



J34 Combating Terrorism

ANTITERRORISM FORCE PROTECTION Installation Planning Template

1 July 1998

ANTITERRORISM FORCE PROTECTION INSTALLATION PLANNING TEMPLATE
TABLE OF CONTENTS

INTRODUCTION	v
USING THE TEMPLATE.....	vi
BUILDING THE AT/FP INSTALLATION PLAN.....	vii
USER'S GUIDE.....	ix
AT/FP INSTALLATION PLANNING TEMPLATE.....	1
TASK ORGANIZATION	1
SITUATION.....	1
<i>General</i>	<i>1</i>
<i>Enemy Forces.....</i>	<i>1</i>
<i>Friendly Forces</i>	<i>1</i>
<i>Attachments & Detachments</i>	<i>1</i>
<i>Assumptions.....</i>	<i>1</i>
<i>Intelligence</i>	<i>2</i>
MISSION/PURPOSE.....	2
EXECUTION.....	2
<i>Commander's Intent</i>	<i>2</i>
<i>Concept of Operations.....</i>	<i>3</i>
<i>Tasks and Responsibilities</i>	<i>3</i>
<i>Jurisdiction.....</i>	<i>3</i>
<i>Coordinating Instructions</i>	<i>4</i>
Alert Notification Procedures	4
Rules of Engagement	4
Installation AT/FP Exercises	4
Incident Response.....	4
Consequence Management	4
Distinguished Visitor Protection	4
Operations Security.....	5
Access Controls	5
Barriers	5
Lighting	5
On-Site Security Elements	5
Technology.....	5
Training	5
Weapons of Mass Destruction	5
Information Operations	5
Airfield Security.....	6
Port Security	6
Buildings.....	6
LOGISTICS & ADMINISTRATION.....	6
<i>Readiness</i>	<i>6</i>
<i>Material and Services.....</i>	<i>6</i>
<i>Weapons and Ammunition.....</i>	<i>6</i>
<i>Medical Services.....</i>	<i>6</i>
<i>Personnel.....</i>	<i>6</i>

<i>Civil Affairs</i>	6
<i>Updates</i>	7
COMMAND & SIGNAL	7
<i>Command</i>	7
<i>Signal</i>	7
ANNEX A: RISK ASSESSMENT AND MANAGEMENT	8
ANNEX B: THREAT CONDITION (THREATCON) SYSTEM	1
<i>Appendix 1: THREATCONs</i>	5
<i>Appendix 2: Random Antiterrorism Measures</i>	6
ANNEX C: BUILD THE ACTION SET MATRICES	1
ANNEX D: TOOLBOX	1
<i>Appendix 1: Tasks & Responsibilities</i>	2
<i>Appendix 2: Alert Notification Procedures</i>	9
<i>Appendix 3: Installation AT/FP Exercises</i>	10
<i>Appendix 4: Incident Reaction Planning</i>	11
Bombing	12
Arson	15
Hijacking	16
Assassination	17
Assaults	18
Kidnapping	19
Hostage & Barricade	20
<i>Appendix 5: Consequence Management</i>	21
<i>Appendix 6: Executive or Distinguished Visitor Protection</i>	24
<i>Appendix 7: Operations Security</i>	28
<i>Appendix 8: Access Controls</i>	32
Pedestrian Access Control	33
Vehicle Access Control	38
Mail and Package Control	40
<i>Appendix 9: Barriers</i>	43
Pedestrian Barriers	45
Vehicle Barriers	46
Fences	48
<i>Appendix 10: Lighting</i>	51
<i>Appendix 11: On-Site Security Elements</i>	54
<i>Appendix 12: Technology</i>	57
<i>Appendix 13: Training</i>	59
<i>Appendix 14: Weapons of Mass Destruction</i>	67
<i>Appendix 15: Information Operations</i>	69
<i>Appendix 16: Airfields</i>	70
<i>Appendix 17: Ports</i>	72
<i>Appendix 18: Buildings</i>	77
ANNEX E: REFERENCES	1
ANNEX F: GLOSSARY	1
ANNEX G: ACRONYMS	1

INTRODUCTION

Protection of DOD personnel and assets from acts of terrorism is one of the most complex challenges for all Commanders. Planning to confront this challenge requires a comprehensive, integrated approach. DOD Directive 2000.12 (DOD Combating Terrorism Program) and DOD Instruction 0-2000.16 (DOD Combating Terrorism Program Standards) provide the Antiterrorism Force Protection requirements. The purpose of this Antiterrorism Force Protection Installation Planning Template is to provide Installation Commanders and DOD Antiterrorism Force Protection Planners a single tool to assist in the development of Antiterrorism Force Protection Plans.

The inherent responsibility of command, to protect personnel, is the focus of the Antiterrorism Force Protection Installation Planning Template. This tool is designed to assist you in developing your plan. Careful preparation of your AT/FP Plan with the Planning Template will help you achieve the four AT/FP objectives: deterring terrorist incidents, employing countermeasures against terrorists, mitigating the effects of terrorist acts, and recovering from terrorist incidents should they occur.

The Planning Template uses three simple steps. In the first step, you will complete an assessment of four central elements: threat, criticality, vulnerability, and deterrent & response capabilities. You will then use this assessment's linked elements to assist you in subjectively quantifying risk, as the first portion of risk management. In the second step, you will develop a set of implementation actions which form a coherent, comprehensive set of force protection "How-to" measures for your installation. In the third step, you will prepare your AT/FP Plan in a 5-paragraph OPORD format, based on the results of the first two steps. When completed, this plan will contain thorough pre-planned action sets to respond to discrete terrorist threats.

The Antiterrorism Force Protection Planning Template will help you manage Antiterrorism Force Protection at your installation. This template is still being refined. Therefore, your comments are welcome. The JCS J-34 Point of Contact, MAJ John Alexander, USA, can be reached at (DSN) 223-7561, (COM) 703-693-7561.

Using the Template

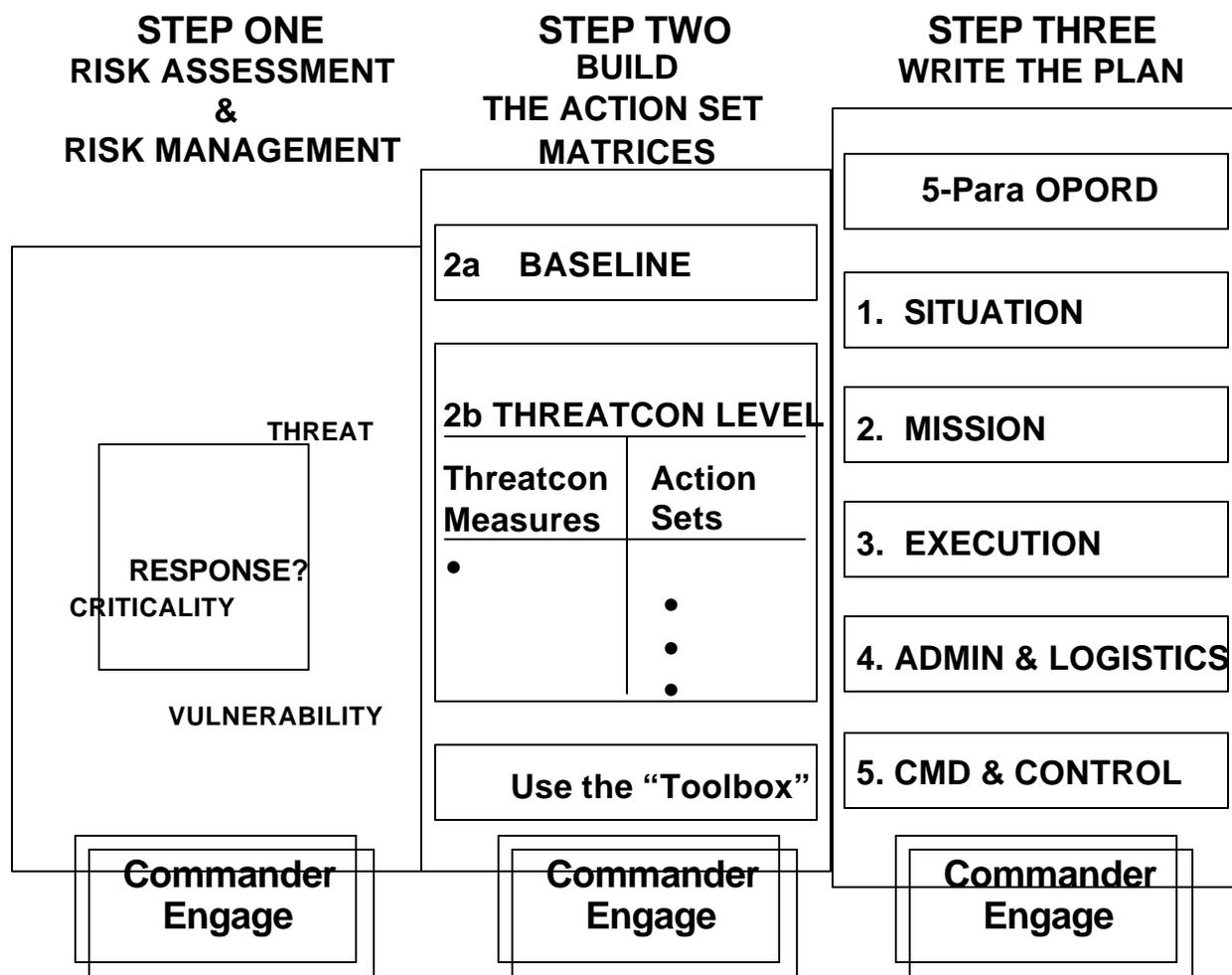
The Antiterrorism Force Protection Installation Planning Template (AT/FP Plan) is based on the standard five-paragraph operations order (OPORD) format. The installation's AT/FP Officer (required by DODI 0-2000.16, DOD Standard 23) and the installation commander will be the primary users of this planning tool. The AT/FP Plan can and should be used by all installation personnel, units, and facilities to ensure it is both understood and fully implemented.

To develop your Installation's AT/FP Plan, complete the following activities:

- Read DODI 0-2000.16.
- Review the User's Guide, the Master Template, & the Toolbox.
- Complete Step One, Risk Assessment & Risk Management (Use Annex A).
 - « Conduct a Threat Assessment.
 - « Develop an installation-specific Threat Level.
 - « Conduct a Criticality/Vulnerability (CV) Assessment.
 - « Develop a CV Assessment Table.
 - « Conduct an AT/FP Response Functions Assessment.
 - « Develop an AT/FP Response Functions Table.
 - « Develop a Risk Assessment *Area* Graph.
 - « Develop a Risk Assessment AT/FP *Function* Graph.
 - « Set aside these tools for use in Step Two.
- Complete Step Two, Build the Action Set Matrices (Use Annex C).
 - « Hold on to all of the tools from Step One.
 - « Baseline for THREATCON NORMAL, Annex B.
 - « (This may have been informally done prior to use of the template.)
 - « (Use the "Outside-In" Approach.)
 - « Develop the THREATCON Level Alpha-Delta Matrices.
 - « Apply each THREATCON Measure at each THREATCON Level.
 - « Develop Integrated Action Sets for each THREATCON Measure.
- Complete Step Three, Write the Plan.
 - « Use the Master Template to write OPORD paragraphs 1 & 2.
 - « Use the data developed in Step Two to write the Concept of Operations and complete the matrices in OPORD paragraph 3.
 - « Use the Master Template to write the remainder of paragraph 3.
 - « Return to the Master Template to write OPORD paragraphs 4 & 5.

The result of these activities should be a coherent, comprehensive AT/FP Installation Plan tailored to local conditions, which reflects the commander's operational approach on how to best address the threat and complete the installation's mission.

Building the AT/FP Installation Plan



USER'S GUIDE

Introduction

The responsibility for the protection of installation personnel, facilities, and other assets rests with you, the commander. This book is a user's guide to building a comprehensive Antiterrorism & Force Protection (AT/FP) Installation Plan—to help you successfully meet that responsibility. Although its length initially appears daunting, don't be discouraged; everything you, the commander, need is in the “blue-tabbed” section (Introduction, User's Guide, and the Master Template). The rest of this book, the “white-tabbed” section containing the annexes, supplements and supports the blue-tab information you need to know--and provides your staff with detailed information about how to assess your installation and develop your AT/FP Plan.

The book walks you and your staff through a three-step methodology, a “building block” approach, using a five-paragraph operations order (OPORD) format to write your plan.

Organization

The book is divided as follows:

- Introduction
 - « Introductory Letter
 - « Executive Summary -- “Using the Template”
 - « Methodology Graphic
- The User's Guide
 - « Introduction
 - « Organization
 - « Process: The Three-Step Methodology
 - « Risk Assessment & Risk Management
 - « Build the Action Set Matrices
 - « Write the Plan
- The Master Template
- Annexes
 - « A: Risk Assessment & Management
 - « B: THREATCON System
 - « C: Build the Action Set Matrices
 - « D: Toolbox
 - « E: References
 - « F: Glossary
 - « G: Acronyms

Prior to beginning the AT/FP planning process, the commander and staff should familiarize themselves with DODI 0-2000.16. The commander should read through the blue-tabs of this book. The installation staff should read through the blue-tabs in detail, and then familiarize themselves with the organization and general content of the white-tabs. Afterward, follow the three-step plan development method, using the book to assist you in completing the process. At the end, the installation will have the coherent, comprehensive AT/FP Installation Plan it requires.

The Process

Introduction to the Process. The three-step methodology in this book provides a walk-through for preparing to write and actually writing your AT/FP Plan. Step One allows you and your staff to develop risk assessments and to begin the risk management process upon which your

AT/FP Plan will be based. Step Two takes the process an additional stride forward by using the several tools developed in Step One to design AT/FP implementation guidance (integrated action sets). It also gives you a way to put these action sets in a context which is meaningful to you and which applies DOD guidance (THREATCON Levels & Measures). You will be able to ***plug these implementing action sets into a matrix and then insert the matrices directly into your plan's Concept of Operations*** when it is time to write the AT/FP Plan. The third step is then writing the plan, based on the preparatory work you completed in the first two steps. That plan will be in a five-paragraph OPOD format, immediately recognizable and functional for your installation.

Step One: Risk Assessment & Management.

Risk assessment is a logical, step-by-step method, but one which cuts across your staff lines (the intelligence staff prepares the threat assessment, the operations staff prepares the criticality assessment, the operations staff is joined by the provost marshal to determine vulnerability, and all staff elements become central to the response function assessment). At Step One, you should use four elements--threat, criticality, vulnerability, and response functions--to complete the initial risk assessment.

- Threat = capability & intent of the adversary to inflict injury to a person or damage to a facility or asset
- Criticality = both the term & the measure of importance to the installation's mission
- Vulnerability = susceptibility of a person, facility, or asset to a damaging incident
- Response functions = those activities which support the installation's ability to either deter or respond to terrorist threats and incidents.

As you will see, these tools are then used (in Step Two) in the continuation of the risk management function as you develop the Action Set Matrices.

The end product will be in the identification of areas and assets which are vulnerable to the identified terrorist threats and development of associated assessment tables. At the end of the risk assessment & risk management process the commander must engage and concur with the entire assessment in order to focus the next steps in risk management.

At the heart of the threat assessment are threat *intentions & capabilities*.

Step One-A: Conduct a Threat Assessment. The installation's intelligence staff will use all available intelligence support to prepare its first staff assessment, taking the form of a threat assessment. The intelligence staff should identify the current country-specific DOD Threat Level and the installation THREATCON Level. The threat assessment should explore the full range of probable and likely threats (groups and means), highlighting terrorist *intentions and capabilities*. This will be developed into a threat assessment for the installation. As all following steps hinge on this initial threat assessment, the staff must gain concurrence with the assessment from the commander.

(See Annex A, Risk Assessment & Management, for further details.)

Step One-B: Conduct an Area Criticality & Vulnerability (CV)

Area = fixed or mobile locations on an installation.

Assets = personnel, equipment, or stocks located on the facility, often within a defined area.

Assessment. The Area Assessment is conducted based on the *criticality* of the assets located within it and its *vulnerability* to specific threats. Although all of the installation's personnel are critical and their protection essential, not all of the installation's areas and assets are mission critical, but all must be considered when conducting the installation assessment. To build the CV Assessment Table:

- First, determine the *Area* to be examined. Label the Table with the Area ID.
- Second, determine the specific group or type of threats against which the area will be assessed. Place these in the left-hand column of the table.
- Third, examine and grade the Area for *Criticality* based on its three facets of Importance, Effect, and Recoverability. Use the scoring guidelines in Annex A. Enter that in the first three columns of the CV Assessment Table. (See Annex A for further details.)
- Fourth, examine & grade the Area for *Vulnerability* based on its three facets of Construction, Accessibility, and Recognizability. Use the scoring guidelines in Annex A. Enter that in the second three columns of the CV Assessment Table. (See Annex A for further details.)
- Fifth, total the six columns & place the table to the side.

Step One-C: Conduct an AT/FP Response Functions Assessment.

On your installation you have specific capabilities to either deter or respond to terrorist threats or incidents. We will call these capabilities "AT/FP Response Functions". (See Annex A for a list of Response Functions used by JSIVA Teams, provided as an example, or the WMD Appendix for installation specific Response Functions.)

To build the AT/FP Response Function Table:

- First, determine the AT/FP Function to be assessed. Label the Table with the Response Function ID.
- Second, determine the specific group or type of threats against which the area will be assessed. Place these in the left-hand column of the table.
- Third, examine and grade the function based on the *effectiveness facets* of Timeliness; Policy, Plans, and Procedures; Equipment; and Training.
- Fourth, total the four columns & place the table to the side.

Step One-D: Build a Risk Assessment Area Graph. This graph will portray the likelihood of an incident's occurrence and the severity of that incident. The Area Graph uses the CV numbers (produced at Step One-B). To complete the matrix:

- First, enter the CV number on the x-axis.
- Second, determine the likelihood of incident occurrence.
- Third, plot the result of these two considerations. Repeat this process until all CV pairs have been associated with the expected likelihood and then plotted. The staff then inserts the CV pairs according to *likelihood* and *severity*.
- You, the commander, make an operational decision on how much risk you are willing to accept. Determine your threshold for taking substantive deterrent, countermeasure, mitigation, or recovery actions. The staff then graphically portrays this threshold by establishing three

Risk level is based on Likelihood of an incident & Severity of an incident.

bands (Green, Yellow, Red—representing the risk from low to high) and placing those bands on the matrix.

- You now have a completed graph with CV pairs, which fall within the three bands. You will use this graph to develop implementation matrices at Step Two-C.

Step One-E: Build a Risk Assessment AT/FP Function Graph. This graph will also portray the likelihood of an incident’s occurrence and the severity of that incident, but will use the AT/FP Functions (produced at Step One-C) numbers instead of the CV numbers. To complete the matrix:

- First, enter the At/FP Functions number on the x-axis.
- Second, determine the likelihood of incident occurrence.
- Third, plot the result of these two considerations. Repeat this process until all AT/FP Response Function pairs have been associated with the expected likelihood and then plotted.
- Apply the same risk threshold bands that you used in Step One-D, insert the AT/FP Functions pairs according to likelihood and severity, and you will have completed a graph for AT/FP Functions which is the twin of the graph completed in the previous step. You will also use this graph to develop implementation matrices at Step Two-B.

At the conclusion of Step One, the commander should engage and concur with the results of the assessments. NOTE that Annex A has graphic representations of each of the tools mentioned throughout the Step One process.

That concludes the Step One process. With the risk assessment completed and several risk management tools in hand, the commander and staff can move forward into further management of the identified threat through development of Integrated Action Set Matrices.

