leave immediately.

??Avoid touching his face or breathing in any of the powder.

??Not try to clean substance area.

??Not touch, smell, taste, or try to identify powder.

??Not shake or empty contents.

??Slowly set the package down on a stable surface and not handle it any more.

??Not cover a package, even if leaking. Air movement from covering it could spread contamination. Covering it makes it impossible to assess from a distance.

??Gently remove any clothing contaminated with the substance and place on floor.

??Call leader/supervisor, if available, and explain situation.

??Initiate leader actions if leader/supervisor not available.

??Turn off fans and air conditioners in the room. Close windows and doors into the room as you leave.

??Go directly to restroom and wash hands thoroughly with soap and water.

??Evacuate facility to designated rally point.

??Shower as soon as possible and change clothes.

??Put clothes in plastic bag and maintain possession for turn-in to authorities or first responders.

LEADER/SUPERVISOR

N-11. The leader/supervisor will, if possible, determine whether the package is safe by finding out if it is expected or can be identified by a sender known to the addressee. If in doubt, assume it is suspicious and—

??Initiate emergency response by notifying MP/provost marshal.

??Disable ventilation systems or notify department of public works to shutdown ventilation systems.

??Assign monitors to manage clearing the immediate area. Instruct the monitors—

✍To clear the offices and restrooms in the immediate area of the room.

✍To direct departing personnel to the designated rally point.

✍To prevent reentry of unauthorized personnel into the immediate area.

✍To direct the employee(s) in the room to go directly to the restroom, wash their hands, evacuate, and await instructions.

??Hold all personnel at evacuation rally point to provide information until released by incident command.

??Make a list of all personnel in the area that was evacuated.

??Notify the installation leadership of the situation.

N-12. Response preparation activities—

??Identify controls for ventilation systems and how to disable, if possible, by user.

??Identify evacuation routes and rally points and ensure all personnel are aware of them.

??Rehearse evacuation plan.

??Provide utility coveralls to potentially contaminated personnel to change clothes.

??Provide plastic bags for contaminated clothes.

Appendix O

Family Media Guide

Note: It is command policy that the public affairs office coordinates all contact, on and off-post, between the media and service members/government employees.

MEDIA

O-1. Mission readiness and family readiness are complementary concepts. Both rely on using information as a critical tool. Wide distribution of information can enhance recruiting, retention, and family readiness. At the same time, wide distribution of unfavorable information can damage the image of the US Army and your unit and threaten the morale of family members. Incorrect or incomplete information can mislead family members and cause unnecessary concern during periods of mobilization and deployment. The bottom line is this: Messages you want to send about family readiness can be aided by using the news media.

O-2. You cannot dictate what the media says about you, nor can you necessarily attract their interest when you want it. There are times, however, when the media will be interested in your unit and your family members. If you are prepared, you can use the news media as a great tool to get your key messages out. Deployments and reunions are always newsworthy events that will attract press attention—so will bad news, such as casualties.

O-3. The news media must always receive accurate, complete, and timely information, whether it comes from you, your unit, or your family members. Well-informed unit members and their families can be confident interview subjects capable of giving the press the full story.

O-4. Learning to deal with the news media is vital for family members. Both the service member and the family members must understand their rights during interaction with the media.

O-5. Everyone needs to plan for a media event (see Figure N-1 for media tips for family members) well before it occurs. You should identify the three most favorable and three most unfavorable questions you might receive from the press. Prepare answers for those questions and rehearse how you would handle follow-up questions. Never forget—the press can serve as a highly effective conduit for information, which will boost the morale of not only the unit and its members, but other family members as well.

O-6. The news media is an integral part of American society and should be cultivated on a continuing basis. Not only can it be used as a means of providing information during periods of deployment, but it can also be used to enhance the public's image of the US Army, individual units, soldiers, and the families that support them.

O-7. Media wants to talk with soldiers, commanders, and subject-matter experts and family members, not *talking heads* or PAOs. You are the ones with credibility who can best tell the Army's story to the American people.

GUIDELINES FOR FAMILY MEMBERS

O-8. Know your rights. It is up to you whether or not to speak to reporters. If you do choose to speak, you may stop at any time. How much information you choose to provide the media is up to you, but remember that anything you say is on-the-record, that is everything you say can be published or broadcasted and identifies you by name, title, etc. Based on your wishes, the PAO can provide as much or as little information to the media as you desire.

O-9. Know the role and purpose of the American press. They perform an important job in our democracy by keeping the public informed. It is not harassment if they call you at home or stop you out in public asking for an interview. It becomes harassment only when they persist after you have said NO.

O-10. Know the reporter's identity. Write down the reporter's name, telephone number, and news organization before answering any questions. Do this even if you are not going to comment; this will discourage the reporter from persisting after you have said NO.

O-11. Know your limits. It is best not to talk about anything of which you do not have first-hand knowledge. A response of "I don't know" is perfectly

fine in response to questions for which you have no answer. Do not speculate or engage in rumor or gossip.

O-12. Know who will hear what you say. Even family members might have sensitive information, which should not be released. With today's technology, unauthorized sources can access what you say the moment you say it. On a positive note, your enthusiastic response about your spouse's mission can help build morale and show American resolve.

O-13. If you reside in government housing, you may not invite media to your home without prior clearance from the PAO. Media must be escorted when on post.

O-14. As a matter of courtesy, whether you live on or off post, please contact the PAO when media approaches you. The PAO is available to advise and assist you in any contact with the media.

O-15. Be careful about information you share. It would be typical terrorist tactics and asymmetric warfare to strike at the family members of deployed soldiers, especially for those who have gained a profile in the media. An attack on family members would be disastrous for the morale of deployed soldiers and that is precisely why such an attack is a possibility.

O-16. If your spouse calls home with information about the unit's return to the states, about casualties, or how the mission is going, remember that deployments spawn rumors. Some of what you are told could be sensitive, wrong, or subject to change. Unless information is verified, it is best to keep it to yourself. Keep in touch with your chain of command for accurate information.

O-17. For your own safety and security, as well as other family members, it is best not to announce to the general public that you are alone by giving out personal information such as your home address or telephone number. You may also want to consider not releasing your last name or the name of your children's school.

O-18. When speaking to media, you need to understand that everything you say is on-the-record. Spelled out below are explanations of the media terms on-the-record, background, deep background, and off-the-record:

??On-the-record. Everything you say can be published or broadcast, identifying you by name, title, etc.

??Background. Everything you say is subject to publication or broadcast, identifying you by whatever ground rules are established, such as a spouse of…, a mother of…, etc., but not by name.

??Deep background. Everything you say is subject to publication or broadcast, identifying you by whatever ground rules are established, but ensuring that your identity is protected. Examples: A knowledgeable family member, an on-post source, etc.

??Off-the-record. DON'T use this unless your life depends on it! First, reporters don't like to use it. It is only valid if you and the reporter agree ***in advance*** of anything that is said is off-the-record. You cannot say something and retroactively declare or request that it is off-the-record. Assume that the reporter can and will make every attempt to get the same information elsewhere. Since you have already given the information, the reporter will merely use that as ammunition to confirm it with other sources.

Appendix P

Suspicious Incident Reporting Procedures

OVERVIEW

P-1. Suspicious activities include such things as potentially hazardous packages, mail, or substances. Additionally, suspicious activities include surveillance activities of military facilities or operations on/near installations.

REPORTING PROCESS

P-2. Report suspicious incidents to the IOC via the SPOTREP IAW IOC procedures.

P-3. Initial report will be submitted immediately upon discovery by e-mail or telephone, using the SPOTREP format. Telephonic report will be followed with a written report within one hour. When written or electronic reports are used, call the IOC to confirm receipt. The report should cover the initial information available concerning each incident.

P-4. When reporting a suspicious incident, include the following information:

- ??Initial response or action taken (e.g. evacuation, HAZMAT team, rescue/recovery, first responders, etc.).
- ??Initial determination or identification of substance if known.
- ??Whether media coverage occurred or is likely.
- ??Casualties as a result of incident (names of individuals, illness, injury, or death).