Step Two: Build the Action Set Matrices. The goal of the AT/FP Installation Plan is to assign specific Action Sets (for each applicable THREATCON Measure at each THREATCON Level) which allow implementation of the plan as threat conditions change. To reach this goal, the commander must make an operational decision on how best to address the threat with the assets available. This establishes a baseline at THREATCON Normal and identifies the steps which must be taken at each successive THREATCON Level.

Step Two-A: Establish a Baseline.

(Note: Many commander’s will have already made baselining adjustments to the installation’s profile—additional lighting, additional fencing, improved access controls.—prior to completing the installation’s AT/FP Plan. Some may even do so with this template in hand. To complement these “adjustments”, you should use the formal structure of the template. The use of the template provides a formal, analytical structure which adds to those actions previously implemented.)

Helpful Hint:
Establishing the baseline will assist the staff when developing Action Sets for higher THREATCON Levels.

The installation must establish a baseline, representing an acceptable installation profile at THREATCON Normal. To accomplish this, the staff should evaluate the security posture of each *area and asset* and apply a simple system. This system describes an informal manner in which an

asset:

- meets the commander's AT/FP standards, requiring no improvements,
- is inadequate, needing improvement,
- is unsatisfactory, requiring improvement.

This should be done from the perimeter of the installation working to the center (See Annex C for the "Outside-in" Approach). It seeks to identify individual physical security elements that are not to standard. While informal, this simple adequate/inadequate/unsatisfactory designation provides the installation commander with an early "snapshot" of his installation. Use the snapshot to review the status of physical security elements at the installation, determine where fixes are required, and then apply resources to move the profile of these assets to an acceptable profile at THREATCON Normal. Recommend that the more formal approach contained in the template (the next step described) be used as well, as it ensures that a more rigorous method of approach to problem solving has been employed.

The commander should engage here because this step represents an opportunity to decide how to best address the threat and apply resources.

Step Two-B: Develop the Action Sets and Incorporate into Matrices.

Having established a satisfactory installation baseline profile, the installation must prepare for increases in threat or THREATCON Level. An area or asset meeting the standard at THREATCON Normal can easily become inadequate or unsatisfactory at a higher THREATCON Level. Using the CV Risk Assessment graph or the AT/FP Function Risk Assessment Graph (See Steps One-D and One-E), apply the DoD THREATCON Measures (See Annex B) and develop Integrated Action Sets. These action sets should provide simple, straight-forward implementation instructions for each Measure at each THREATCON Level. See Annex C for detailed information for developing the action sets; use the information, guidance, and tools in Annex D for further assistance. For each THREATCON Level, the staff will develop a matrix, outlining the appropriate THREATCON Measures and Integrated Action Sets. To complete this matrix:

- Label the matrix with the appropriate THREATCON Level (ALPHA-DELTA).
- In the matrix's left-hand column, list the applicable THREATCON Measures (plus additional Measures the commander identifies) which apply to the THREATCON Level.
- In the matrix's right-hand column, list the sets of actions required to fully implement each THREATCON Measure. Develop these action sets working from the outside of the installation inward. These Integrated Action Sets should describe exactly *how* the Measures will be applied, by answering the appropriate *who, what, where, when, why* questions. (See the graphic below for an example of a THREATCON Measure and its related Integrated Action Set.)
- Once you have developed an Integrated Action Set for each Measure at the selected THREATCON Level, move on to a new matrix for the next THREATCON Level and repeat the process until a matrix has been completed for each THREATCON Level.

- In addition to the Measures prescribed by DOD for a THREATCON Level, the commander should list any additional Measures including, those from a higher THREATCON Level, any new Measures, and/or RAM.

Identify shortfalls,
Prioritize solutions, &
Report shortfalls to HQ.

For areas where the installation has inadequate resources to provide an appropriate level of protection, the commander must notify the chain of command of shortfalls. These shortfalls represent the residual risk that cannot practically be reduced further or cannot be reduced given the resources available. IAW DODI 2000.12, the installation commander should identify any activity that does not meet the force protection standards to its cognizant chain of command, responsible Service, and the Chairman of the Joint Chiefs of Staff. In addition, the installation commander should submit a quarterly report listing these deficient activities to the Chairman of the Joint Chiefs of Staff and the responsible Service Secretary until the military activity in question is assessed as satisfactory.

THREATCON DELTA

Measure 46: Control access...	<ul style="list-style-type: none"> • Gate 1: <ul style="list-style-type: none"> • Barriers <ul style="list-style-type: none"> • G-4 provides 4 J-barriers, located at _____ • 1/11 EN Bn provides one heavy forklift to move barriers • 1/11 FA Bn uses 1 ELWB 5T truck to recover the barriers • PMO will direct placement of the barriers • Fences <ul style="list-style-type: none"> • 1/11 EN Bn provides 50M of concertina wire • 1/11 FA Bn installs 25M of concertina on each side of the access road • Lights <ul style="list-style-type: none"> • G-4 provides 4 lights with appropriate power source • 1/11 IN Bn recovers the lights & moves them to Gate 1 • PMO directs placement of the lights • Sensors N/A • Guard Force <ul style="list-style-type: none"> • PMO provides sufficient personnel to man Gate 1 with 3 guards 24/7 • HHC, Garrison provides ROE & other relevant training • PMO will issue weapons & ammunition • DOL, Garrison, will provide and place the portable guard shed and portable toilet at Gate 1 • HHC, Garrison provides rations • These actions will occur within three hours of change in THREATCON Level alert • Mission Essential Site 1 (Power Plant) • Mission essential Site 2 (Garrison HQ) • Mission Essential Site 3 (Garrison antenna farm) • Mission Essential Site 4 (Garrison Dining Facility) • Continue until all MEVAs have been planned
Measure 47:	Develop Actions Sets using the process above.
Measure "n"	

Step Three: Write the Plan. The final step places the critical information gathered in the preceding steps in the standard 5-paragraph OPORD format. While the data in the plan is largely consistent with standard OPORDs, pay careful attention to the tailoring of that information to fit the AT/FP requirements of the installation. The Master Template provides instructions in brackets to ensure each subparagraph is comprehensive. The text contained within the brackets of the Master Template is not for inclusion in your plan. Text outside the brackets is recommended language for that subparagraph. To write the plan:

- Complete OPORD paragraphs 1 (Situation) and 2 (Mission) using the instructions contained in the Master Template.
- Complete OPORD paragraph 3 (Execution). In addition to following the Master Template's instructions, the Concept of Operations subparagraph should contain the THREATCON Level matrices completed in Step Two (or refer the implementing units to an appropriate annex).
- Complete OPORD paragraphs 4 (Administration & Logistics) and 5 (Command and Signal), using the instructions contained in the Master Template.
- Develop supporting annexes required to complete the plan.
- Finally, the staff should ensure that the AT/FP Installation Plan adequately applies the commander's operational decision prior to implementation of the plan.

Use an:

Execution Matrix
to capture the AT/FP Plan's
Concept of Operations inputs.

Synchronization Matrix
to capture the WMD Appendix
Concept of Operations inputs.

NOTE: The Execution paragraph, subparagraph 3b, Concept of Operations, of the standard five-paragraph Operations order (OPORD), normally written as a series of clear, concise, phased mission statements; is directive; gives a specific date and time of execution; and is centralized in planning and decentralized in execution (Commander tells "what", not "how"). Most often concentrating on combat and supporting arms roles, the use of brief declaratory paragraphs is the norm. These listed attributes are somewhat different than those required in the AT/FP Plan (and the WMD Appendix). Therefore, we recommend a different manner of presentation to best capture the information needed to plan and execute the AT/FP Plan and its associated WMD Plan.

AT/FP planning, focused on installations, requires that staff directorates work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT/FP mission, and the unpredictability of its execution, requires that very specific "How To" instructions be provided, which sharply define when, where, and by whom specific AT/FP implementation measures must be conducted, and in what manner these actions must be coordinated. This level and manner of planning can be captured in an "execution matrix", as defined in Army FM 101-5. This type of execution matrix has been selected to best, most briefly and coherently, capture the complex data required to execute the AT/FP Plan. For that reason, we recommend that the format for the Concept of Operations sub-paragraph in the AT/FP Plan be in execution matrix format.

Further, the even more complex management of a WMD incident, and the unfamiliarity of the staff when working with the complex problems that an NBC event poses, indicates that a similar matrix format should be used in

the WMD Plan's Concept of Operations. A "synchronization matrix", also described in FM 101-5, is the best tool for our purpose here—because it clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a WMD incident. For that set of reasons, we recommend that the format for the Concept of Operations sub-paragraph in the WMD Plan be in synchronization matrix format.

We believe that this simple deviation from the traditional OPORD method of presenting data will provide you and your staff with a more clear, concise tool to conduct AT/FP operations.

ANTITERRORISM FORCE PROTECTION INSTALLATION PLANNING TEMPLATE

TASK ORGANIZATION: All installation personnel are responsible for developing a high state of readiness and responding to support this plan. [ENTER all organizations present for installation AT/FP defense either here or, if voluminous, in an annex. Include the AT/FP requirements of Host Nation (HN), United States (US), and other civilian organizations quartered within the installation. The commander should consider each unit's ability to assist in the AT/FP Installation Plan.]

NAME/LOCATION: [ENTER specific installation name, to include any short title or nicknames if they exist, and exact location of the installation (UTM/GPS coordinates).]

MAPS OR CHARTS: [ENTER a reference to all maps and charts that apply to the installation's AT/FP Plan. Consider including an engineer's grid map of the installation. This map can be used by the installation commander and his staff during the AT/FP planning and execution processes.]

TIME ZONE: [ENTER the time zone of the installation. Indicate the appropriate number of hours to calculate (plus/minus) ZULU time.]

REFERENCES: [ENTER either a compilation of DOD, joint, and service publications, or the selected reference list the installation develops, to include Memoranda of Agreement/Understanding (MOAs/MOUs), pertinent to this AT/FP Installation Plan.]

1. **SITUATION:**

a. General: This plan applies to all personnel assigned or attached to the installation. [DESCRIBE the political/military environment in sufficient detail for subordinate commanders, staffs, and units to understand their role in the installation AT/FP operations.]

b. Enemy Forces: The enemy is any adversary capable of threatening the installation's personnel, facilities, and equipment. [ENTER the general threat of terrorism to this installation including; the intentions and capabilities, identification, composition, disposition, location, and estimated strengths of hostile forces.]

c. Friendly Forces: [ENTER the installation's AT/FP posture and forces available, including the next higher headquarters and adjacent installations. Include information on any units not under installation command required to assist in AT/FP planning and execution. These units may include HN and US military police forces, fire support, special operations forces, engineers, nuclear biological and chemical (NBC) decontamination or smoke units, and explosive ordnance disposal (EOD).]

d. Attachments & Detachments: [DEVELOP a process for identifying and tracking individuals/units at the installation. ENTER this process and identify the person(s), staff, or unit responsible. Also ENTER the attached or detached units. Incorporate any reserve units, which are mustering and/or training at the installation. Do not repeat information already listed under Task Organization.]

e. Assumptions: [ENTER all critical assumptions used as a basis for this plan. Assumptions are those factors that are unlikely to change during the implementation of the AT/FP Installation Plan. They may range from troop strength on base to the major political/social environment in the surrounding area. Examples follow:

- (1) The installation is vulnerable to theft, pilferage, sabotage, and other threats.

(2) The owner and/or principal user of a resource, personnel, or facility should develop AT/FP protection procedures for both normal and contingency operations.

(3) Terrorist activity should be considered for contingency purposes. Absolute protection against terrorist activities is not possible. Therefore this AT/FP Installation Plan provides overarching guidance and procedures, which balance mission requirements, available manpower, and fiscal resources, and the degree of protection required based on the current threat.

(4) Security personnel, both military and civilian, may be insufficient to provide total protection of all installation resources; therefore, the principal owner or user of a facility, resource, or personnel must develop adequate unit awareness and safeguard measures.

(5) Local, non-military response forces will arrive within [time] of notification.]

f. Intelligence: [ENTER the person, staff, or unit responsible for intelligence collection and dissemination. The installation commander must have a system in place to access current intelligence. National level agencies, CINCs, and intelligence systems provide theater or country threat levels and threat assessments. These assessments serve as a baseline, so the installation commander can develop a threat assessment tailored to the installation. The installation's tailored threat assessment should be continuously evaluated, updated, and disseminated, as appropriate, and as directed by the installation commander. The commander should determine the frequency and the means of dissemination of the installation's tailored AT/FP product. Note: The OCONUS commander cannot change the threat level, which is developed at the national-level; the CONUS installation will obtain current intelligence and develop its own threat level, using the threat assessment methodology. The installation can and should tailor the local threat assessment for the installation.]

2. MISSION/PURPOSE: [ENTER a clear, concise statement of the command's mission and the AT/FP purpose or goal statement supporting the mission. The primary purpose of the AT/FP Installation Plan is to safeguard personnel, property, and resources during normal operations. It is also designed: to deter a terrorist threat; to enhance security and AT/FP awareness; and to assign AT/FP responsibilities for all installation personnel. DODD 2000.12 states that it is "DOD policy to protect DOD personnel and their families, facilities, and other materiel resources from terrorist acts." In meeting this goal, the installation should meet the following four objectives:

a. Deter terrorist incidents: Installation commanders will dissuade terrorists from targeting, planning against, or attacking U.S. DOD assets by communicating US intent and resolve to defeat terrorism.

b. Employ countermeasures: Installation commanders will employ the appropriate mix of countermeasures, both active and passive, to prevent terrorists from attacking U.S. DOD assets.

c. Mitigate the effects of a terrorist incident: Installation commanders will employ the full range of active and passive measures to lessen the impact of terrorist events against DOD assets.

d. Recover from a terrorist incident: Installation commanders will design plans to recover from the effects of a terrorist incident. [Note: Terrorist use of Weapons of Mass Destruction (WMD) represents a central and potentially overwhelming task for the installation. WMD-specific planning considerations are published as a separate Appendix to this AT/FP Plan.]

3. EXECUTION:

a. Commander's Intent: [ENTER how the commander envisions the development, implementation of the AT/FP Installation Plan, and the establishment of overall command priorities.]

b. Concept of Operations: [ENTER how the overall AT/FP operation should progress. This plan stresses deterrence of terrorist incidents through preventive measures common to all combatant commands and Services. During day-to-day operations, the installation should stress continuous AT/FP planning and passive, defensive operations. This paragraph should provide subordinates sufficient guidance to act upon if contact or communications with the installation chain of command is lost or disrupted. The installation's AT/FP Concept of Operations should be phased in relation to pre-incident actions and post-incident actions. AT/FP planning and execution requires that staff elements work with a much greater degree of cohesiveness and unity of mission than that required during the conduct of normal base sustainment operations. The AT/FP mission, and the unpredictability of its execution, requires very specific "How To" implementation instructions of DoD THREATCON Measures and in what manner these actions must be coordinated. This "How To" element is not included in the normal Concept of Operations paragraph. The necessity to provide "How To" guidance in the AT/FP Plan requires a different manner of data presentation to ensure brevity and clarity. Commanders and planners can display this information graphically in an "execution matrix". As stated in the User's Guide, recommend that this subparagraph be in execution matrix format, as it best captures the complex data required to execute the AT/FP Plan. (The WMD Plan's Concept of Operations reflects a similar matrix format -- a "synchronization matrix" -- which clearly describes relationships between activities, units, supporting functions, and key events which must be carefully synchronized to minimize loss of life and to contain the effects of a WMD incident.) Therefore, the heart of the Concept of Operations subparagraph and the AT/FP Plan will be the THREATCON Level matrices, which represent the culminating step of the methodology described immediately below. Specific instructions are listed in the applicable annexes.]

- Conduct Risk Assessment/Risk Management (Annex A), integrating the
 - Results of the Threat Assessment,
 - Results of the Criticality/Vulnerability (CV) Assessment
- Results of the Risk Assessment Area Graph
- Results of the Risk Assessment AT/FP Response Function Graph
- Baseline the Installation at THREATCON NORMAL, using "Outside-In" Approach (Annex C) and applicable tools from Annex D
- Be prepared to respond to increased THREATCON Levels
- Develop specific action sets to implement each THREATCON Measure at increased THREATCON Levels (Annex C)
- Develop an Action Set Matrix (Annex C)
- Incorporate the matrix into the AT/FP Plan
- Implement AT/FP THREATCON Measures, as appropriate

c. Tasks and Responsibilities of Key Elements: [ENTER the specific tasks for each subordinate unit or element listed in the Task Organization paragraph. Key members of the installation have responsibilities that are AT/FP specific. The commander should ensure that a specific individual/unit/element within the installation is responsible for each action identified in this plan. Each individual/unit/element must know the AT/FP tasks and responsibilities, what these responsibilities entail, and how these will be implemented. Further information and a sample format are located at Appendix 1, Annex D.]

d. Jurisdiction: [ENTER the jurisdictional limits of the installation's commander and key staff . Although the Department of Justice, Federal Bureau of Investigation (FBI), has primary law enforcement responsibility for terrorist incidents in the United States, the installation commander is responsible for maintaining law and order on the installation. For OCONUS incidents, the installation commander must notify the HN and the geographic combatant commander; the geographic combatant commander will notify the Department of State (DOS). The installation should establish HN agreements to address the use of installation security forces, other military forces, and host-nation resources that clearly delineate jurisdictional limits. There may be exceptions due to the wide dispersal of work and housing areas, utilities, and other installation support mechanisms which may require the installation to be responsible for certain areas outside of the installation perimeter.]

e. Coordinating Instructions: [This paragraph should include AT/FP specific coordinating instructions and subparagraphs, as the Commander deems appropriate. In addition, this section of the AT/FP Plan outlines aspects of the installation's AT/FP posture which require particular attention to guarantee the most effective and efficient implementation of the AT/FP Plan. For the purposes of this plan, there are three types of coordinating instructions: 1) Procedural; 2) Implementation Responsibilities; and 3) Special Installation Areas. The sections listed below are representative, and may not be all-inclusive. Installation Planners should use these coordinating instructions and corresponding tools (Toolbox, Annex D) for baselining the installation and for developing the action set matrices for each THREATCON Level.]

(1) Procedural:

a Alert Notification Procedures: [ENTER the person, staff, or unit responsible for establishing the proper notification systems and procedures. Refer to Appendix 2, Annex D. ENTER a description of the alert notification procedures here. Include alert rosters for all units/organizations on the installation. Note: Establish procedures for notifying not only the appropriate staff elements, the crisis management team, and responding forces, but also the installation's units, service personnel, and other installation occupants of an impending or actual situation.]

b Rules of Engagement for the Application of Force: [ENTER the standing operating procedures for use of deadly force. (This may include information on minimum standards for weapons qualification prior to issue of a weapon.) Note: Establish the procedures for use of force, and educate and train on-site security elements and the auxiliary force in these procedures. When force is used, apply only the minimum force necessary to effectively control the situation. Applying force in degrees ensures deadly force will not be used inadvertently. Ensure that installation personnel are aware of the degrees of force and by whose authority each degree of force is applied.]

c Installation AT/FP Exercises: [ENTER the appropriate means and frequency to exercise this AT/FP Plan. Note: Terrorist use of WMD is an exercise and planning area that merits special inclusion. DODI O-2000.16, Standard 16 requires that AT/FP be folded into exercise planning. Standards 31, 32, and 33 give further guidance as they pertain to WMD. Further information is located at Appendix 3, Annex D.]

d Incident Response: [ENTER the several plans that will be activated upon initiation of the incident (assassination, assault, hostage and barricade, hijacking, kidnapping, bombing, civil disorder, WMD (See Appendix 14), and information operations). Note: Each case may require a different series of forces to successfully respond to and conclude the incident. DODI O-2000.16, Standards 27, 28, & 29 give further guidance in this area. Establish mechanisms to respond to a variety of terrorist incidents and integrate them into the AT/FP Installation Plan. Describe the interaction with local authorities which use MOAs and MOUs. Further information is located at Appendix 4, Annex D.]

e Consequence Management: [ENTER information on how the installation will handle the consequences of a terrorist incident. This section does not apply only to WMD, but to other terrorist incidents, as well. This section should include references to coordination with the PAO, medical, and mortuary affairs. Describe the interaction with local authorities which use MOAs/MOUs. Further information is located at Appendix 5, Annex D.]

f Executive or Distinguished Visitor Protection Procedures: [ENTER the person or staff with overall responsibility for protection procedures. This person or staff will identify the forces available for executive or distinguished visitor protection. This plan should facilitate the coordination with the visitor's security office or protective/security detail. DODI O-2000.16, Standard 30 gives specific guidance in this area. High risk personnel are covered in Standard 26. Further information is located at Appendix 6, Annex D.]