P-5. After a final determination has been made for each incident—

- ??For incidents determined to be unfounded, provide telephonic report, followed by an operational report (OPREP), to the IOC.
- ??For incidents determined to be legitimate, provide telephonic report, followed by an OPREP, and official serious incident report IAW AR 190-40 in message format.

Glossary

A

AA	avenue of approach
ACERT	Army Computer Emergency Response Team
AIAP	Army information assurance program
AO	area of operation
APOE	aerial port of embarkation
AR	Army regulation
AT	antiterrorism
ATO	antiterrorism office

B

BCTP	Battle Command Training Program
BPA	blanket purchase agreement

C

C^2	command and control
CBRNE	chemical, biological, radiological, nuclear materials as high-yield explosive devices
CBRN-IST	chemical, biological, radiological, and nuclear installation support team
CBRN-RRT	chemical, biological, radiological, and nuclear rapid response team
Cbt-T	combating terrorism
CCIR	commander's critical information requirement
CDAP	computer defense assessment program
CI	counterintelligence

CID	criminal investigative division
COA	course of action
COMSEC	communications security
COP	common operating picture
CSLA	Communications Security Logistics Activity

D

DITSCAP	DOD information technology security certification and accreditation process
DITYVAP	do-it-yourself vulnerability assessment program
DOD	Department of Defense
DODD	Department of Defense Directive
DOIM	director of information mangement
DP	decision point
DPTM	director of plans, training, and mobilization
DST	division support template

E

EDD	explosive detector dog
EEFI	essential elements of friendly information
EOD	explosive ordnance disposal

F

FAA	forward assembly area
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FFIR	friendly force information requirement
FLETC	Federal Law Enforcement Training Center
FP	force protection
FPCON	force protection condition
FPHB	force protection handbook

H

HAZMAT	hazardous material
HRP	high-risk personnel
HRT	high-risk target

I

IASO	information assurance security officer
IAW	in accordance with
IDS	intrusion detection system
IED	improvised explosive device
INFOCON	information operations condition
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
IA	information assurance
IAM	information assurance manager
IAPM	information assurance program
IAVA	information assurance vulnerability alert
IO	information operations
IOC	installation operations center

M

MDMP	military decision-making process
MEDCOM	US Army Medical Command
METT-C	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MEVA	mission-essential vulnerable area
MI	military intelligence
MOA	memorandum of agreement
MOU	memorandum of understanding

MP	military police
MTF	medical treatment facility
MTTP	multiservice tactics, techniques, and procedures

N

NAI	named area of interest

O

O&O	operational and organizational
OPREP	operational report

P

PAO	public affairs office
PIR	piority intelligence requirement
PS	physical security

Q

QRF	quick reaction force

R

RAMP	random antiterrorism measures program
RCERT	regional computer emergency response team
ROE	rules of engagement
RUF	rules for the use of force

S

SBCCOM	Soldier and Biological Chemical Command
SITEMP	situation template
SMART	special medical augmentation response team
SOP	standing operating procedure
SPOE	seaport of embarkation

SRT	special reaction team
STAT	security test and analysis tool

T

TAI	target areas of interest
TRADOC	US Army Training and Doctrine Command

U

UNIX	Uniplexed Information and Computing System
UXO	unexploded ordnance

V

VA	vulnerability assessment

W

WMD	weapons of mass destruction

Bibliography

Public Law 100-707, *The Stafford Act* (with revisions), 1974. http://www.fema.gov/library/stafact.htm

Public Law 104-201, *Defense Against Weapons of Mass Destruction Act*, 1996. http://fas.org/spp/starwars/congress/1996/p1104-201-xiv.htm

10 USC 372-380, *Military Support for Civilian Law Enforcement Agencies*, 1956. http://www4.law.cornell.edu/uscode/10/ch18.html

18 USC 1385, *Use of Army and Air Force as posse comitatus*, 1981. http://www4.law.cornell.edu/uscode/18/1385.html

50 USC 36, *Foreign Intelligence and Surveillance Act of 1978*, 1978. http://www4.law.cornell.edu/uscode/50/1801.html

EO 12333, *United States Intelligence Activities*, 1981. http://www.tscm.com/EO12333.html

EO 12863, *President's Foreign Intelligence Advisory Board*, 1997. http://www.loyola.edu/dept/hula/eo12863.html

PDD 39, *US Policy on Counterterrorism*, 3 June 1995. http://www.fas.org/irp/offdoes/pdd39.htm

PDD 62, *Protection Against Unconventional Threats to the Homeland and Americans Overseas*, May 1998. http://fas.org/irp/offdocs/pdd-62.htm

PDD 63, *Critical Infrastructure Protection*, May 1998. http://www.fas.org/irp/offdocs/pdd/pdd-i63.htm

DODD 2000.12, *DOD Antiterrorism/Force Protection (AT/FP) Program*, April 1999. http://www.dtic.mil/whs/directives/corres/html/20012.htm

DODD 3025.1, *Military Support to Civil Authorities*, January 1993. http://www.dtic.mil/whs/directives/corres/html/30251.htm

DODD 3025.15, *Military Assistance to Civil Authorities*, February 1997. http://www.dtic.mil/whs/directives/corres/html/302515.htm

DODD 3025.16, *Military Emergency Preparedness Liaison Officer Program*, December 2000. http://www.dtic.mil/whs/directives/corres/html/302516.htm

DODD 3150.5, *DOD Response to Improvised Nuclear Device (IND) Incidents*, March 1987. http://www.dtic.mil/whs/directives/corres/html/31505.htm

DODD 3224.3, *Physical Security Equipment (PSE): Assignment of Responsibility for Research, Development, Testing, Evaluation, Protection, Procurement, Development, and Support*, February 1989. http://www.dtic.mil/whs/directives/corres/html/32243.htm

DODD 4500.9, *Transportation and Traffic Management*, December 1993. http://www.dtic.mil/whs/directives/corres/html/45009.htm

DODD 5160.54, *Critical Asset Assurance Program (CAAP)*, January 1998. http://www.dtic.mil/whs/directives/corres/html/516054.htm

DODD 5200.8, *Security of DOD Installations and Resources*, April 1991. http://www.dtic.mil/whs/directives/corres/html/52008.htm

DODD 5200.27, *Acquisition of Information Concerning Persons*, June 1979. http://www.dtic.mil/whs/directives/corres/html/520027.htm

DODD 5240.1, *DOD Counterintelligence (CI)*, May 1997. http://www.dtic.mil/whs/directives/corres/pdf/d52402_052297/d52402p.pdf

DODD 5525.5, *DOD Cooperation with Civilian Law Enforcement Officials*, December 1989. http://www.dtic.mil/whs/directives/corres/html/55255.htm

DODI 2000.14, *DOD Combatting Terrorism Procedures*, June 1994. http://www.dtic.mil/whs/directives/corres/html/200014.htm

DODI 2000.16, *DOD Combatting Terrorism Program Standards*, June 2001. http://www.dtic.mil/whs/directives/corres/html/200016.htm

DOD Manual 0-2000.12-H, *Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence*, February 1993. (Hard copy only)

Joint Pub 1-02, *Department of Defense Dictionary of Military and Associated Terms*, April 2001. http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

Joint Pub 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, March 1998. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_07_2.pdf

Joint Pub 4-01, *Joint Doctrine for the Defense Transportation System*, June 1997. http://www.dtic.mil/doctrine/jel/new_pubs/jp4_01.pdf

AR 55-46, *Travel Overseas*, June 1994. http://www.usapa.army.mil/pdffiles/r55_46.pdf

AR 190-11, *Physical Security of Arms, Ammunition and Explosives*, September 1993. http://www.usapa.army.mil/pdffiles/r190-11.pdf

AR 190-13, *The Army Physical Security Program*, September 1993. http://www.usapa.army.mil/pdffiles/r190-13.pdf

AR 190-14, *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*, April 1993. http://www.usapa.army.mil/pdffiles/r190_14.pdf

AR 190-16, *Physical Security*, May 1991. http://www.usapa.army.mil/pdffiles/r190_16.pdf

AR 190-30, *Military Police Investigations*, June 1998. http://www.usapa.army.mil/pdffiles/r190_30.pdf