(2) Security Posture Responsibilities

a Operations Security (OPSEC): [ENTER the person, staff element or unit responsible for installation OPSEC. That person, staff, or unit should produce the criticality and vulnerability reports. The commander will use these reports to enhance the installation's AT/FP posture, design countermeasures, incident response, and post incident planning. Further information is located at Appendix 7, Annex D.]

b Access Controls: [ENTER the person(s), staff(s) or unit(s) responsible for pedestrian, vehicular, and package/mail access onto the installation. DESCRIBE the installation's access control system. Note: An installation's access control system may include several discrete systems (i.e., perimeter, key facilities, SCIFs). Coordinate all elements in the access control plan with other security measures. Further information is located at Appendix 8, Annex D.]

c Barriers: [ENTER the person, staff or unit responsible for planning barriers for the AT/FP Installation Plan. Note: This person, staff, or unit is responsible for ensuring that barrier planning is included in the THREATCON Level matrices' Integrated Action Sets. Further information is located at Appendix 9, Annex D.]

d Lighting: [ENTER the person, staff, or unit responsible for the lighting plan. Note: This person, staff, or unit is responsible for ensuring that lighting planning, which augments existing fixed lighting, is included in the THREATCON Level matrices' Integrated Action Sets. Further information are located at Appendix 10, Annex D.]

e On-Site Security Elements: [ENTER the person or staff with overall responsibility for installation security. LIST the military and civilian security force that is specifically organized, trained, and equipped to provide the physical security and law enforcement for the command. Further information is located at Appendix 11, Annex D.]

f Technology: [ENTER the person, staff, or unit to identify emerging technologies, which could enhance the overall protection of the installation. Note: Emerging technologies are particularly important to the terrorist WMD threat. Further information is located at Appendix 12, Annex D.]

g Training: [ENTER the person, staff, or unit responsible for preparation and execution of individual security training. Establish an effective security education/training program for the entire installation (which includes required actions to different threat alarms and specific training for civilian personnel, contractors, family members and tenant units). Note: Training areas of interest are further highlighted and guidance offered in DODI O-2000.16, Standard 24 & 26. Further information is located at Appendix 13, Annex D.]

(3) Threat Specific Responsibilities

a Weapons of Mass Destruction: [The threat of terrorist attack poses different and in some cases more difficult challenges. ENTER a special task-organized staff or unit to plan for a WMD attack against the installation. Note: The responsible staff or unit should build the WMD plan with checklists, and develop tools appropriate to the installation. DODI O-2000.16, Standards 31, 32, & 33 offer further guidance in this critical area of interest. Further information is located at Appendix 14, Annex D. The WMD Planning Template, Appendix 14, is published as an adjunct to this AT/FP Installation Planning Template.]

b Information Operations: [Terrorists may choose to strike at an informational source to terrorize an installation or DOD asset. ENTER the person, staff, or unit responsible for information operations. Note: The responsible planner should develop a plan for safeguarding of information and integrate this plan into the overall AT/FP plan. Further information is located at Appendix 15, Annex D.]

(4) Special Installation Areas:

a Airfield Security: [ENTER the person, staff, or unit responsible for airfield security. ENTER the airfield security plan here (or include as an annex) as part of the overall AT/FP plan. Further information is located at Appendix 16, Annex D.]

b Port Security: [ENTER the person, staff, or unit responsible for port security. DESCRIBE the port security plan here (or include as an annex) as part of the overall AT/FP Plan. Further information is located at Appendix 17, Annex D.]

c Buildings: [ENTER a person, staff, or unit to review each building on the installation in accordance with the installation's criticality/vulnerability assessments. Note: The responsible person, staff, or unit should develop a plan, series of checklists, or other tools to bring the installation to a level of AT/FP protection consistent with the installation's THREATCON Level. Further information is located at Appendix 18, Annex D.]

4. **LOGISTICS & ADMINISTRATION:** [ENTER the logistics and administrative requirements to support the AT/FP Installation Plan, which should include enough information to make clear the basic concept for planned logistics support. Specific logistics and administrative requirements will emerge throughout the planning process outlined in the Concept of Operations, specifically when developing the action sets. These requirements should be incorporated into this paragraph. Note: Each installation will require a review of its mission and threat to provide information in sufficient detail. When applicable, it should refer to appropriate annexes.]

a. Readiness & Concept of Combat Service Support: [ENTER service support instructions and arrangements pertinent to the AT/FP Plan. If the arrangements are lengthy, include in an annex or separate Administrative and Logistics Order. Note: Organizations tasked throughout this plan to provide logistics support during increased THREATCON Levels should ensure they constantly maintain the capability to do so. In the event any specific requirement cannot be met for any reason, the unit commander responsible for the activity in question must notify the AT/FP Planner to reallocate resources.]

b. Material and Services: [ENTER supply, maintenance, transportation, construction, and allocation of labor which apply to AT/FP efforts prior to a terrorist incident. Note: Significant actions and support must take place in the post-incident response phase. Specifics should be here or included in the WMD and Consequence Management Appendices.]

c. Weapons and Ammunition: [ENTER the weapons and basic ammunition allowances required to support the AT/FP augmented security forces. Note: Planners should identify the location, authority for issue, and basic level of issue. Planners should determine whether a pre-determined allocation of ammunition exists, where the allocation of ammunition is stored, who has access to the ammunition, and whether the AT/FP package contains explosives.]

d. Medical Services: [ENTER plans, policies, and HN/local agreements for AT/FP treatment, hospitalization, and evacuation of personnel, both military and civilian. Note: Planners should include aerial medical evacuation support, the nearest trauma center, the ability to set up a crisis center, WMD response capability, and ability to support a mobile medical hospital.]

e. Personnel: [ENTER procedures for strength reporting, replacements, and other procedures pertinent to base defense, including handling civilians and prisoners of war. ENTER instructions for submitting status reports.]

f. Civil Affairs: [ENTER the person, staff, or unit responsible for coordinating and interfacing with the local population to provide assistance for civilian needs in the event of casualties. Note: Planners should also develop community relations to support the installation's needs or requirements during a time of crisis.]

g. Updates to this AT/FP Installation Plan: [ENTER the appropriate person, staff, or unit responsible for developing a process for updating the installation plan (derived from this template) and for the distribution of those updates.]

5. COMMAND & SIGNAL: [ENTER instructions for command and operation of communications-electronics equipment. Highlight any deviation from that chain of command that must occur as a result of a terrorist incident. Command includes subordinate and higher unit command post and emergency operations center locations and designated alternate command posts. The chain of command may change based on the deployment of a Joint Task Force or an National Command Authority-directed mission.]

a. Command: [ENTER command relationships to include command succession. Note: The installation commander must ensure that the key AT/FP staff members understand the differences inherent in the installation's incident response command structure, with special consideration to the location of the installation (CONUS/OCONUS). Whether these operations occur CONUS or OCONUS, the relationships should be represented in the plan to reflect the agreements between supporting government agencies or HN. These relationships may be presented in a chart as an annex to this installation plan. This is an excellent tool to formulate the alert notification procedures (to be placed in the front of the AT/FP Plan) and paragraph 3c, Task and Responsibilities. Also note that the command, control, and reporting responsibilities for foreign terrorist attacks on DoD property or personnel belong to the geographic combatant commander within whose AOR the attack has occurred. For assets under the control of a functional combatant commander, the functional combatant commander will coordinate with the affected geographic combatant commander for an appropriate division of responsibilities. The installation commander should ensure proper reporting procedures are in place with higher headquarters.]

b. Signal: [Communications for AT/FP contingency operations will be the normal base communications augmented by portable radio, landlines, courier, and runners, and will be IAW OPSEC and COMSEC requirements. ENTER information on requirements for additional equipment (computers, hand held radios), its type, and its dissemination; pertinent communications nets; operating frequencies; codes and code words; recognition and identification procedures; type of alarms and required responses; and electronic emission constraints.]

ANNEX A: Risk Assessment and Management

ANNEX B: THREATCON System

ANNEX C: Building the Action Sets

ANNEX D: Toolbox

ANNEX E: References

ANNEX F: Glossary

Annex A: Risk Assessment and Management

1. Introduction.

Given the resource-constrained environment in which installations now operate, installation commanders require a method to assist them in making resource allocation decisions designed to protect the installation from possible terrorist threats. The Risk Management process allows installation commanders to use risk as one of the principal factors in their decision-making process. **Risk** is the probability that an incident will produce harm or damage under specified conditions, and combines two factors:

- the likelihood that a terrorist incident will occur; and
- the consequences of the terrorist incident.

By using Risk Management as a decision-making tool, installation commanders will be able to address threats to their installation that are the most likely and that will have the most severe implications. The following methodology provides a basic framework for structuring this risk management in a manner which is both comprehensive and tailored to the installation's unique situation and environment.

2. The First Step: Risk Assessment.

The first step in Risk Management is to conduct a Risk Assessment. The Risk Assessment process allows the installation commander to obtain a clear picture of the installation's current AT/FP posture and identify those aspects on the installation which need improvement. During the Risk Assessment, important information is also collected which can be used when writing the overall AT/FP Installation Plan.

The Risk Assessment process analyzes four elements:

- 1) the terrorist threat to the installation;
- 2) the criticality of the assets located on the installation;
- 3) the vulnerability of different areas of an installation to terrorist threats; and
- 4) the installation's ability to conduct activities to deter terrorist incidents, employ countermeasures, mitigate the effects of a terrorist incident, and recover from a terrorist incident.

During the Risk Assessment process, all of these elements must be considered for an Installation Commander to make a well-informed decision.

The process outlined in this annex does not discuss *how* the assessment is conducted or *how* to identify deficiencies and vulnerabilities, but outlines what type of information must be collected and how that information is organized and displayed for decision making. If the installation does not have the resident expertise to conduct an AT/FP Risk Assessment, consider using the reports prepared by a Joint Staff Integrated Vulnerability Assessment (JSIVA), CINC or Service AT/FP assessment. Vulnerabilities and deficiencies gathered from these useful tools can be plugged directly into the methodology outlined in this manual.

Risk Assessment: The Threat Assessment Element.

An Installation's Threat Assessment process examines intelligence information and products to examine possible terrorist activity, and, in turn, determine the *intentions*, *capabilities*, and likelihood of different types of terrorist incidents. Terrorist threat analysis is a continual process of compiling and examining all available information in order to identify terrorist targeting of US interests. DOD has established a methodology to assess the terrorist threat to DOD personnel and their families, facilities, material, and interests which examines six factors:

- **Existence.** A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.
- **Capability.** The acquired, assessed, or demonstrated level of capability for a terrorist group to

- conduct attacks.
- **Intentions.** Demonstrated, anti-US terrorist activity, or states an assessed desire to conduct such activity.
- **History.** Demonstrated terrorist activity over time.
- **Targeting.** Current, credible information on activities indicative of preparations for specific terrorist operations.
- **Security Environment.** The internal, political and security considerations that impact on the capability of terrorist elements to carry out their intentions.

The Director of the Defense Intelligence Agency (DIA) is responsible for prompt dissemination of intelligence information on terrorist threats, including specific warning of threats against DOD personnel and their family members, facilities and other material resources, in accordance with DOD Directive 5240.1 and DOD Directive 5240.6. For more information on specific information requirements for terrorist threat analysis, see Joint Pub 3-07.2.

On OCONUS installations, the DIA uses this information to set the DOD general terrorism **Threat Level**, indicating the potential risks to US personnel in a particular country. The Geographic CINCs may also raise the terrorism Threat Level in countries within the CINC's area of responsibility. DIA does not issue a Threat Level for CONUS installations; therefore, the installation must assess the terrorist threat by querying its intelligence system, local law enforcement, and federal agencies to determine its Threat Level. Table 1 provides some basic guidelines for determining the Threat Level based on the six analysis factors. Specific Threat Level information and guidance can be found in DOD 0-2000.12-H, Chapter 5, pages 5-4 and 5-16.

Level	Existence	Capability	Intentions	History	Targeting*	Security Environ.
Negligible	May be present	May be present				
Low	Must be present	Must be present		May be present		
Medium	Must be present	Must be present	May be present	Must be present		
High	Must be present	Must be present	Must be present	Must be present	May be present	
Critical**	Must be present	Must be present	Must be present	May be present	Must be present	

Table 1. Threat Level Development.

*Specific target information is not generally available to analysts.

**This threat level is the only level where specific targeting information is present. Installation commanders must take appropriate protective measures at this level.

In addition to establishing the Threat Level, intelligence information is also used to identify specific terrorist threats against assets located on the installation. It is these specific threats and the likelihood of materialization of those threats that are used when assessing the installation's areas and AT/FP functions. Prior to this assessment, the Installation Commander must decide which threats the installation is going to be assessed against. Although based on current intelligence estimates of the terrorist threat in the region, this decision should also consider threats that fall outside the current threat assessment because the effects of that type of terrorist incident would be devastating. For example, even though nuclear, biological and chemical (NBC) threats may not have surfaced during the Threat Assessment, the installation should consider these threats. (For more information, see WMD Appendix #14 of this AT/FP Installation Planning Template.)

During the Threat Assessment, it may also be useful to link identified threats to a *specific time*

period or location. For example, a terrorist group operating in the proximity of the installation may typically target areas which contain a large number of dependents, such as schools or the commissary. With this knowledge, the vulnerability assessment team should pay close attention to vulnerabilities in these areas.

Risk Assessment: Introduction to the Area Assessment and AT/FP Functions Element.

The center of the Risk Assessment process is the examination of all the physical areas and AT/FP Functions on an installation. **Areas** are defined as fixed or mobile locations on an installation (i.e. buildings, recreation areas, or transportation systems). **Assets** are defined as personnel, equipment, or stocks physically located on the installation at any given time. This is an important distinction. For example, an **area** is the headquarters building, while the **assets** are the personnel and equipment that are inside the building. When looking at areas, the assessment team will rate the criticality of assets located in the area and the vulnerability of the area to specific threats.

AT/FP Functions are those activities which contribute to the installation's ability to deter, employ countermeasures, mitigate, and recover from a terrorist incident. When looking at AT/FP Functions, the assessment team will rate the installation's effectiveness in performing these activities.

Risk Assessment: The Area Assessment Element.

There are many different types of areas on an installation. Because AT/FP deals with protecting *all* assets on an installation, it is important not to exclude some areas because they are not necessarily mission essential. The following is a list of different types of areas that may be located on an installation¹:

- Operations buildings;
- Administration buildings;
- Medical facilities;
- Food service (dining facilities, Officer/NCO Club, fast food);
- Shopping (exchange, commissary);
- Lodging (barracks, housing areas, apartments, guest housing);
- Recreation (athletic fields, theaters);
- Religious/Education (church, school);
- Transportation (parking lots, bus system, air fields, ports, motor pool);
- Utilities / substations.

Prior to conducting this portion of the Risk Assessment, the Installation Commander should determine the group or the type of terrorist threats to which the assessment process will be applied.

An Area is assessed in terms of the *criticality* of the assets located within it and its *vulnerability* to specific threats.

- **Criticality** can be divided into three facets: 1) Importance; 2) Effect; and 3) Recoverability. For each type of threat, the installation assessment team will give each area a rating for each of these facets.

- **Vulnerability** can be divided into three facets: 1) Construction; 2) Accessibility; and 3) Recognizability. For each type of threat, the installation assessment team will give each area a rating for each of these facets.

You may want to record these values in a table created for each area. After you have completed assigning the values for each threat, total the values across the table in order to determine the Criticality/Vulnerability (CV) rating for each pair of areas and threats (see Table 2). For example, in the sample table below the CV rating for Car Bombs and the Commissary is 51. This value will be used during Risk Management to measure the severity of an incident occurring at that area.

AREA: *Commissary*

¹ These are the areas on an installation that the JSIVA teams examine during their assessment, focusing on areas which have high population concentrations. The installation can assure parallel vulnerability assessment effort by assessing the same areas used by the DoD-level vulnerability assessment teams.

Threats	Importance	Effect	Recoverability	Construction	Accessibility	Recognizability	Total (CV)
Car Bomb	9	9	9	9	8	7	51
CW	5	8	8	4	5	4	34
BW	9	8	9	9	7	5	47
Letter Bomb	3	2	3	3	3	5	19

Table 2. Example Criticality/Vulnerability Assessment

The following are the definitions for the three facets of both criticality and vulnerability and the criteria by which they are rated. It is important to note that this rating system is not meant to be a precise science. It is one method of quantifying a subjective decision in order to generally prioritize areas in terms of criticality and vulnerability.²

Importance: Importance measures the value of assets located in the area, considering their function, inherent nature, and monetary value. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major importance	9-10
Significant importance	7-8
Moderate importance	5-6
Minor importance	3-4
Negligible importance	1-2

Effect: Effect measures the ramifications of a terrorist incident in the area, considering the psychological, economic, sociological, and military impacts. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major impact	9-10
Significant impact	7-8
Moderate impact	5-6
Minor impact	3-4
Negligible impact	1-2

Recoverability: Recoverability measures the time it takes for the function occurring at that area to be restored, considering the availability of resources, parts, expertise and manpower, and redundancies. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major amount of time	9-10
Significant amount of time	7-8
Moderate amount of time	5-6
Minimum amount of time	3-4
Negligible amount of time	1-2

² ***The assessment process included in this annex has been specifically designed for AT/FP assessment and planning.*** Other DOD processes, such as MEVA and CARVER, offer similar types of subjective assessments but are not specifically tailored for force protection assessments. While the MEVA and CARVER processes have been included as additional, optional tools in Annex D, Appendix 18 (Buildings), for those who are familiar with their use--both have design limitations, and are *best used only as an adjunct* to the risk assessment & management methodology contained in this annex.

Construction: Construction measures the degree to which the area protects the assets within it from the effects of a terrorist incident. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major vulnerability	9-10
Significant vulnerability	7-8
Moderate vulnerability	5-6
Minor vulnerability	3-4
Negligible vulnerability	1-2

Accessibility: Accessibility is measured in terms of the relative ease or difficulty of movement for terrorist elements and the likelihood of detection. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major vulnerability	9-10
Significant vulnerability	7-8
Moderate vulnerability	5-6
Minor vulnerability	3-4
Negligible vulnerability	1-2

Recognizability: Recognizability measures the degree to which a terrorist can determine the function and importance of an area and/or the assets located within it. Use the scale below to determine the numeric value assigned to a particular area.

Criteria	Value Scale
Major vulnerability	9-10
Significant vulnerability	7-8
Moderate vulnerability	5-6
Minor vulnerability	3-4
Negligible vulnerability	1-2

Risk Assessment: The AT/FP Functions Assessment Element.

On all installations specific activities exist, which support the installation’s ability to either deter or respond to terrorist threats and incidents. These functions can be broken down or “re-boxed” to whatever level of detail deemed necessary. The following, however, are the AT/FP Functions which JSIVA teams examine during their installation assessment³:

Intelligence Process: How the installation at all levels deals with the intelligence process (i.e., planning/direction, collection, processing, and dissemination). Includes how the installation responds to threats with appropriate use of THREATCONS.

Installation AT/FP Plan and Programs: The overall AT/FP posture of the installation, including AT/FP and emergency response plans, exercises, personnel awareness and training.

Installation Perimeter Access: The installation’s ability to secure the perimeter against and control the access of a terrorist threat, including:

- high speed approach;

³ The areas listed here, when used in an overall vulnerability assessment, will assure parallel effort between the installation’s and DOD-level assessment teams. As an example of a modified “Re-boxing” and breakdown of functions, See the WMD Appendix to this Planning Template.

- observable existing guard force;
- vehicle searches;
- procedures/guidelines for observing and reporting suspicious activity; and
- barrier weaknesses, lighting, and placement of gates.

Security System Technology: The technology components of the installation security system including:

- the alarm system;
- data transmission media, and interior/exterior sensors;
- access points;
- CCTV coverage;
- detection systems.

Medical: The availability and capability of installation medical support in response to a terrorist incident.

Fire Protection: The overall fire protection system of an installation, including:

- fire department availability and capabilities;
- building design and construction;
- automatic fire suppression systems;
- extinguishers and hoses; and
- alarm sensors and training.

Executive/Personnel Protection: Protecting VIPs and high visibility personnel on an installation including office locations, home, parking spaces/markings and car markings, and routes to and from work.

Security Forces: Military police/security/response force performance including their contribution to deterrence, detection, delay and response to terrorist activity including activity with local police and response agencies.

Communication Systems: The installation-wide system for exchanging information about a terrorist threat or incident (i.e., dedicated alert system).

Incident Response and Recovery: The installation's ability to mitigate the effects and recover from a terrorist incident and resume normal operations (i.e., decontamination, mass care).

Mail Handling Systems: The installation's ability to secure, handle, and inspect incoming mail for possible terrorist threats.

AT/FP Functions are assessed in terms of how effective the installation performs activities related to addressing the terrorist threat. **Effectiveness** can be divided into four facets: 1) Manpower; 2) Policy/Procedures/Plans; 3) Equipment; and 4) Training/Exercising. For each threat group/type, give each AT/FP Function a rating for each of the four facets.

As with assessing Areas, you may want to record these values in a table created for each function. After you have completed assigning the values for each threat, total the values across the table in order to determine the overall Effectiveness rating for each pair of functions and threats (see Table 3). For example, in the sample table below, the Effectiveness rating for Car bombs and Installation Perimeter Access is 41. This value will be used during Risk Management to measure the severity of an incident.

AT/FP Function: <i>Installation Perimeter Access</i>					
Threat	Timeliness	Policy/ Plans/ Procedures	Equipment	Training	Total
Car Bomb	7	8	6	9	41
CW	7	9	8	9	44
BW	7	5	3	6	30
Letter Bomb	7	10	7	9	46

Table 3. Example Response Function Table

The following are the definitions for the four facets of effectiveness and the criteria by which they are rated. As with the rating system used when assessing Areas, these values provide a general, subjective understanding of how effective the installation can perform the given function and are not an exact measure of performance.

Manpower: This facet measures the existence of an appropriate level of manpower to effectively perform the function. Use the scale below to determine the numeric value assigned to a particular function.

Criteria	Value Scale
Major deficiency	9-10
Significant deficiency	7-8
Moderate deficiency	5-6
Minor deficiency	3-4
Negligible deficiency	1-2

Policy/Procedures/Plans: This facet measures the presence of effective plans, MOAs/MOUs and other agreements, as well as procedures for effectively performing the function. Use the scale below to determine the numeric value assigned to a particular function.

Criteria	Value Scale
Major deficiency	9-10
Significant deficiency	7-8
Moderate deficiency	5-6
Minor deficiency	3-4
Negligible deficiency	1-2

Equipment: This facet examines and measures the adequacy of equipment used to perform the function. Consider whether the equipment is working properly, maintained properly, if there is a sufficient amount of equipment or if the equipment is obsolete. Use the scale below to determine the numeric value assigned to a particular function.

Criteria	Value Scale
Major deficiency	9-10
Significant deficiency	7-8
Moderate deficiency	5-6
Minor deficiency	3-4
Negligible deficiency	1-2

Training / Exercising: This facet examines and then measures if the installation's personnel are properly trained to perform the function. Use the scale below to determine the numeric value assigned to a particular function.

Criteria	Value Scale
Major deficiency	9-10
Significant deficiency	7-8
Moderate deficiency	5-6
Minor deficiency	3-4
Negligible deficiency	1-2

3. The Second Step: Risk Management.

Risk Management is the process of identifying, evaluating, selecting, and implementing actions to reduce risk. Using Risk Management as a decision making tool, allows installation commanders to take a disciplined approach to a complex, and often subjective decision, which balances the likelihood of an incident occurring and the impact of the incident if it occurs. Furthermore, in a constrained budget environment, Risk Management can help installation commanders optimize the protection return for each dollar invested.

The Risk Management process outlined in this manual follows three simple steps: 1) Build Risk Assessment Graphs; 2) Determine Levels of Risk; and 3) Determine Risk Reduction Measures.

Risk Management: Building Risk Assessment Graphs.

Risk Assessment Graphs display the information collected during Risk Assessment. In other words, they provide a snapshot view of the installation's current AT/FP posture. These matrices are based on the association between the likelihood of an incident occurring (the y-axis) and the severity of that incident if it occurs (the x-axis).

The installation will prepare two separate risk assessment graphs:

- Risk Assessment Area Graph;
- Risk Assessment AT/FP Function Graph.

The Area Risk Assessment Graph plots pairs of threats and areas in terms of the likelihood of that threat occurring and the area's CV rating. The AT/FP Functions Risk Assessment Graph plots pairs of threats and functions in terms of the likelihood of that threat occurring and the function's Effectiveness rating. Figure 1 shows sample Area and Function Risk Assessment Graphs.

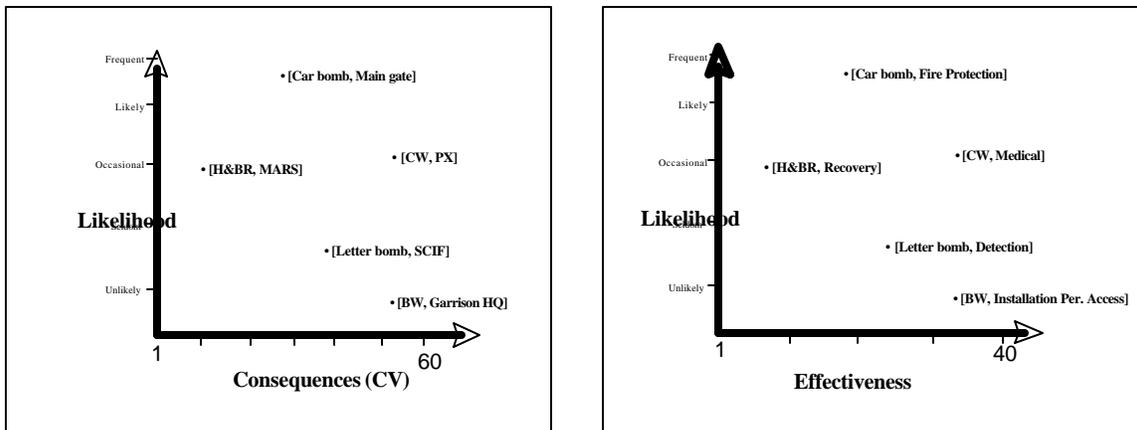


Figure 1. The Two Risk Assessment Graphs.

Risk Management: Determining Risk Levels

Risk Levels are indicators of the commander's threshold for taking substantive actions to deter, employ countermeasures, mitigate the effects, and recover from different types of terrorist incidents. Risk Levels can be used by the commander and the installation-level staff to prioritize actions for improving the installation's overall AT/FP posture.

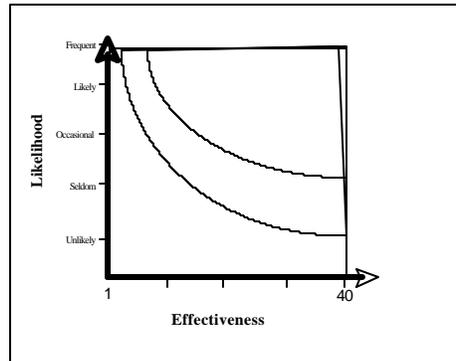


Figure 2. Risk Levels

Installation Commanders need to record the level of risk at which they are willing to operate, in terms of the likelihood of different types of incidents occurring and the assets, areas, and functions involved with those incidents. This is done by applying different colored areas to the Risk Assessment Matrices. **Red** areas on the graph highlight situations that require immediate and definitive action. **Yellow** areas highlight situations that do not require immediate action, but should be addressed eventually. **Green** areas highlight situations that do not require definitive action. For example, Figure 2 shows that this installation commander wants to take immediate and definitive actions in situations where the threat is high and the AT/FP functions are highly ineffective.

No standard methodology exists for establishing Risk Levels and their determination will vary from installation to installation, based on the commander's judgement. Although this process is subjective, considering the following questions may help commanders focus their decision on where to establish the colored areas:

- What is the installation's mission? How important is that mission to overall U.S. military objectives in the region?
- What resources are available for AT/FP activities on the installation?
- What assets are critical to mission accomplishment?

After determining the risk levels, apply these colors to the filled out Area and Function Risk Assessment Matrices (see Figure 3). The combination of the Risk Levels Graph and the Risk Assessment Graph together creates the installation Risk Management Graphs. These graphs are the basis for making decisions about where to employ risk reduction measures.

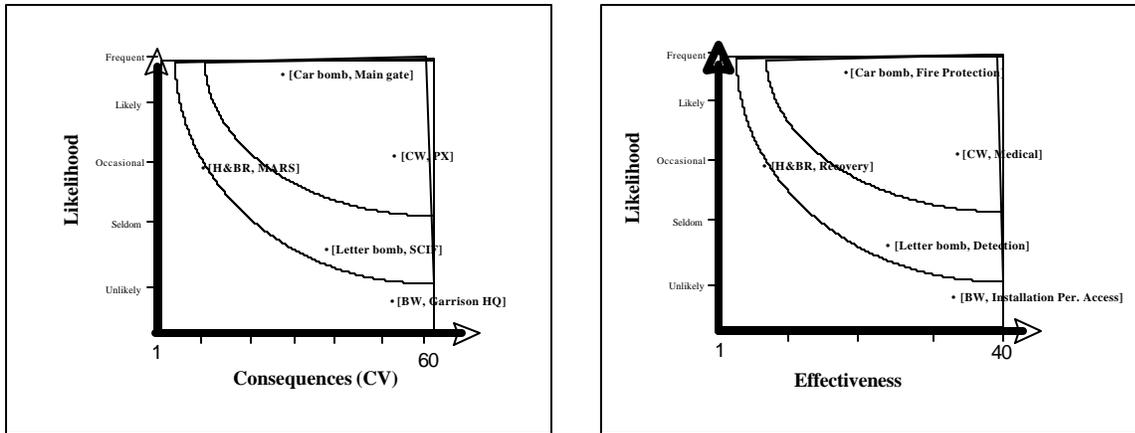


Figure 3. Risk Management Graphs.

Risk Management: Determining Risk Reduction Measures.

The objective of Risk Management is to help the local commander make decisions on where to improve that installation’s AT/FP capability. The purpose of the Risk Management Matrices is to help identify *which* areas and functions need to be addressed first. Determining *how* to address deficiencies and vulnerabilities in the installation’s AT/FP posture is an entirely different challenge.⁴

Remember that AT/FP is a system of systems. Improvements made in one functional area may improve not only the effectiveness of that function, but also negate vulnerabilities in other areas. Many physical security experts suggest that installations should focus first on addressing those threats that can be mitigated at the first line of defense—the installation perimeter. For example, the Risk Assessment may have identified a building that is vulnerable to 20,000 lb truck bombs. Rather than applying resources to protect that building from a 20,000 lb truck bomb, the installation commander may decide to improve Installation Perimeter Access, for example through better vehicle entry inspection, which negates the need to take such strong risk reduction measures at the building. Instead, the appropriate decision might be to protect the building against a 250 lb bomb, which may be able to get through the vehicle inspection at the perimeter.

However, this approach should not be the only guideline for making risk reduction decisions. For example, some installations have open access so an Installation Perimeter Access improvement is not a factor. In other cases, the solution for a vulnerability in one area may negate vulnerabilities in other areas, but it may be so expensive that it is cost prohibitive. Ultimately, installation commanders need to use their own judgment and cost-benefit analysis techniques to choose a system which matches their threshold for risk.

There are many resources available to installation commanders on risk reduction measures from mylar windows to barriers. A source of recommendations tailored to the installation is a JSIVA, Service or CINC assessment team final report. The Toolbox section of this document also contains some information on different risk reduction measures which may be applied to the *areas and assets* to be protected.

⁴ Annex C: Building Action Sets contains a walk-through methodology for the “How”.

Annex B: Threat Condition (THREATCON) System

Purpose :

The THREATCON system describes the progressive level of protective measures implemented by all DOD components in response to terrorist threats in accordance with DOD Directive 0-2000.12. The THREATCON system complements the national level intelligence community assessment of terrorist intentions and capabilities.

Commanders at the military community, air base, or geographically separated unit level will normally declare THREATCON levels for their units. This approach is designed to ensure the most appropriate response to an assessed threat for a specific area, installation or unit/command. Higher level commanders in the chain of command may, at any time, exercise their prerogative to declare THREATCON levels for their area of responsibility or any portion thereof. When this is done, more stringent security measures may be implemented by subordinate commanders, but the THREATCON set by the higher headquarters represents a baseline to which the installation commander must adhere.

Background:

Whereas the threat level is an intelligence community judgment about the likelihood of terrorist attacks on DOD personnel and facilities, the THREATCON system is the principal means the commander has to apply an operational decision on how to guard against the threat. THREATCON Levels are selected by assessing the terrorist threat, the capability to penetrate existing physical security systems at an installation, the risk of terrorist attacks of which DOD personnel and facilities expose themselves, the ability or units of installations to carry-on with missions even if attacked, and the criticality to DOD missions of assets to be protected. Assessed threat levels do not dictate the specific THREATCON posture that the installation assumes. The installation commander will declare a THREATCON Level appropriate for his location.

NOTE: More stringent security measures may be implemented by the installation commander, but the higher headquarters THREATCON Level represents the minimum baseline measures. THREATCON information and guidance are in DODI O-2000.16, Standard 11, 12, & 13.

DOD 0-2000.12-H and CJCS Handbook 5260 identify the five THREATCON Levels and the applicable THREATCON Measures for each Level. A similar list of measures which apply to shipboard terrorist threat conditions, see Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," 25 June 1993, Appendix J, pages J-6 through J-14. For a similar list of measures which apply to aviation facility terrorist threat conditions, see Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," 25 June 1993, Appendix J, pages J-14 through J-17.

Condition	Description	Measures
NORMAL	Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture.	
ALPHA	Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable.	1-10
BRAVO	Applies when an increased and more predictable threat of terrorist activity exists.	11-29
CHARLIE	Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent.	30-39
DELTA	Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, THREATCON DELTA is declared as a localized warning.	40-50

Measure 1: At regular intervals, remind all personnel and dependents to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Watch for unidentified vehicles on or in the vicinity of US installations. Watch for abandoned parcels or suitcases and any unusual activity.

Measure 2: Have the duty officer or personnel with access to building plans and plans for area evacuations available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on call and readily available.

Measure 3: Secure buildings, rooms, and storage areas not in regular use.

Measure 4: Increase security spot checks of vehicles and persons entering the installation and unclassified areas under the jurisdiction of the United States.

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

Measure 6: As a deterrent, apply measures 14, 15, 17, or 18 from THREATCON BRAVO individually or in combination.

Measure 7: Review all plans, orders, personnel details, and logistic requirements related to the introduction of higher THREATCONs.

Measure 8: Review and implement security measures for high-risk personnel, as appropriate.

Measure 9: Spare.

Measure 10: Repeat measure 1 and warn personnel of any other potential from of terrorist attack.

Measure 11: Keep all personnel involved in implementing antiterrorist contingency plans on call.

Measure 12: Check plans for implementation of the next THREATCON.

Measure 13: Move cars and objects (e.g., crates, trash containers) at least 25 meters from buildings, particularly buildings of a sensitive or prestigious nature. Consider centralized parking.

Measure 14: Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.

Measure 15: At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.

Measure 16: Examine mail (above the regular examination process) for letter or parcel bombs.

Measure 17: Check all deliveries to messes, clubs, etc. Advise dependents to check home deliveries.

Measure 18: Increase surveillance of domestic accommodations, schools, messes, clubs, and other soft targets to improve deterrence and defense and to build confidence among staff and dependents.

Measure 19: Make staff and dependents aware of the general situation in order to stop rumors and prevent unnecessary alarm.

Measure 20: At an early stage, inform members of local security committees of actions being taken. Explain reasons for actions.

Measure 21: Physically inspect visitors and randomly inspect their suitcases, parcels, and other containers.

Measure 22: Operate random patrols to check vehicles, people, and buildings.

Measure 23: Protect off-base military personnel and military transport in accordance with prepared plans. Remind drivers to lock vehicles and check vehicles before entering or driving.

Measure 24: Implement additional security measures for high-risk personnel as appropriate.

Measure 25: Brief personnel who may augment guard forces on the use of deadly force.

Measures 26-29: Spares.

Measure 30: Continue or introduce all measures listed in THREATCON BRAVO.

Measure 31: Keep all personnel responsible for implementing antiterrorist plans at their places of duty.

Measure 32: Limit access points to absolute minimum.

Measure 33: Strictly enforce control of entry. Randomly search vehicles.

Measure 34: Enforce centralized parking of vehicles away from sensitive buildings.

Measure 35: Issue weapons to guards. Local orders should include specific orders on issue of ammunition.

Measure 36: Increase patrolling of the installation.

Measure 37: Protect all designated vulnerable points. Give special attention to vulnerable points outside the military establishment.

Measure 38: Erect barriers and obstacles to control traffic flow.

Measure 39: Spares.

Measure 40: Continue or introduce all measures listed for THREATCONs BRAVO and Charlie.

Measure 41: Augment guards as necessary.

Measure 42: Identify all vehicles within operational or mission support areas.

Measure 43: Search all vehicles and their contents before allowing entrance to the installation.

Measure 44: Control access and implement positive identification of all personnel.

Measure 45: Search all suitcases, briefcases, packages, etc., brought into the. Installation.

Measure 46: Control access to all areas under the jurisdiction of the United States.

Measure 47: Frequent checks of building exteriors and parking areas.

Measure 48: Minimize all administrative journeys and visits.