AR 190-45, *Law Enforcement Reporting*, October 2000. http://www.usapa.army.mil/pdffiles/r190_45.pdf

AR 190-51, *Security of Unclassified Army Property*, September 1993. http://www.usapa.army.mil/pdffiles/r190-51.pdf

AR 190-56, *The Army Civilian Police and Security Guard*, June 1995. http://www.usapa.army.mil/pdffiles/r190_56.pdf

AR 190-58, *Personal Security*, March 1989. http://www.usapa.army.mil/pdffiles/r190_58.pdf

AR 195-2, *Criminal Investigation Activities*, October 1985. http://www.usapa.army.mil/pdffiles/r195_2.pdf

AR 360-1, *Army Public Affairs, Public Information*, September 2000. http://www.usapa.army.mil/pdffiles/r360_1.pdf

AR 380-5, *Department of the Army Information Security Program*, September 2000. http://www.usapa.army.mil/pdffiles/r380_5.pdf

AR 380-13, *Acquisition and Storage of Information Concerning Nonaffiliated Persons and Organizations*, September 1974. http://www.usapa.army.mil/pdffiles/r380_13.pdf

AR 380-19, *Information Systems Security*, February 1998. http://www.usapa.army.mil/pdffiles/r380_19.pdf

AR 380-67, *Personnel Security Program*, September 1988. http://www.usapa.army.mil/pdffiles/r380_67.pdf

AR 381-10, *The US Army Intelligence Activities*, July 1984. http://www.usapa.army.mil/pdffiles/r381_10.pdf

AR 381-12, *Subversion and Espionage Directed Against the US*, January 1993. http://www.usapa.army.mil/pdffiles/r381_12.pdf

AR 381-20, *The Army Counterintelligence Program*, November 1993. (Hard copy only)

AR 381-100, *Army Human Intelligence Collection Program* (Secret), May 1988. (Hard copy only)

AR 525-13, *Antiterrorism Force Protection AT/FP: Security*, September 1998. https://akocomm.us.army.mil/usapa/epubs/DR_pubs/DR_b/r525-13.pdf

AR 525-20, *Command and Control Countermeasures (C2CM)*, July 1992. http://www.usapa.army.mil/pdffiles/r525_20.pdf

AR 530-1, *Operational Security*, March 1995. (Hard copy only)

AR 550-51, *Emergency Employment of Army and Other Resources*, April 1998. http://www.usapa.army.mil/pdffiles/r550_51.pdf

TRADOC Reg 525-13, *US Army Training and Doctrine Command (TRADOC)*, December 1997. http://www.tradoc.army.mil/tpubs/regs/52513frm.htm

TRADOC Cir 25-01-1, *Information Operations Condition (INFOCON) Program*, August 2001. https://tradocsec.monroe. army.mil/tpubs/circular/c25-01-1.doc

TRADOC Cir 25-01-2, *Leaders' Guide for Identifying and Handling Hazardous Mail*, December 2001. http://www.tradoc.army.mil/tpubs/cirs/c25-01-2/c25-01-2.doc

Blueprint, *U.S. Army Installation Commander's Blueprint*, May 2001. http://www.doms.pentagon.mil/Blueprint/blueprint.pdf

Commander's Guide, *US Army Antiterrorism and Force Protection Installation Commander's Guide*, March 2000. http://www.doms.pentagon.mil/AT%20FP%20Installation%20Cdr's%20Guide/doms_new.pdf

DA Pam 50-6, *Chemical Accident or Incident Response*, May 1991. http://www.usapa.army.mil/pdffiles/p50_6.pdf

DA Pam 190-51, *Risk Analysis for Army Property*, September 1993. http://www.usapa.army.mil/pdffiles/p190-51.pdf

MEDCOM Pam 525-XX, *Medical Emergency Management Planning*, June 2002. (Hard copy only)

FM 3-0 (100-5), *Operations*, June 2001. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-0/toc.htm

FM 3-07, *Stability Operations and Support Operations* (Final Draft), 1 February 2002. http://www-cgsc.army.mil/cdd/index.htm

FM 3-4, *NBC Protection*, May 1992. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-4/toc.htm