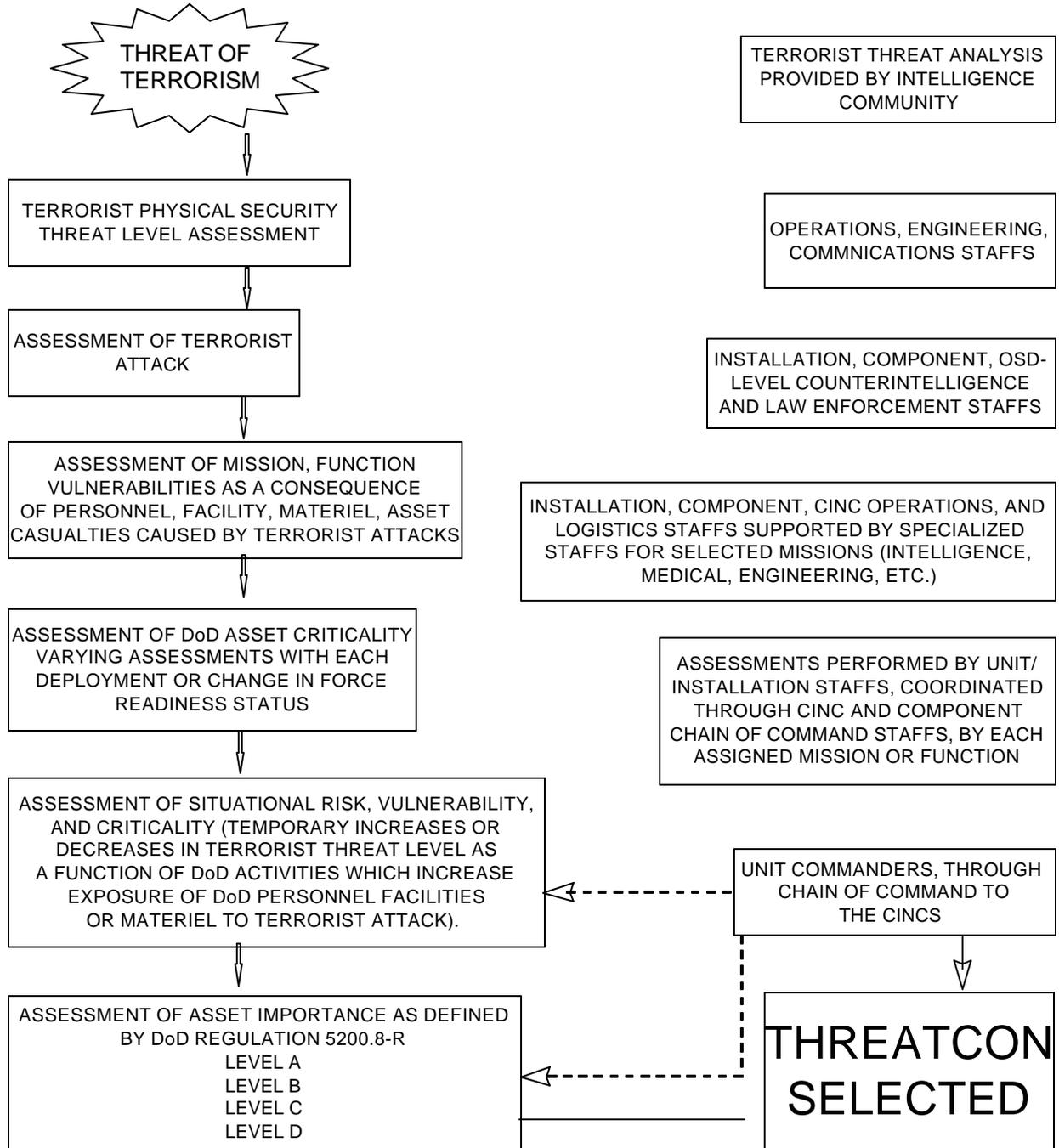
Measure 49: Coordinate the possible closing of public and military roads and facilities with local authorities.

Measure 50: Spare.

Specific THREATCON general information and guidance can be found in DOD 02000.12-H, Chapter 17 and Annex BB-1.

Note that Random Antiterrorism Measures (RAM) complement and supplement—but do not replace—the Measures defined in the THREATCON system. By altering security patterns and responses, the ability of a terrorist to use those patterns is greatly disrupted, making RAM an effective OPSEC tool.

GENERAL THREATCON SELECTION PROCESS



Appendix 2 to Annex B, Random Antiterrorism Measures

Background:

Random Antiterrorism Measures (RAMs) should be used to enhance the THREATCON measures identified in DOD 0-2000.12-H. While not replacing the handbook's required measures, RAMs allow the command to enhance security, break patterns, and vary responses to threats. These measures may include vehicle searches, ID card checks, and similar measures.

Critical Questions:

- Who is responsible for the RAM development/implementation at the installation?
- What type of plan is he to produce?
- How will these measures be integrated into the overall AT/FP Plan?

Considerations:

- Are the RAMs based upon the THREATCON?
- Are the RAMs conducted with/without increase to the THREATCON?
- What is the cost to increasing or decreasing RAMs once implemented?
- Does the installation's RAMs include increased threat education programs?
- What forces are responsible for implementing the desired RAMs?
- How will the RAMs be rehearsed to insure proper function when needed?
- How will rehearsals be conducted for minimum disturbance when not required?
- Who coordinates with local civilian authorities?
- How is the relationship with off base community affected?
- How is non-military transportation effected?
- Is any special equipment required to implement RAMs as there is an increase in THREATCON?
- What special training may be required?
- How are installation activities effected?
- How are the dependents lives effected?
- Will the RAMs include installation housing?
- Will the RAMs include installation support programs?
- Are the RAMs outlined for continuity purposes?

Annex C: Build the Action Set Matrices

1. Introduction. Annex A: Risk Assessment and Risk Management presented a methodology for examination of the installation and an assessment of current AT/FP posture. This annex extends that methodology by presenting a methodology to list exactly “How” the installation will prepare for and react to a terrorist threat. The end product of this annex will be a matrix of Integrated Action Sets that the installation will take for each THREATCON Measure at the five distinct THREATCON Levels. Each Integrated Action Set will identify who will act, when they will act, where the action will take place, what resources will be used, and detail what/how these actions will occur at the various THREATCON Levels. Upon completion, installation planners will enter the matrices into the AT/FP Installation Plan, paragraph 3b, Concept of Operations.

These action sets *serve as the implementation instructions* for employing the DoD THREATCON Measures. (Note: For easy reference, the THREATCON Levels and Measures are provided at Annex B.) To develop this end product the installation should:

- (a) Baseline the Installation at THREATCON NORMAL, using “Outside-In” Approach and applicable tools from Annex D;
- (b) Be prepared to respond to increased THREATCON Levels;
- (c) Develop specific action sets to implement each THREATCON Measure at increased THREATCON Levels;
- (d) Develop an Action Set Matrix; and,
- (e) Incorporate the matrix into the AT/FP Plan.

2. Baseline the Installation. Upon completing the Risk Assessment, the installation will have identified what areas/assets are critical and vulnerable to terrorist threats. As stated in Annex A, managing that risk is a continuous process. *Commanders may make immediate adjustments* to the installation’s AT/FP profile based on available resources, such as provision of additional lighting, additional fencing, and improved access controls and based on the experience and desires of the installation’s commander. Or the installation may make adjustments during the more structured “baselining” process.

Installation commanders must establish the installation’s AT/FP posture. DODI 0-2000.16, E1.1.17. DOD Standard 17 states: “Baseline Force Protection Posture. Commanders at all levels shall routinely review the effectiveness of daily physical security measures under THREATCON NORMAL. Employment of DOD standards contained in this Instruction become more applicable as commanders prepare for and implement responses to increases in THREATCON levels. However, effective THREATCON NORMAL procedures and associated daily physical security operations are the foundation for successful AT efforts.”

“Baselining” gives the installation commander a snapshot of the installation based on its current AT/FP security posture. It then allows for the implementation of immediate steps to be taken by the installation. For the purposes of this template, the following Outside-In Approach is recommended for baselining the installation.

Baselining: The Outside-In Approach:

One method of “baselining” the installation is to start from the perimeter of the installation and work inward (See Figure 1.) The AT/FP Officer and installation planners should collect background materials about the installation including: aerial photos, blueprints, maps, plans, and agreements with HN or local, state, and national agencies. During the baselining process, planners should remember to evaluate *all* assets, not just areas.

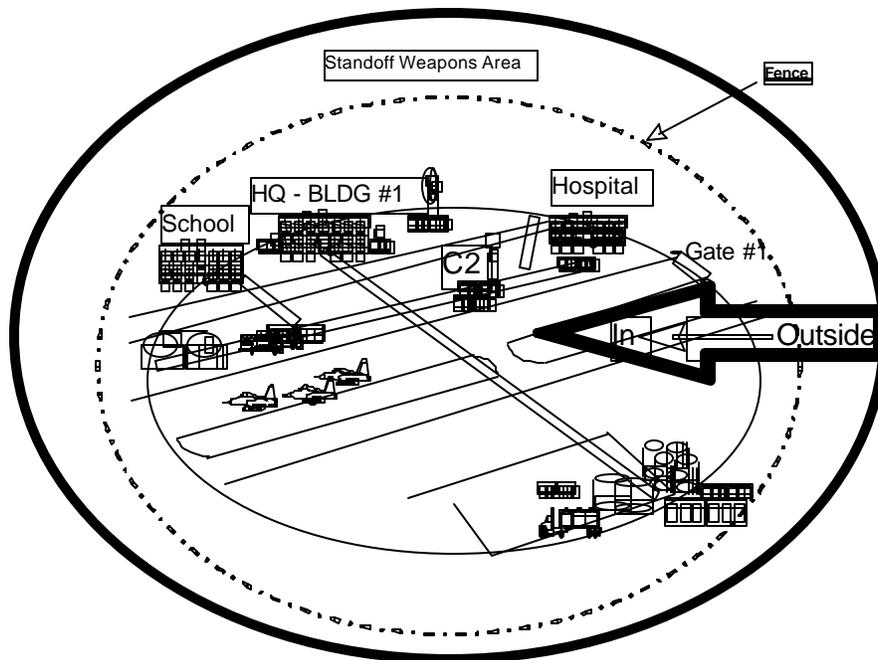


Figure 1. Baselining: The “Outside-In” Approach

To establish the installation’s baseline:

- *Collect the products* generated in the Threat, Criticality, & Vulnerability Assessments and the Risk Levels Tables from Annex A.
- Using the “outside-in” approach, start with the installation’s perimeter fence and *examine each area and asset* to determine the security posture of each.
- *Assess each area/asset* as:
 - (1) meeting the commander’s AT/FP standards, requiring no improvements,
 - (2) inadequate, needing improvement, or
 - (3) unsatisfactory, requiring improvement.
 - Throughout this process, the staff identifies the vulnerabilities and proposed solutions for enhanced protection of each area/asset (IAW DOD Standard 14). While this is a subjective process, the staff can formalize somewhat the process by using the various tools in Annex D of this template.
- The commander must take an active part in setting the baseline installation AT/FP posture by approving the immediate actions, based on available resources, to bring the installation to a minimum acceptable safe standard at THREATCON NORMAL.

3. Developing Action Sets. Changes in the terrorist intentions and capabilities, or changes to the installation environment may result in an increase in THREATCON Level. Therefore, the installation commander must be prepared to employ additional actions to enhance the installation’s AT/FP posture. While DoD 2000.12-H and CJCS Handbook 5260 identify the five THREATCON Levels and the applicable THREATCON Measures for each Level, the actual design and implementation of specific, measurable steps to act on the THREATCON Measures is left to the discretion of the installation commander.

To develop the action sets to carry out specific DOD THREATCON Measures:

- Review the THREATCON Measures (1-50) for each THREATCON Level;
- Review the AT/FP functional areas outlined in Annex D, The Toolbox;

- For each THREATCON Measure (1-50), determine the various functional areas required to implement the Measure (i.e., barriers, access control);
- Define each action as a discrete Integrated Action Set, using the five interrogatives (who, what, when, where, and why = W5) to outline “how” to implement the actions. These action sets should provide simple, straight-forward implementation instructions for each Measure at each THREATCON Level.

EXAMPLE: After a change to THREATCON DELTA notification, the G-4 provides 4 Jersey Barriers from the Post Engineers Warehouse (Building 111) at the corner of Butner and Kelly Rd. The 1/11th ENG Bn provides one heavy forklift to move the barriers and one ELWB 5ton truck to recover and transport the barriers. They will deliver the barriers within 2 hours of the alert notification. Until the Barriers arrive the MPs will conduct blockade functions with their vehicles. The Provost Marshal will direct the emplacement of the barriers. Emplacement of the barriers will be accomplished within 3 hours of THREATCON notification. The Jersey Barriers are required due to the Threat Assessment indication of increased terrorist activity including the use of 2,000 - 4,000 lb. vehicle bombs.

NOTE: The value-added to preparing Integrated Action Sets at this level of detail is to ensure that anyone, given a variety of circumstances (new service member on the installation, illness of the individual with primary responsibility for the action, midnight watch officer) can pick up the installation’s AT/FP Plan and activate the appropriate THREATCON Measures at the appropriate THREATCON Level. This also allows the AT/FP Officer, on behalf of the installation commander, to coordinate numerous tasks simultaneously, and have an excellent understanding of all measures in place.

Once planners have established a list of appropriate action sets, the installation commander should determine which action sets to employ (this is the commander’s operational decision on how to address the threat, a fundamental command responsibility.) It is the commander’s operational decision to determine which of these action sets, grouped by applicable THREATCON Measure, will be added to the AT/FP Installation Plan. Once this decision has been made, a matrix for each THREATCON Level should be prepared.

4. Develop the THREATCON Measure Matrix.

The matrix must include each THREATCON Measure, plus any additional Measures the commander determines are required to adequately face the installation’s terrorist threat. The matrix below illustrates one THREATCON Measure (#46) and one illustrative action set for one functional area (Gate #1). Actions will need to be repeated for each functional area that applies to the THREATCON Measure and for each THREATCON Measure itself.

For each THREATCON Level, the staff will develop a matrix, outlining the appropriate THREATCON Measures and Integrated Action Sets. To complete this matrix:

- Label the matrix with the appropriate THREATCON Level (ALPHA-DELTA).
- In the matrix’s left-hand column, list the applicable THREATCON Measures (plus additional Measures the commander identifies) which apply to the THREATCON Level.
- In the matrix’s right-hand column, list the sets of actions required to fully implement each THREATCON Measure. (Methodology should follow the “outside-in” approach. The Integrated Action Sets should describe exactly *how* the Measures will be applied, by answering the appropriate *who, what, where, when, why* questions. (See the example matrix below for an example of a THREATCON Measure and its related Integrated Action Set.)
- Once you have developed an Integrated Action Set for each Measure at the selected THREATCON Level, move on to a new matrix for the next THREATCON Level and repeat the process until a matrix has been completed for each THREATCON Level.

In addition to the Measures prescribed by DOD for a THREATCON Level, the commander should list any additional Measures including, those from a higher THREATCON Level, any new Measures, and/or Random Anti-Terrorism Measures.

THREATCON DELTA

Measure 1...45

Measure 46: Control access...

- List the applicable Action Sets.
- Gate 1:
 - Barriers
 - G-4 provides 4 J-barriers, located at _____
 - 1/11 EN Bn provides one heavy forklift to move barriers
 - 1/11 FA Bn uses 1 ELWB 5T truck to recover the barriers
 - PMO will direct placement of the barriers
 - Fences
 - 1/11 EN Bn provides 50M of concertina wire
 - 1/11 FA Bn installs 25M of concertina on each side of the access road
 - Lights
 - G-4 provides 4 lights with appropriate power source
 - 1/11 IN Bn recovers the lights & moves them to Gate 1
 - PMO directs placement of the lights
 - Sensors N/A
 - Guard Force
 - PMO provides sufficient personnel to man Gate 1 with 3 guards 24/7
 - HHC, Garrison provides ROE & other relevant training
 - PMO will issue weapons & ammunition
 - DOL, Garrison, will provide and place the portable guard shed and portable toilet at Gate 1
 - HHC, Garrison provides rations
 - These actions will occur within three hours of change in THREATCON Level alert
- Mission Essential Site 1 (Power Plant)
- Mission essential Site 2 (Garrison HQ)
- Mission Essential Site 3 (Garrison antenna farm)
- Mission Essential Site 4 (Garrison Dining Facility)
- Continue until all MEVAs have been planned

Measure 47:

Measure "n"

Develop Actions Sets using the process above.

List applicable Action Sets.

Table 1: Example THREATCON Level Action Set Matrix.

It is likely that some recommended THREATCON action sets that would enhance the security posture of the installation may not be applied due to resource constraints. The staff should prepare plans and budgets to address these vulnerabilities, and identify these shortfalls to the next higher headquarters. DOD guidance requires that the installation commander advise the chain of command on AT/FP posture and implementation shortfalls.

Note: This matrix will form the heart of the installation's AT/FP Plan, as it captures the actual implementation steps to be taken on the installation. Should the installation staff and commander decide to publish the AT/FP Plan using the five-paragraph OPORD format (which we highly recommend), this matrix will be the center of paragraph 3 (Execution) in the Concept of Operations subparagraph.

Annex D: Toolbox

Purpose: The attached appendices are standing operating procedures that may apply to an installation as part of ongoing AT/FP efforts. These coordinating instructions are “tools” which will assist the installation commander and staff with the development of the specific implementation instructions or “action sets” to be applied to DoD THREATCON Measures. All of the elements of this plan are integral and must be linked in an integrated “system of systems” to ensure successful ongoing AT/FP operations. This integration and linkage will occur as installation planners use the applicable tools throughout Annex D (Toolbox) to baseline the installation and develop appropriate action sets. They will then insert the action sets into the THREATCON Level matrices, and then insert the matrices into the AT/FP Installation Plan’s Concept of Operations, Paragraph 3b. (This methodology is outlined in Annex C).

Several appendices, tabs, and enclosures are included to assist the commander and staff to “jump-start” the planning process for each functional area. Each individual tool is not required to complete the plan.

Appendix 1: Tasks & Responsibilities

Purpose:

This annex provides the basic foundation for the delineation of tasks and responsibilities for selected staff and subordinate elements. If not previously described, the commander should define the specific tasks and responsibilities for each listed staff officer, commander, and subordinate element to reflect his operational requirements and desired span of control.

- **Secretary of Defense and the CINC.** Pursuant to 10 U.S.C. Section 164 and 22 U.S.C. Section 4802, the Secretary of Defense and CINC are responsible with covered countries for the security of all DOD elements, personnel, and facilities under the command of the CINC.
- **Department of State.** Pursuant to 22 U.S.C. Section 4802, the Secretary of State is responsible within covered countries for developing and implementing policies and programs to provide for the security of DOD elements, personnel, and facilities not under the command of the CINC. IAW 22 U.S.C. Section 4805(a), the Secretary of State retains ultimate authority and responsibility for the security of DOD elements, personnel, and facilities—unless a specific MOU assigns parts or all of that responsibility to the Department of Defense. Normally, the Secretary of State's responsibilities includes defense Attaché Offices, Marine Security Guard Detachments, DOD personnel detailed to other USG departments or agencies, and DOD elements which form an integral part of the U.S. country team for which a Chief of Mission has assumed responsibility.

NOTE: The following are examples that the installation commander should use to assign task and responsibilities and to ensure completeness.

- **Commander**
 - A combating terrorism checklist for new commanders can be found in DOD 02000.12-H, Appendix W.
 - The DOD Installation commander will designate a single point of contact to oversee the antiterrorism and fore protection programs (DODI 2000.16 & DOD 0-2000.12-H).
 - Develop necessary standard policies and procedures to supplement the provisions of this regulation to meet installation specific needs, including joint supplementation, when possible.
 - Ensure that Antiterrorism plans, at a minimum, include procedures to collect and analyze terrorist threat data, procedures to enhance security posture, and procedures to respond to a terrorist event. (DODI 2000.16 # 5).
 - Coordinate and maintain liaison with the other Departments and Agencies on physical security matters.
 - Establish procedures for sharing threat information expeditiously through law enforcement and intelligence channels.
 - Formalize Antiterrorism procedures for joint response.
 - Develop specific Antiterrorism installation threat assessments and update them frequently.
 - Coordinate the acquisition of Antiterrorism equipment and establish procedures to identify requirements for related research and analysis.
 - Develop training, qualification, and suitability requirements for dedicated security forces.
 - Conduct combined operations with Host Nation security or Local (if CONUS) law enforcement organizations.
 - Ensure that AT/FP Plans are reviewed periodically at a higher level. (DODI 2000.16 # 6)
 - Installation Commanders shall make use of the DOD Terrorism Threat Level System to establish the proper THREATCONs and RAM. (DODI 2000.16 # 7, 8, &9)
- **Installation AT/FP Officer**

- A combating terrorism checklist for installation antiterrorism and force protection officer can be found in DOD 02000.12-H, Appendix W.
 - Attend the Combating Terrorism on Military Installations or Bases Course (5 days) at the U.S. Army Military Police School, Fort McClellan, Alabama, or an equivalent.
 - Unit/ship AT/FP Officers will attend the above course when deployment is to a high-threat area.
 - Develop an installation Combating Terrorism Program (UP DODD 2000.12 and CJCS Handbook 5260).
 - Develop an installation Combating Terrorism Plan (UP DODD 2000.12 and CJCS Handbook 5260).
 - Coordinate the Combating Terrorism Plan with foreign, state, and local law enforcement agencies as recommended by DOD 2000.12-H & CJCS Handbook 5260.
 - Ensure that AT/FP Planning is integrated into overall force protection planning as recommended by DOD 2000.12-H & CJCS Handbook 5260.
 - Ensure that the installation's AT/FP library contains the current versions of all appropriate directives, instructions, regulations, SOP/SOIs, and other pertinent documents. (UP CJCS Handbook 5260).
 - Establish an AT/FP Awareness Program IAW DODD 2000.12.
 - Provide periodic terrorism awareness briefings IAW DODD 2000.12.
 - Ensure that the installation conducts an AT/FP exercise annually IAW DODI 2000.14 & service implementing instructions.
 - Ensure that installation training scenarios integrate into training exercises IAW DODI 2000.14.
 - Conduct a vulnerability assessment or risk analysis, as referenced by DOD 2000.16.
 - Prepare a prioritized list of Mission Essential Vulnerable Areas as recommended by DOD 2000.12-H & service implementing guidance.
 - Assist in the identification of the installation's crisis management team, ensuring that this team meets quarterly and conducts its business IAW DOD 2000.12-H, Chapter 15.
 - Identify AT/FP physical security requirements.
 - Develop AT/FP Installation Plan.
 - Assist in development of Incident response Plan.
 - Program AT/FP resources.
 - Identify new construction requirements.
 - Bring existing structures to baseline standards using IVA tools.
 - Coordinate AT/FP efforts with HN authorities and the U.S. Country Team.
 - Provide appropriate level I AT/FP training to installation personnel
 - Identify, in concert with the installation AT/FP Officer where the lack of AT/FP funding has adversely impacted the installation's AT/FP program as recommended by CJCS Handbook 5260.
 - Ensure that the commander and key staff officers of the installation have an understanding of AT/FP preventive measures and considerations, as outlined in Joint Pub 3-07.2, Chapter VII.
- **Operations Center**
 - Ensure well-defined and location-specific pre-deployment AT/FP requirements are developed and implemented as recommended by DOD 2000.12-H, Joint Pub-07.2, & CJCS Handbook 5260
 - Ensure that the above requirements provide for pre-deployment threat awareness planning, for identification of key elements for additional protection, and assurance that the flow of critical threat information to deployed units will not be interrupted, IAW DOD 0-2000.12-H.
 - Develop a crisis management plan IAW Joint Pub 3-07.2, Appendix G.
- **Intelligence Officer**
 - Collect threat information.

- Conduct threat analysis.
 - Produce threat assessment.
 - Develop threat assessment plan and ensure that it is current IAW DODD 2000.12.
 - Ensure procedures exist to allow for the timely dissemination of immediate terrorist threats, assessments and other intelligence to all appropriate users both during and after duty hours IAW DODD 2000.12 & CJCS Handbook 5260.
 - Ensure the installation has a travel security program and that it provides for travelers threat information briefings IAW DODD 2000.12 & CJCS Handbook 5260.
 - Ensure that the installation commander reviews the collection and dissemination of terrorist information plan (and the information itself) at least annually and assesses that information and plan as adequate IAW DOD 0-2000.12-H.
 - Ensure that the installation receives recurring threat updates IAW DODD 2000.12 and service implementing instructions.
 - Ensure that the intelligence analysis at the installation is a blend of all appropriate intelligence disciplines and that the intelligence officer and the AT/FP officer understand the sources of the information IAW DOD 0-2000.12-H.
 - Ensure that the intelligence cell for the installation reviews information to identify indications that all available information is being collected or disseminated IAW DOD 0-2000.12-H.
 - Ensure that LEA developed information is shared and blended with intelligence information as recommended by DOD 2000.12-H.
 - Conduct, in concert with the installation's security personnel and the AT/FP Officer, a vulnerability assessment IAW Joint Pub 3-07.2, Appendix A.
 - Provide the commander and key staff with the antiterrorism introduction and terrorist overview background information contained in Joint Pub 3-07.2, Chapters I & II.
 - Develop scenarios for threat evaluation.
- **Provost Marshal, Security Police & Forces**
 - Ensure the installation has a current, adequate physical security plan IAW DODD 2000.12, DODD 5200.8, & CJCS Handbook 5260.
 - Ensure that the physical security plan includes AT/FP protective measures as recommended by DOD 2000.12-H.
 - Ensure that there is a mutual understanding between all local agencies that might be involved in a terrorist incident on the installation regarding authority, jurisdiction, and possible interaction as recommended by DOD 2000.12-H & CJCS Handbook 5260.
 - Ensure that LEA developed information is shared and blended with intelligence information as recommended by DOD 2000.12-H.
 - Conduct a vulnerability assessment IAW Joint Pub 3-07.2, Appendix A.
 - Develop an installation-wide program to all installation offices which highlights office procedures which will assist the deterrence of terrorist acts on the installation. A general background overview containing this type of information is in Joint Pub 3-07.2, Appendix D.
 - Provide security coordination with local and jurisdictional entities.
 - Provide primary reaction/special reaction teams.
 - Provide on-scene commander.
 - Provide executive protection.
 - Man traffic control points and observation post .
 - Provide security for applicable personnel and facilities.
 - Ensure security personnel are thoroughly trained in military police duties to allow maximum effective use of assets.
 - Ensure internal security of "facilities" particularly during hours of darkness by conducting security checks of designated activities .
 - Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military law enforcement office, other supported activities, local counterintelligence office, and local military criminal investigation office.

- Conduct regular liaison visits with the supporting military law enforcement office, counterintelligence office and local criminal investigation office.
 - Coordinate with the supporting military law enforcement office and counterintelligence offices on their preparation and continual updating of the threat assessments.
 - Assist in providing terrorism threat awareness training and briefings to all personnel and family members as required by local situations.
 - Provost marshal, military police commander, or military police physical security staff officer, assigned or attached to the terminal advises, recommends, and assists in preparation of physical security plans and implementing directives. He also either commands or supervises security guard forces assigned to the terminal (military and civilian), and participates in the coordination of all security and defense activities of the terminal (tactical and non-tactical).
 - Assist in directing the hospital command's crime prevention and hospital security program.
- **Public Affairs Officer.** Because terrorists seek media recognition, media information management must be in the best interest of USG in managing the situation.
 - Additional general information on public affairs duties and functions can be found in TC 19-16, Appendix R.
 - Screens information to the media to ensure OPSEC and provides advise and counsel to those in charge.
 - Check with the operations center manager frequently.
 - Revise public affairs plans to meet the installation's information distribution requirements for AT/FP issues or occurrences.
 - Disseminate information to the media IAW the established PAO & AT/FP Plans.
 - control press releases.
 - coordinate press releases with the commander, the operations center staff, and higher echelon PAOs prior to dissemination.
 - control the movement of news media personnel with press passes, escorts, and other similar means.
 - obtain approval for the following prior to release:
 - news releases.
 - news media personnel to enter outer perimeter.
 - release of photos.
 - interviews with anyone other than the commander.
 - direct communications between the press and involved persons.
- **Staff Judge Advocate**
 - The SJA or other installation AT/FP legal advisor will ensure that the commander, and key staff—particularly the Installation At/FP Officer—understand the legal considerations of developing and implementing a Combating Terrorism Program. A thorough introductory overview can be found in Joint Pub 3-07.2, Chapter III.
 - Interpret legal issues dealing with such issues as use of force.
 - Interpret status of forces agreements and local laws as pertaining to AT/FP.
 - Aid in the interface between the military and local authorities dealing with AT/FP issues.
 - Aid in the interpretation of appropriate documentation concerning any AT/FP issue.
 - Interpret International Agreements that would affect security issues.
 - Understand the rules of engagement.

- **Chaplain**
 - Act as advisor and consultant to the commander on all matters of religion, morals, and morale as affected by religion.
 - Help in coordinating all potential AT/FP issues that arise in connection with foreign local customs and religions.
 - Coordinate and maintain liaison with local churches, indigenous religious bodies, and religious groups throughout the communal area of responsibility.
 - Provide unit, area, and denominational ministry for all personnel.

- **Safety Officer**
 - Develop a standard operating procedure for safety inspections.
 - Conduct safety inspections of installation facilities.
 - Coordinate with the Military Police.

- **Comptroller**
 - Ensure AT/FP funding requirements are included in the installation's budgeting process for ultimate inclusion in the POM cycle as recommended in DOD 0-2000.12-H.
 - Ensure required AT/FP enhancements have been identified, prioritized, and funded.
 - Identify AT/FP funded project shortfalls for each FY and advise the installation commander as recommended in DOD 0-2000.12-H.
 - Identify, in concert with the installation AT/FP Officer where the lack of AT funding has adversely impacted the installation's At program as recommended by DOD 0-2000.12-H.

- **Subordinate Commanders**
 - Create a level of awareness, appreciation, and readiness commensurate to the threat.
 - Ensure proper coordination of all local policies and measures for protecting DOD facilities, resources, equipment, personnel, and family members in foreign areas from terrorist acts and for assisting their subordinate commanders in implementing military service programs.
 - Ensure the DOD THREATCONs for combating terrorism are uniformly implemented as specified in DOD Directive O-2000.12.
 - Serve as the DOD point of contact with US embassies and host nation officials on matters regarding such policies and measures.
 - Assess the terrorist threat for the theater and provide a copy of the threat assessment to the services.

- **Explosive Ordnance Disposal**
 - Train postal personnel in letter bomb recognition and procedures.
 - Train security personnel in bomb search procedures.
 - Assist in training of personnel in IEO recognition.
 - Develop an SOP for EOD procedures of WMD incidents.
 - Develop an SOP for the render safe and disposal of explosive materials.

- **Base Civil Engineer**
 - Ensure that procedures have been established to ensure that all military construction projects are reviewed at the conceptual stage to incorporate physical security, AT/FP, or protective design features IAW DODD 5200.8-R & DOD 0-2000.12-H.
 - Aid in the development of construction policies for incorporating FP design measures into MILCON projects and modification to existing facilities.
 - Obtain/provide a base grid map for installation planning.

- **Communications Commanders**
 - Assign qualified personnel to manage and operate communications in the Emergency Operations Center.
 - Build contingency plans for situations when the normal forms of communications are intercepted.
 - Establish and maintain communications during non-critical and critical situations.

- **Medical Commanders**
 - Establish a medical/Disaster Control Element Control Center (ref NASPNCLA).
 - Organize, equip, train, and direct medical centers.
 - Assist in the location of survivors and deceased, and assist in the rescue of survivors.
 - Establish a field emergency medical aid station at the disaster site and coordinate ambulance support with the Hospital.
 - Catalog survivors and direct segregation for further treatment.
 - Perform mortuary duties as required.
 - Assign appropriate qualified personnel to assist in medical emergencies.
 - List plans and policies for the treatment, hospitalization and evacuation of military and civilian personnel.

- **Logistics Commanders**
 - Provide inventory and accountability procedures input into the physical security program for the administrative control of property.
 - Aid in the formulation and announcement of policy for integrated logistics support (ILS) program for multi-service programs (AR 700-129).
 - Establish a central logistics control center.
 - Organize, equip, train, and direct the operations of the control center.

- **Maintenance Commanders**
 - Ensure that a proper maintenance plan has been established.
 - Conduct proper maintenance procedures on all equipment .
 - Ensure proper command and control over all property assigned.
 - Develop contingency plans for movement of equipment .
 - Develop Standard Operating Procedures for all equipment that has been moved and is currently in the “motor pool” to ensure that proper security measures have been followed to prevent incidents.

- **Munitions Commanders**
 - Maintain positive control over all sites and munitions.
 - Conducts inspections of munitions facilities.
 - Develop a standard operating procedure for command and control of munitions.
 - Ensure proper security measures have been followed.
 - Ensure proper procedures are followed in the decimation of munitions.

- **Transportation Commanders**
 - Assess the threat, sensitivity of cargo, vulnerability, and mode of transportation to dictate the degree of security required during storage and in transit of cargo being shipped. The degree or type of security needed is determined by:
 - Facility size and location.
 - Complexity of storage or shipment.
 - Volume/value of items.
 - Economic and geographical situation.
 - Available crime statistics.
 - Security/law enforcement available.
 - Transit shipments.

- Responsible for the development of an effective cargo security system, which should be based on:
 - Experiences of personnel responsible for shipments and storage of cargo.
 - Loss potential based on a risk analysis.
 - Established security standards and policy.
 - Minimize exposure to individuals who display a motive to steal by illustrating and using countermeasures, screening prospective personnel, by eliminating in-facility gambling among employees, by insuring close coordination between packaging, shipping, and receiving personnel.
- **Air Mobility Commanders**
 - Coordinate the movement of personnel and equipment through proper command and control measures.
 - Liaison with airfield security personnel, assist in departures and arrivals at airfields and en route, and determine weapons and ammunitions policies.
 - Provide liaison with host nation if arriving at a foreign post or airport.
 - Maintain open communications net between all elements until the aircraft is loaded and re-establish communications upon arrival.
- **Air Base Commanders**
 - Provide necessary personnel and equipment for operations in the AO.
 - Provide Explosive Ordinance Disposal services as required.
 - Obtain authority to transport civilian NIS and FBI agents in government aircraft as required.
 - Provide internal security for surrounding airfields and hangers
 - Provide search and rescue capability.
 - Provide Communication-Electronic support .
- **Port Commander**
 - Protect the port, e.g., by fencing and pass control; protect the part of the pier that protrudes over the water by such things as patrols, protective lighting, booms, and nets.
 - Coordinate with the supporting military law enforcement office and counterintelligence offices on their preparation and continual updating of the threat assessments.
 - Assist in providing terrorism threat awareness training and briefings to all personnel and family members as required by local situations.
 - Conduct regular liaison visits with the supporting military law enforcement office, counterintelligence office, and local criminal investigation office.
 - Report all actual or suspected terrorist incidents or activities to their immediate commander, supporting military law enforcement, other supported activities, local counterintelligence office, and local criminal investigation office.
- **Transportation Terminal Commander**
 - Ensure the safety and security of the entire terminal.
 - Protect the personnel assigned to, passing through, or working within the terminal.
 - Security of all cargo from time of arrival in terminal to departure, either inbound or outbound.

Appendix 2: Alert Notification Procedures

Purpose :

This appendix deals with the dissemination to the appropriate officials and the public timely warning/forecasting of all situations requiring response actions. This warning information is vital and must be made available in order to ensure that not only the staff and responding forces, but also the installation occupants, are adequately notified of an impending or actual situation. Alert notification appendix should describe the warning systems in place and the responsibilities and procedures for using them.

Critical Questions:

- Who is responsible for developing the alert notification/warning system?
- What type of plan will the responsible person produce?
- How will these measures be integrated into the overall AT/FP Plan?

Considerations:

- What are the procedures to “alert” the AT/FP Crisis Management Team?
- What are the procedures to “activate” the AT/FP Crisis Management Team?
- Is a system in place to ensure alert rosters in the AT/FP Plan are up-to-date?
- What means is available to communicate with general populace/installation residents?
- What notification procedures is in place to notify all personnel to remain at their place of duty?
- What procedures are in place if there are people who are directly threatened by a hazard but ignore, may not hear, or not understand the warnings issued?
- What procedures are in place to notify special needs groups such as the hearing-impaired, sight-impaired, or physically disabled, who require special attention?

Appendix 3: Installation AT/FP Exercises

Purpose :

The purpose of this annex is for planners to establish a plan and a mechanism to adequately exercise the AT/FP Installation Plan. This identifies shortfalls and weaknesses, so the commander can implement additional measures to enhance the installation security posture.

The installation staff should include the installation AT/FP exercise planning schedule here.

Appendix 4: Incident Reaction Planning

Purpose :

Incident reaction planning is a sequence of command and staff actions undertaken to solve a terrorist incident or other unique event. Other than differing in its area of emphasis, it essentially follows the same sequence and involves the same people as other military operations. Attached as several tools and tabs that can be used in a variety of incidents which will assist in developing an Incident Reaction Plan. This plan should be integrated into the overall AT/FP Plan.

Background:

Studies of terrorist methods of operation and case studies show that the best chance of success against terrorism lies in the prevention & planning phase. Terrorists are formidable adversaries who may choose a hardened, well defended target, if results are demonstrated as worth the risk. They will reconnoiter extensively, gather detailed intelligence, and plan and rehearse an attack that has a high probability of success.

Responding to a terrorist incident requires special capabilities. The special requirements of this OPLAN are:

- Preparation for multiple incidents or diversionary tactics
- Establishment of communications nets
- Activation of required resources
- Preparation for prolonged incidents
- Education and Training for Consequence Management
- Management of the media
- Preparation of an after action report

Critical Questions:

- Who is responsible for the incident reaction planning for the installation?
- What specific plans must be included in the AT/FP Plan?
- What element or unit will be the first responders?

Considerations:

- What is the threat?
- What historical data is available on past incident?
- What is the terrorist threat's method of operations?
- What is the installation's MEVA?
- Who are the high risk personnel (HRP)?
- How do HRPs most commonly travel?
- Do the HRPs have escort teams with them?
- Who coordinates with local law enforcement?
- What are the local law enforcement capabilities?
- What are the emergency response capabilities of the local government?
- What security capabilities are organic at the installation?
- What special equipment does the security force need?
- What special training does the security force require?
- Have the installation's MEVAs been identified for the commander?
- What Intrusion Detection System is currently in place at the MEVAs?

Tab 1: Bombing

Purpose:

Terrorists commonly use the bombing tactic, since a bomb is inexpensive to produce, easy to make, adaptable to a variety of uses and difficult to detect and trace after the event. Other advantages include their attention-getting capacity and the ability to control casualties through time of detonation and placement of the device. This tab will assist the planner in developing the incident response plan.

Critical Questions:

- Who is responsible for counter bombing planning?
- What information should be incorporated into the Incident Response Plan?
- What force has been identified to respond to a bombing incident?

Considerations:

- Has there been a previous bomb attack against this installation?
- Has there been a previous bomb attack against a DOD installation in this region, country, or area?
- What was the type of bomb and method of delivery?
- Is there a EOD team on the installation?
- If not, where is the closest EOD team?
- Does the local law enforcement agency have an EOD team?
- Who will be first responder to a bomb threat?
- What equipment is needed to respond to a bombing incident?
- Who will conduct a bomb threat search?
- What equipment is available for bomb searches?
- What special training is required for bomb searches?
- Is there a personnel awareness training program for parcel bombs?
- Is there an individual awareness for vehicle bombs?
- What security measures are maintained for unattended HRP vehicles?
- What security measures are taken for HRP home awareness?
- What technologies are being used for bomb detection?

Enclosure 1: Bomb Threats

Upon receiving an anonymous telephone call:

- Try to keep a word for word record of the conversation.
- Attempt to obtain the caller's name, address, and telephone number. Point out to the caller that by giving these details he is indicating his call is a genuine warning.
- Attempt to keep the caller engaged and elicit further information if possible.
- Summon assistance (through a telephone exchange) to listen to the call and to corroborate facts and opinions.
- Comply with the caller's request to be connected with another extension. Monitor the call if possible. Alert the security officer or the officer of the day.