FM 3-5, *NBC Decontamination*, July 2000. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-5/fm3-5.htm

FM 3-19.1, *Military Police Operation*, March 2001. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.1/toc.htm

FM 3-19.30 (19-30), *Physical Security*, January 2001. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm

FM 3-100, *Chemical Operations, Principles, and Fundamentals*, May 1996. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-100/toc.htm

FM 3-100.12 (100-14), *Risk Management*, March 2001. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-100.12/fm3-100.12.htm

FM 4-0, *Combat Service Support* (final draft), 22 August 2001. http://www.cascom.army.mil/Multi/Doctrine/FM_4-0_Combat_Service_Support/

FM 8-10-7, *Health Service Support in a Nuclear, Biological and Chemical Environment*, April 1993. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/8-10-7/toc.htm

FM 8-55, *Planning for Health Service Support*, September 1994. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/8-55/toc.htm

FM 8-285, *Treatment of Chemical Agent Casualties and Conventional Military Chemical Injuries*, December 1995. http://www.adtdl.army.mil

FM 19-10, *The Military Police Law and Order Operations*, September 1987. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/19-10/toc.htm

FM 19-20, *Law Enforcement Investigations*, November 1985. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/19-20/toc.htm

FM 34-60, *Counterintelligence*, October 1995. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-60/toc.htm

FM 34-130, *Intelligence Preparation of the Battlefield*, July 1994. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/34-130/toc.htm

FM 101-5, *Staff Organization and Operation*, May 1997. http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/101-5/default.htm

SBCCOM Preparedness Guide, *Improving Local and State Agency Response to Terrorist Incidents Involving Biological Weapons*, September 2000. http://www2.sbccom.army.mil/hld/downloads/bwirp/bwirp_interim_planning_guide. pdf

CJCSI 3125.01, *Military Assistance to Domestic Consequence Management Operations in Response to a Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive Situation*, August 2001. http://www.dtic.mil/doctrine/jel/cjcsd/cjcsl/cjcsi/3125_01.pdf

CJCSM 3150.03A, *Joint Reporting Structure Event and Incident Reports*, November 2000. https://ca.dtic.mil/doctrine/jel/cjcsd/cjcsl/limcjcsmdirectives.htm

CJCS Handbook 5260, *Commander's Handbook for Antiterrorism Readiness*, January 1997. http://www.dtic.mil/jcs/force_protection/gdi.html

US Army War College Reference Handbook, *How the Army Runs*, January 2001. http://carlisle-www.army.mil/usawc/dclm/HTARRevised.pdf

CD ROM Set, J34 Level IV Antiterrorism Executive Seminar After Action Report and Antiterrorism Informational CD-ROM, 19-21 June 2001.

Website, FEMA, http://www.fema.gov/

Website, Center for Army Lessons Learned, http://call.army.mil/

Website, J-34 Combating Terrorism, http://www.dtic.mil/jcs/force_protection/

Website, DOMS, http://doms.pentagon.mil/

Website, NGB, http://www.ngb.dtic.mil/

Website, Army NGB, http://www.arng.army.mil/

Website, National Disaster Medical System, http://www.oep.dhhs.gov/NDMS/ndms.html

Website, Off of Emergency Preparedness Counter Terrorism Program, http://www.oep.dhhs.gov/CG_Program/ct_program.html

Website, Center for Disease Control and Prevention, http://www.cdc.gov/

Website, National Preparedness Office, http://www.ndpo.gov/

Website, Department of Justice, http://www.ojp.usdoj.gov/

Website, SBCCOM (Homeland Defense), http://www2.sbccom.army.mil/hld/

Website, DOT Library, http://isweb.tasc.dot.gov/library/library.htm

Website, National Trans Library, http://www.bts.gov/ntl/

Website, Oklahoma City National Memorial Institute for the Prevention of Terrorism, http://www.mipt.org/rfp/

Note: The appearance of commercial web sites does not constitute endorsement by the US Army or the information, products, or services contained therein. The US Army does not exercise any editorial control over the information found at these locations. Such commercial web sites are provided consistent with the stated purpose of this handbook.

Top 10 CCIR

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____