During call:

- Try to obtain answers to the questions listed on the telephone at information sheets.
- Try to determine the type of telephone call by contacting the operator immediately after the call ends. Was the call operator-connected? If the call was operator-connected, Can the operator identify the caller/phone? Was it from a pay phone? If dialed from a pay phone was it direct dialed?

After the call is complete:

- Provide the police duty officer with details of the telephone call
- Make a full written record of the conversation and your impressions based on the information annotated on the telephone at information sheet. This could be invaluable to the local or military police.

The following actions should be taken upon receipt of a Bomb threat:

- Questions to ask for all threats:
 - Why are you making this threat?
 - What is your address?
 - What is your name?
 - Where are you calling from?
- Questions to ask for Bomb Threats:
 - When is the bomb going to explode?
 - Where is it right now?
 - What does it look like?
 - What kind of bomb is it?
 - What will cause it to explode?
 - Did you place the bomb?
 - Exact wording of the threat (attempt to capture a verbatim record)
- Other threat information:
 - Sex, race, age, length of call, number here call was received, time received, and date
 - Caller's voice (calm, angry, loud, slow, deep, accent, disguised, familiar, whispered, distinct, other)
 - Background sounds (static, voices, clear, motor, music, noise, local, street, animals, office machines, other machines, other)
 - Threat language (well-spoken, foul, irrational, taped, incoherent, other)
- The following data will be included in a Bomb Threat Report:
 - Any warning received
 - Identity of the person who discovered the device
 - How the device was discovered
 - Location of the device
 - Time of discovery
 - Estimated length of time device has been in place

- Description of the device
 - Safety measures taken
 - Suggested routes to/fm the scene
 - Other pertinent details
 - Summon assistance to trace the call and to corroborate facts and opinions
- In the event that an explosive device is found/suspected, the installation will follow these explosive device procedures: Suspicion that a device is within the installation may stem from an anonymous phone call. Treat all calls seriously.
 - Upon receipt of warning, inform local installation law enforcement and EOD personnel. Decide on need for evacuation, & type of evacuation (search without evacuation, movement of personnel from given area/facility, partial evacuation of the installation, total evacuation of the installation).
 - Determine method of search (nominated persons, occupant, team, dog)
 - Plan search organization
 - Plan alarm procedures
 - Plan evacuation procedures
 - Plan assembly areas for evacuation from all areas and facilities
 - Plan routes to assembly areas
 - Plan building and are clearance search procedures
 - Conduct evacuation drills
 - Plan isolation procedures
 - Plan reactions to explosions (with casualties, without casualties)
 - Plan for access control)

Tab 2: Arson

Purpose :

Terrorists use arson to destroy or disrupt such targets as public utilities, political headquarters, and more commonly, economic industrial targets such as shops, factories, and hotels. While arson is less dramatic than most tactics, it is low risk, inexpensive, and easy to apply. This tab will assist the planner in developing information regarding arson to be included in the Incident Response Plan.

Critical Questions:

- Who is responsible for counter arson planning?
- What information should be included in the Incident Response Plan?
- What force will be the first responder to an arson incident?

Considerations:

- What security measures are currently in place on the installation?
- What fire detection systems are presently being used?
- What IDS is available?
- Are there evacuation programs at each facility?
- Are the installation personnel properly trained?
- Are sensitive materials properly maintained from fire damage?
- Are all flammable materials maintained separately from facilities?
- What response equipment is organic to the installation?
- What special equipment is required for firefighting?
- What special training is required?
- What equipment is available from the local area?
- Is there an airfield firefighting capability?
- What is security responsibility at a facility fire?
- What is the mass casualty medical trauma capability?

Tab 3: Hijacking

Purpose :

While hijacking is sometimes employed as a means for escape, it is normally carried out to produce a spectacular hostage situation. Although trains, buses, and ships have been hijacked, aircraft are the preferred target because of their greater mobility and vulnerability.. Throughout regions of the world, the hijacking of vehicles for the goods and food has been historically used to enhance the terrorist organization and to be dispersed among the population as a 'Robin Hood' gesture. Hijacking, along with skyjacking, is still a popular tactic for terrorists. Some terrorist organizations may hijack vehicles as a means of delivery for a future more deadly operation. This tab will assist the planner in preparing the Incident Response Plan.

Critical Questions:

- What person, staff, or unit is responsible for the development of the counter-hijacking plan?
- What information regarding hijacking will be integrated into the Incident Response Plan?
- What force(s) will respond to a hijacking situation?

Considerations:

- What is the threat?
- What historical data can be provide to method of operation?
- Are all installation vehicles dispatched out with a clear timeline for arrival to the destination?
- How are vehicles secured at evening?
- How are vehicles identified?
- What IDS is used at the motor pool?
- What portable IDS system is available for vehicles that travel out of installation area?
- How is cargo secured on trucks?
- What locking system is used for trailers?
- Who is responsible for organizing escort details?
- What special equipment is required for escort details?
- Who coordinates with local authorities for escort movements?
- Is there an airfield at the installation? If so, review the airfield appendix.
- How are aircraft secured?
- What IDS systems are being used?
- Is there a VIP aircraft at the installation?
- Who is responsible for checking the security, pre and post flights?
- Who insures security is in place prior to VIP arrival?
- Who secures visiting VIP aircraft?
- How are visiting personnel identified into the aircraft area?

Tab 4: Assassination

Purpose :

Assassination is perhaps the oldest terrorist tactic. It is still widely used today. Invariably, terrorist will claim responsibility for an assassination. For the most part, these acts are carried out against government officials, corporate executives, and security forces. This tab will assist the planner in identifying information for inclusion in the Incident Reaction Plan.

Critical Questions:

- Who is responsible for the counter-assassination program?
- What information should be included in the Incident Reaction Plan?
- What force will respond to an assassination incident?

Considerations:

- What terrorist groups employ assassination in this region?
- What historical documentation is available on terrorists methodology?
- What are the likely targets for assassination (VIPs and HRPs)?
- What special training is required for VIPs and HRPs?
- What special training is required for the response force?
- What special equipment is required for the response force?
- Where are the quarters/housing of VIPs and HRPs?
- Are they provided security details?
- Are they provide details during travel?
- How are their quarters secured?
- How are their offices secured?
- What IDS is employed?
- What special communications are required?
- Where is the duress signal located in their office/quarters?
- Who controls the adjacent buildings?
- Where is vehicle parking?
- How are the walls/windows protected?
- Do visiting HRPs have escort details?
- Who controls visiting HRP vehicles?
- What procedures have they employed enroute to the installation?

Tab 5: Assaults

Purpose :

Well planned assaults seldom fail. This is especially true of terrorist operations. They are generally well planned, properly rehearsed and precisely executed. Terrorists have an advantage in that they can choose their time and place of operations. The purpose of this tab is to assist the planner in preparing information for insertion into the Incident Reaction Plan.

Critical Questions:

- Who is responsible for planning for an assault incident?
- What is the reaction force(s)?
- What information should be included in the Incident Reaction Plan?

Considerations:

- What is the threat?
- What historical data available that will provide method of operations?
- What installation security measures are currently being employed?
- What IDS is available at the installation MEVA?
- Are barriers being used at installation MEVA?
- Is the lighting adequate at installation MEVA?
- What IDS is at the HRP office area?
- Is there a duress signal at the HRP office?
- What IDS is provided at the HRP quarters?
- Is there a duress signal at the HRP quarters?
- When traveling, who provides HRP with threat briefings?
- Does the HRP travel with escort?
- Does the installation HRP provide advance team prior to travel?
- What coordination is conducted with local law enforcement?
- Who is the installation first responder?
- What special equipment is required for security personnel?
- What special training is required for security personnel?

Tab 6: Kidnapping

Purpose :

Kidnapping is usually a covert seizure of one or more specific persons in order to extract specific demands. While similar to hostage taking, kidnapping has significant differences. Successful kidnapping requires elaborate planning and logistics. The risk to the terrorist is less than in the hostage situation. The perpetrator may not be known for a long time. While DOD targets may be perceived as more difficult to attack, they have and will continue to be targets of interest for terrorists. The purpose of this tab is to assist the planner in preparing information for insertion into the Incident Reaction Plan.

Critical Questions:

- Who is responsible for planning a response to kidnappings?
- What is the response force?
- How will this information be integrated into and coordinated with Incident Reaction Plan?

Considerations:

- How many kidnappings have occurred in the region?
- What terrorist group utilize kidnapping in this area?
- Are these terrorist groups anti-US?
- What historical data is available to provide method of operation?
- What special personnel are to be assembled ?
- What is the notification to higher headquarters?
- What coordination is in existence with Federal Law Enforcement?
- What coordination is in existence with Department of State?
- Who is responsible to coordinate with family members?
- Who is responsible to interface with media personnel?
- What communications is available for use by the response force?
- What MOUs or MOAs are prepared with foreign governments?
- Who has responsibility for negotiations?
- What special training and equipment are required?
- Who are the high risk personnel (HRP) on the installation?
- Where are their quarters?
- Are they provided security details? Are they provided details during travel?
- How are their quarters/offices secured?
- What IDS is employed?
- What special communications are required?
- Where is the duress signal located in their office/quarters?
- Do visiting HRPs have escort details?
- Where are HRP quarters?
- Who controls visiting HRP vehicles and travel routes?

Tab 7: Hostage & Barricade

Purpose :

Hostage & Barricade is usually an overt seizure of one or more individuals with the intent of gaining publicity or other concessions in return for release of the hostage. While dramatic, hostage and hostage barricade situations are risky for the perpetrator. Kidnapping and hostage-taking are similar, except the kidnapper is usually someone who confines the victim, while the hostage-taker confronts authorities and openly holds victims for ransom. The hostage-takers demands are often more than just material in nature. Political concessions are frequently demanded in exchange for lives. The USG policy on hostage negotiations is not to negotiate with terrorists, not to pay ransom, not to release prisoners, and not to submit to political blackmail. The purpose of this tab is to assist the planner in developing a response to a Hostage Barricade situation for inclusion in the Incident Reaction Plan.

The following priorities apply in hostage situations: Preservation of life, Hostages, Public, Security Police, Subject, Protection & Recovery of Property.

The three basic phases of hostage situations are immediate action, initial negotiation, and execution phases.

Critical Questions:

- Who is responsible for planning for hostage and barricade incidents?
- What information should be integrated into the Incident Reaction Plan?
- What is the reaction force(s) to a hostage and barricade situation?

Considerations:

- What is the threat?
- What historical data is available that will provide method of operations?
- Who is the installation first responder?
- What special equipment is required?
- What special training is required?
- Who interfaces with the primary counter-terrorist elements?
- Has a crisis management plan been established?
- Where is the communications equipment for the assault team location?
- Where is the assault team preparation area?
- What sniper teams are available?
- Where is the negotiation team located?
- Who is responsible to cordon off the area?
- Who controls the media?
- Has the installation identified those individuals on the installation who are high risk or VIPs who would be more likely to be targeted by a hostage-taker
- What IDS is at the HRP office area?
- Is there a duress signal at the HRP office?

Appendix 5: Consequence Management

CM is beyond the scope of this AT/FP Planning tool. Provided below are rudimentary planning considerations.

Purpose :

Consequence Management is a critical portion of the DOD response to terrorism. Installation commanders have the opportunity to plan consequence management in order to reduce the impact of terrorism on their community and the DOD. This appendix will assist the planner in preparing a Consequence Management Plan.

Background:

Installation commanders designate a specific office or selected staff to form a team to plan and coordinate the command's consequence management efforts during training and to serve as the operations center during training exercises and actual crises. Key members of this team should also be members of the preventive planning team, since they know the key infrastructures and assets critical to the installation's operation. To be successful, the team should be predesignated, so they can train together, and be prepared to perform individual and collective consequence management missions under the control of the installation commander or designated representative. Tenant commanders may also serve or have staff representation in this organization. The most common participants in the consequence management organization are listed in below.

Consequence Management Participants

- Command Staff
- Personnel
- Intelligence/Security
- Operations
- Counterintelligence
- Logistics
- Civil Affairs
- Major Tenant Commands
- Local Investigative Field Office
- Civilian Authorities/Representatives
- Federal, State, or Local
- Host Nation Police
- Special Staff Sections:
 - Military Law Enforcement Authorities
 - Command Legal
 - Public Affairs
 - Transportation
 - Aviation
 - Communications
 - Engineers/Utilities
 - Medical Activity/Red Cross
 - Chaplain
 - Psychologist
 - EOD

The following consequence management considerations, immediate disaster issues and cleanup issues will form the basis of a comprehensive Consequence Management Plan.

Critical Questions:

- What person(s), staff(s), or unit(s) is(are) responsible for consequence management?
- What CM product is the responsible entity to produce?
- How will the product be effectively integrated into the overall AT/FP Installation Plan?
- How will the plan be exercised?

Considerations:

- Where is the crisis center?
- What are alert notification procedures?
- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, material, and time will be needed to make these changes?
- Is equipment pre-positioned for CM?
- What equipment is available for search and rescue operations?
- Are confined space rescue personnel included in the on-call or alert roster?
- Where is HAZMAT located on the installation?
- What type of debris is expected to result in the destruction of any facility on the installation?
- Who is responsible for the removal of debris?
- Who is responsible for damage assessment?
- Who is responsible for utilities and lifeline repairs?
- What type of protective gear is available?
- Who is responsible for formulating clean up and containment teams?
- What actions have been taken to ensure that the area directly affected by the incident is safe enough for the return of the evacuated personnel or for the continued presence of those who did not evacuate the area?
- What provisions have been made to ensure that effects associated with a particular hazard do not prevent or impede the ability of response personnel to communicate with each other during response operations?
- What evacuation plans exist and who is responsible for them?
- What routes are available for evacuation?
- Are all roads mapped and rated for weight bearing capacity?
- Are transportation resources available to support mass evacuation?
- Who is responsible for the construction of emergency access routes?
- Are temporary shelters with food and first aid available in the event of a disaster?
- Are shelter locations outside the area vulnerable to the hazard?
- Are food and water stocks available to support extended stays (over 72 hours)?
- What special medicines does the installation have for potential injuries?
- What capability is available for decontaminating personnel exposed to hazardous materials?
- What personnel, supplies, and equipment exist to fight fires?
- When was the last fire drill, response, and evacuation conducted?
- Is the fire equipment ready?
- Who is responsible for repairing damaged energy sources?
- What interim energy sources are available?
- Who is responsible for resource allocation?
- What natural resources are in the area that might both hinder and aid in CM operations?
- Are blueprints available for all of the buildings on the installation?

Tab 1: Consequence Management Planning Tool:

Crisis management is an umbrella under which consequence management exists. The installation commander and staff will find an introductory overview of crisis management in Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," 25 June 1993, Chapter VI.

The following consequence management considerations, immediate disaster issues and cleanup issues will form the basis of a comprehensive Consequence Management Plan. ENTER the Installation's Consequence Management Plan here or include as an annex to this plan.

1. Consequence Management Considerations
 - a. Rescue
 - (1) Debris
 - (2) Fire
 - (3) Radiological
 - (4) Biological
 - (5) Chemical
 - b. Destruction
 - (1) Buildings
 - (2) Roads
 - (3) Natural Resources
 - (4) Utilities
 - (5) Littoral Areas and Inland Waterways
 - c. Fire fighting
 - d. Medical
 - e. Radiation
 - f. Explosive Ordnance Disposal
2. Immediate Disaster Issues
 - a. Containment
 - b. Evacuation and relocation of people
 - c. Debris and obstruction removal
 - d. Evaluation and re-establishment of natural resources and utilities
 - e. Monitoring plumes from fires
 - f. Radiation, biological, and chemical monitoring and advisory support to hospitals
 - g. Resource allocation, i.e., electrical power, petroleum products, and water
 - h. Water, food, and crops monitoring and supply
3. Clean-up Issues
 - a. Control the source
 - b. Identify and document radiological, biological, and chemical contamination
 - c. Identify critical pathways
 - d. Decontamination of the environment
 - e. Soil removal and disposal

Appendix 6: Executive or Distinguished Visitor Protection

Purpose :

The purpose of this appendix is to have a plan in place to provide additional protection to executive or high risk individuals against terrorist acts. Additional protection, increases the amount of time terrorists need to gain physical access to executives from the onset of hostile actions; and increases the interval of time between detection of a threat and the onset of hostile action. This plan should be integrated into the overall AT/FP Plan.

Critical Questions:

- What person(s), staff(s), or unit(s) is responsible for the protection of High Risk Personnel and executive or distinguished visitors?
- What system is in place to identify and track HRPs and VIPs?
- How is this plan integrated with the overall AT/FP Plan?

Considerations:

- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- What forces are available for protection?
- Who will conduct the protection details?
- Is the detail high visibility or low visibility?
- What is the purpose of the VIP visit?
- Where is the command post for VIP operations?
- How is the advance team organized?
- Who develops the intelligence information?
- Where is the VIP staying?
- How is the VIP traveling?
- What is the VIP itinerary?
- Who coordinated for emergency medical/support?
- What are the medical concerns of the VIP?
- Who has access to surrounding buildings at residence?
- Who has access to surrounding buildings at office complex?
- Has all emergency/security systems been tested at all buildings?
- Who will conduct roving patrols of HRP's and VIP's quarters/offices?
- Who prepares the routes and coordinates convoys?
- Who prepares the emergency evacuation procedures?
- Are all vehicles equipped with emergency equipment?
- What are the most cost-effective means of enhancing the security of executives at risk?
- With whom should the responsible officer or staff coordinate for protection services?
- How many changes in organizational routines and personal behaviors will have to be made in order for security measures to be effective in reducing risk of terrorist attack and the vulnerability of executives to such attacks?
- What are the anticipated costs of additional security measures in terms of dollars, organizational functionality, and the mission capability?
- Who is the focal point for training?
- What specialized equipment may be required?
- Who last tested response equipment (communications/flashlights/computers)?
- Does the accompanying VIP detail provide any equipment to installation team?
- When did the detail last rehearse/exercise?
- Have local authorities been notified of VIP visit?
- Does the installation need limited access or increased access controls?

Tab 1: High Risk Personnel Security Tools

1. INTRODUCTION. The actions of terrorism throughout the installations commanders AOR must be understood as a real possibility when planning visits of high ranking personnel as well as the travel of key installation personnel assigned within each perspective country. Planning for, hosting and safeguarding these officials are essential to the success of the installation mission and are a clear demonstration of America's positive presence.

2. APPLICABILITY. This Appendix applies to operations and personnel activities outside of the continental United States.

3. HIGH RISK PERSONNEL (HRP). Flag Officers and civilian equivalents traveling in the installation AOR are potential terrorist targets, as a result, they are classified as High Risk Personnel. Key elements in ensuring their security/safety are a thorough visit preparation and careful control of travel itinerary details.

a. Upon notification of an impending HRP visit, personal protection for the HRP must be addressed. The installation commander should designate a security POC for HRP visits to facilitate coordination and contact to the Embassy Regional Security Officer (RSO). The type of protection requested or desired by the HRP must first be ascertained (full protection, minimal, high profile, low profile, etc.). Any host nation security assistance should be requested through the RSO. Experience has shown that host nation agencies receiving distinguished visitors do not necessarily initiate protective security measures as a matter of course. Requests for such support, therefore, must be made through ROS channels.

b. If the installation is the host activity, it is responsible for arranging proper security. This will be accomplished by determining if there is a high threat requiring special protective measures. If the threat is not high, then ensure that:

- Accommodations obtained are secured.
- Driver and vehicle are obtained.
- Host national security forces are requested to provide security while the HRP is traveling, in quarters, visiting locations, and at social occasions. If the HRP is utilizing their own aircraft, ask for security to be provided to the aircraft.
- Personal Security Operations for the Installation Commander travel is the responsibility of the Command Provost Marshal. When commander travels outside of the installation facility the Provost Marshal's Personal Security Officer (PSO) will coordinate transportation and lodging security measures. The PSO will insure that proper coordination is accomplished.

c. If the threat is high, ensure HRP are informed of the threat so that changes to the trip itinerary can be made, if appropriate.

d. If travel is still scheduled, then:

- Recommend through HRP's command/detachment advisability of employing, U.S. security agents to assist in security operations.
- If U.S. security agents are used, protective service operations will be conducted in accordance with applicable DOD and service regulations.
- If U.S. security agents are not used, the host must arrange security for the HRP.

e. A basic security checklist should be utilized as a guideline in performing pre-visit security surveys. Advise the organization notifying of HRP intended visit of security arrangements made.

4. CONTROL OF INFORMATION RELATING TO HRP VISIT/ITINERARY. The vulnerability of HRP can be reduced by restricting access to their travel plans. Itineraries and other specific travel information should be controlled to the maximum extent practical to protect the HRP and prevent incidents. It is recognized that

travel must be coordinated with host governments, arrangements made for billeting, messing, and transportation, as well as other actions taken to facilitate passage of personnel and their baggage through customs and airport security.

a. Classification of Itinerary. Detailed travel itineraries of all HRP traveling anywhere within the installations AOR should be classified "CONFIDENTIAL" as a minimum. Detailed travel itineraries of CINC's/equivalent or uniquely special visitors should be classified "SECRET" when names/titles are associated with time/locations. Composite itineraries that contain complete schedules with arrival/ departure times and places, motorcade information, flight numbers or detailed billeting information should also be classified. Separate extracts, portions of the itinerary used to coordinate the visit should be treated as 'OFFICIAL USE ONLY' information and carefully controlled. In implementing the above guidance, the key words are "detailed travel itineraries" as opposed to limited extracts. Desk calendars, scheduled meetings, partial itineraries, and announced appearances do not have to be classified unless there is a specific threat to the HRP, the location, or the event.

b. For "unclassified" schedule or portions of itineraries for HRP, precautions should still be taken to avoid release of information earlier than necessary. Limit dissemination of details to those who have a need-to-know, and protect the FOUO information. Where available, utilize secure voice when HRP visit details are discussed by telephone. In some instances, face-to-face coordination of visit arrangements are preferred to written notification of sensitive details.

c. The necessity for release of HRP visit information to certain host nation agencies is, of course, recognized. However, every effort should be made to limit dissemination to those agencies directly supporting the HRP visit. Further, the intent of this policy is to limit the ability of terrorists to obtain information on an itinerary far enough in advance to plan an attack. Consequently, do not release information to host nation prematurely. Rather, necessary information should be released as late as practical for the circumstances unique to each country.

d. Although all-inclusive rules to fit every occasion are impractical, the following conditions generally increase the need to classify an itinerary:

- Receipt of specific threat information.
- Extensive HRP involvement in non-U.S. sponsored activities
- HRP attendance at highly publicized or high profile events.
- Availability of information well before the visit.
- HRP schedules that provide detailed information covering several days' activities.

e. Where unique circumstances exist which preclude the proper and expeditious in-house handling of HRP itineraries, requests for waiver of requirements should be submitted installation commander and the RSO.

5. USE OF ARMORED VEHICLES. Armored vehicles are to provide protection to key individuals and to afford the greatest flexibility in protecting other potential targets. DOD policy is remised on maintaining current inventory levels and, thus authorizes replacement of current vehicles as necessary. DOD policy also recognizes that commercially-produced, fully-armored or Heavy Armored Vehicles (HAVS) are scarce and costly resources that must be carefully managed. A light armored non-tactical vehicle or Light Armored Vehicle (LAV) is not as costly but does not afford the level of protection provided by a HAV. It must be recognized that the acquisition of hardened vehicles requires significant lead time and hardened vehicles (both HAV and LAN) are costly. The speed in which terrorist threat can escalate makes it almost impossible to quickly obtain a hardened vehicle when the country terrorist threat increases. Therefore, if possible, each installation should possess and utilize at least one hardened vehicle as part of their vehicle fleet. If the daily Terrorist Threat condition is high, installation should consider maintaining more than one hardened vehicle.

a. Armored vehicles will be used solely for protection of officials in the performance of their duties

and/or at other items on the basis of specific threat assessments and vulnerability assessments which have been coordinated with the theater higher HQ.

- b. Requests for HAVs require a detailed justification to include the following information:
 - Manpower position the vehicle is intended for.
 - Current/projected threat and vulnerability assessment.
 - Current armored vehicle assets available.
 - Whether request is a new, requirement or to replace an existing vehicle.
 - Why a LAV would not be appropriate.
 - Funding availability.

- c. Requests for a LAV will include the following information:
 - Manpower position the LAV is intended for.
 - Current projected threat and vulnerability assessment.
 - What type vehicle is the armored car kit is to be placed on (year, make , model, transmission type, whether vehicle has heavy duty radiator/suspension).
 - Whether vehicle is in-country or being procured and shipped.
 - Current armored vehicle assets available.
 - Whether request is for a new requirement or to replace an existing one.
 - Funding availability.

- d. Disposal of HAVs/LAVs will be accomplished in accordance with DOD C-4500.51 and coordinated with the Embassy- Regional Security Officer.

Appendix 7: Operations Security

Purpose :

From the outset, it should be noted that one of the principal building blocks of a successful antiterrorism program is Operations Security (OPSEC). We must understand that preserving vital installation information from the adversary can mean the difference between a precisely targeted facility component, a random symbolic act, or no terrorist act at all.

The objectives of OPSEC as they pertain to AT/FP are:

- (1) Deny intelligence and information to terrorists.
- (2) Avoid rigid operational routines
- (3) Be familiar with techniques used by terrorists to collect information.
- (4) Integrate operations security into physical security and personal protection programs.
- (5) Develop essential elements of friendly information to facilitate and focus efforts to deny information to terrorists.

OBJECTIVES

Background:

OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: (a) identify those actions that can be observed by an adversary intelligence systems; (b) determine what indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; and (c) select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

The installation's threat assessment may reveal security weaknesses in day-to-day-operations. The installation should examine the security of communications systems, information activities, and personnel. Then it should correct any weaknesses, based on available resources, corrected to include countersurveillance techniques when necessary. Information gleaned from communications can provide terrorists with detailed knowledge about potential targets. Communications security is an integral part of OPSEC. Terrorists are not hampered by regulations and fully exploit opportunities presented to them.

Critical Questions:

- Who is the responsible individual, staff, or unit for OPSEC planning?
- How is the OPSEC plan disseminated to the installation?
- What is the desired OPSEC product to be integrated into the AT/FP Installation Plan?

Considerations:

- What is the threat?
- What are the adversary's goals?
- What are the adversary's intelligence collection capabilities?
- What have been their actions to date?
- What is the mission of the installation?
- What is the mission of each unit?
- Is OPSEC applied to daily operations?
- What is the current status of the OPSEC plan?
- When was the OPSEC plan last evaluated?
- What are the reporting procedures for OPSEC violations?
- What target(s) have been identified by the Vulnerability and Criticality Assessment?
- Are there any major activities that deserve special considerations?
- Who conducts OPSEC briefings and procedures to civilian personnel?
- What measures can the installation employ to improve OPSEC?

Tab 1: Examples Of Indicators (Tool)

The following paragraphs provide examples of indicators that are associated with selected military activities and information. This short list only scratches the surface of the almost infinite sources of indicators associated with the wide range of US military operations and activities that could be exploited by an adversary. This list is designed primarily to stimulate thinking about what kinds of actions can convey indicators that betray critical information for specific friendly operations or activities.

Indicators of General Military Force Capabilities:

- The presence of unusual type units for a given location, area, or base.
- Friendly reactions to adversary exercises or actual hostile actions.
- Actions, information, or material associating Reserve components with specific commands or units (e.g., mobilization and assignment of Reserve personnel to units).
- Actions, information, or material indicating the levels of unit manning as well as the state of training and experience of personnel assigned.
- Actions, information, or material revealing spare parts availability for equipment or systems.
- Actions, information, or material indicating equipment or system reliability (e.g., visits of technical representatives or special repair teams).
- Movement of aircraft, ships, and ground units in response to friendly sensor detection's of hostile units.
- Actions, information, or material revealing tactics, techniques, and procedures employed in different types of training exercises or during equipment or system operational tests and evaluations.
- Stereotyped patterns in performing the organizational mission that reveal the sequence of specific actions or when they are accomplished.

Indicators of General C2 Capabilities:

- Actions, information, or material providing insight into the volume of orders and reports needed to accomplish tasks.
- Actions, information, or material showing unit subordination for deployment, mission, or task.
- Association of particular commanders with patterns of behavior under stress or in varying tactical situations.
- Information revealing problems of coordination between the commander's staff elements.
- In exercises or operations, indications of the period between the occurrence of a need to act or react and the action taking place, of consultations that occur with higher commands, and of the types of actions initiated.
- Unusual actions with no apparent direction reflected in communications.

General Indicators from Communications Usage:

- Alert and maintenance personnel using hand held radios or testing aircraft or vehicle radios.
- Establishing new communications nets.
- These might reveal entities that have intrinsic significance for the operation or activity being planned or executed.
- Without conditioning to desensitize adversaries, the sudden appearance of new communications nets could prompt them to implement additional intelligence collection to discern friendly activity more accurately.
- Suddenly increasing traffic volume or, conversely, instituting radio silence when close to the time of starting an operation, exercise, or test. Without conditioning, unusual surges or periods of silence may catch adversaries' attention and, at a minimum, prompt them to focus their intelligence collection efforts.
- Using static call signs for particular units or functions and unchanged or infrequently changed radio frequencies. This usage also allows adversaries to monitor friendly activity more easily and add to their intelligence data base for building an accurate appreciation of friendly activity.
- Using stereotyped message characteristics that indicate particular types of activity that allow adversaries to monitor friendly activity more easily.
- Requiring check-in and checkout with multiple control stations before, during, and after a mission (usually connected with air operations).

Sources of Possible Indicators for Equipment and System Capabilities:

- Unencrypted emissions during tests and exercises.
- Public media, particularly technical journals.
- Budget data that provide insight into the objectives and scope of a system research and development effort or the sustainability of a fielded system.
- The equipment or system hardware itself.
- Information on test and exercise schedules that allows adversaries to better plan the use of their intelligence collection assets.
- Deployment of unique units, targets, and sensor systems to support tests associated with particular equipment or systems.
- Unusual or visible security imposed on particular development efforts that highlight their significance.
- Information indicating special manning for tests or assembly of personnel with special skills from manufacturers known to be working on a particular contract.
- Notices to mariners and airmen that might highlight test areas.
- Stereotyped use of location, procedures, and sequences of actions when preparing for and executing test activity for specific types of equipment or systems.
- Use of advertisements indicating that a company has a contract on a classified system or component of a system, possesses technology of military significance, or has applied particular principles of physics and specific technologies to sensors and the guidance components of weapons.

Indicators of Preparations for Operations or Activities: Many indicators may reveal data during the preparatory, as compared to the execution, phase of operations or activities. Many deal with logistic activity.

- Provisioning of special supplies for participating elements.
- Requisitioning unusual volumes of supply items to be filled by a particular date.
- Increasing proportioning of ammunition, fuels, weapon stocks, and other classes of supply.
- Embarking special units, installing special capabilities, and preparing unit equipment with special paint schemes.
- Procuring large or unusual numbers of maps and charts for specific locations.
- Making medical arrangements, mobilizing medical personnel, stockpiling pharmaceuticals and blood, and marshaling medical equipment.
- Focusing friendly intelligence and reconnaissance assets against a particular area of interest.
- Requisitioning or assigning increased number of linguists of a particular language or group of languages from a particular region.
- Initiating and maintaining unusual liaison with foreign nations for support.
- Providing increased or tailored personnel training.
- Holding rehearsals to test concepts of operation.
- Increasing the number of trips and conferences for senior officials and staff members.
- Sending notices to airmen and mariners and making airspace reservations.
- Arranging for tugs and pilots.
- Requiring personnel on leave or liberty to return to their duty locations.
- Having unusual off-limits restrictions.
- Preparing units for combat operations through equipment checks as well as operational stand downs in order to achieve a required readiness level for equipment and personnel.
- Making billeting and transportation arrangements for particular personnel or units.
- Taking large-scale action to change mail addresses or arrange for mail forwarding.
- Posting such things as supply delivery, personnel arrival, transportation, or ordnance loading schedules in a routine manner where personnel without a need-to-know will have access.
- Storing boxes or equipment labeled with the name of an operation or activity or with a clear unit designation outside a controlled area.
- Employing uncleared personnel to handle materiel used only in particular types of operations or activities.

- Providing unique or highly visible physical security arrangements for loading or guarding special munitions or equipment.
- Requesting unusual or increased meteorological, oceanographic, or ice information for a specific area.
- Setting up a wide-area network (WAN) over commercial lines.

Sources of Indicators During the Execution Phase:

- Unit and equipment departures from normal bases.
- Adversary radar, sonar, or visual detection's of friendly units.
- Friendly unit identifications through COMSEC violation or physical observation of unit symbology.
- Force composition and tracks or routes of advance that can be provided by emissions from units or equipment and systems that provide identifying data.
- Stereotyped procedures; static and standard ways of composing, disposing, and controlling strike or defensive elements against particular threats; and predictable reactions to enemy actions.
- Alert of civilians in operational areas.
- Trash and garbage dumped by units or from ships at sea that might provide unit identifying data.
- Transportation of spare parts or personnel to deploying or deployed units or via commercial aircraft or ship.
- Changes in oceanography high frequency facsimile transmissions.
- Changes in the activity over WAN.

Indicators of Post-engagement Residual Capabilities:

- Repair and maintenance facilities schedules.
- Urgent calls for maintenance personnel.
- Movement of supporting resources.
- Medical activity.
- Unusual resupply and provisioning of an activity.
- Assignment of new units from other areas.
- Search and rescue activity.
- Personnel orders.
- Discussion of repair and maintenance requirements in unsecured areas.
- Termination or modification of procedures for reporting of unclassified meteorological, oceanographic, or ice information.

Appendix 8: Access Controls

Purpose :

An access control plan should include pedestrian, vehicle, and mail/package access to the installation. This plan should be maintained by the proper security forces to ensure employment of the proper measures at all times. Access controls principally delay an adversary from reaching protected areas and inhibit egress from the installation. Access controls increase the amount of time needed to move from one point in the installation to another point on the installation. Access control systems aid in containing and resolving AT/FP incidents.

Background:

A positive control system must be established and maintained to preclude unauthorized entry and theft, and to facilitate authorized entry at personnel control points. Access lists, personal recognition, security identification cards and badges, badge exchange procedures, and personnel escorts contribute to the effectiveness of movement control systems.

The best control is provided when systems incorporate all these elements. Simple, understandable, and workable identification and movement control procedures should be used to achieve security objectives without impeding efficient operations. Properly organized and administered, a personnel and movement control system provides a means not only of positively identifying those who have the right and need to enter or leave an area, but also of detecting unauthorized personnel who attempt to gain entry.

Specific standards for access control can be found in FM 19-30, Chapter 4 (Army).

Specific standards for access control can be found in AFI 31-101, Chapter 5 (Air Force).

Specific standards for access control can be found in DOD 2000.12-H, Chapter 10, Paragraph D, Page 10-10 (DOD).

For background information of installation command and staff officers with AT/FP interest, See Joint Pub 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism," 25 June 1993, Appendix N.

Tab 1: Pedestrian Access Control

Critical Questions:

- What person, staff, or unit is responsible for the pedestrian access control?
- Who integrates this plan into the overall AT/FP Plan?
- What forces are tasked with manning pedestrian entry points?
- Where is the access control plan located/found/attached?

Considerations:

- What is the current status of the access system?
- What is the desired end state?
- What modifications/new starts must be made to enhance security?
- With whom should the guard post be in contact during increased THREATCONs?
- What improvements will be made during increased THREATCON?
- What forces are required to make these improvements?
- From where will the resources come?
- How many gates allow access to the installation?
- What gates will be changed during increased THREATCONs?
- How many guards are present at each gate during various THREATCONs?
- What equipment should be at the guard post?
- To what specification should the guard post be modified?
- Where do you place warning signs?
- What do the warning signs say?
- Is the host nation language considered?
- How often do you test your pedestrian access control system?
- When do the lights activate?
- Are the lights automatic or manual?
- How does the guard post activate the response element?
- Where is the response element located?
- Where are the sensors located?
- Where are the cameras located?
- Who inspects the system?
- Who is called for immediate repairs?
- What locking mechanisms are employed on the pedestrian accesses?
- What are the standard work/duty hours?
- Are there restrictions in place during the various THREATCONs as to who is allowed access to the installation after duty hours?
- Are alarms used in the pedestrian access system?
- Are sensors used in the pedestrian access system?

Enclosure 1: Personnel Movement Control Tools

Perimeter barriers, intrusion detection devices and protective lighting provide physical security safeguards; however, they alone are not enough. A positive personnel movement control system must be established and maintained to preclude unauthorized entry, and to facilitate authorized entry at personnel control points. Access lists, personal recognition, security identification cards and badges, badge exchange procedures, and personnel escorts contribute to the effectiveness of movement control systems.

The best control is provided when systems incorporate all these elements. Simple, understandable, and workable identification and movement control procedures should be used to achieve security objectives without impeding efficient operations. Properly organized and administered, a personnel and movement control system provides a means not only of positively identifying those who have the right and need to enter or leave an area, but also of detecting unauthorized personnel who attempt to gain entry.

Identification of Personnel

Purpose of Movement Control and Identification:

- a. Prevent introduction of harmful devices, materiel, or components.
- b. Prevent misappropriation, pilferage, or compromise of materiel or recorded information by means of: Package, Materiel, & Property Movement Control.
- c. This prevention is accomplished through:
 - (1) Initially determining who has a valid requirement to be in an area.
 - (2) Limiting access to those persons who have that valid requirement.
 - (3) Establishing procedures for positive identification of persons within, and of persons authorized access into, areas.
 - (4) Issuing special identification cards or badges to personnel authorized access into restricted areas.
 - (5) Using access lists.
 - (6) Using identification codes.
 - (7) Using duress codes

Identification System:

- a. An identification (ID) system should be established at each installation or facility to provide a means of identifying all military personnel, civilian employees, and visitors. The system should provide for the use of security identification cards or badges to aid in control and movement of personnel into, within, and out of specified areas or activities.
- b. Standard identification media may be prescribed for personnel by installation or facility commanders as valid identification for access to areas that are basically administrative in nature, contain no security interest, and are not in the restricted area category.
- c. Personnel requiring access to restricted areas should be issued a security identification card or badge. The identification card or badge should be designed as simply as possible and still provide for adequate control of the movement of personnel.
- d. Provisions for identification by card or badge control at an installation or facility should be included as part of the physical security plan.

Card and Badge System:

- a. A security identification card or badge system should be established to admit and control the movement of all persons admitted to restricted areas employing 30 or more persons per shift. However, the commander may authorize a card or badge system in restricted areas where less than 30 persons per shift are employed.
- b. Of the several identification systems used in access control, three of the most commonly used are the single card or badge system, the card or badge exchange system, and the multiple card or badge system. These ID systems may be used either for cards carried on the person or for cards or badges worn on outer clothing.

c. A system may be established (in an appropriate situation) for issuance of identification cards or badges at the main entrance to an installation. Such a system can be used for visitors and similar personnel.

Single Card or Badge:

- a. With this system, permission to enter specific areas is shown by letters, numerals, or colors. It has a major limitation--loose control. The opportunity for alteration or duplication is high.
- b. This system gives comparatively loose control and is not recommended for security areas. Permission to enter does not always go with the need to know, and the fact that ID cards and badges frequently remain in the bearer's possession during off duty or off post hours gives the opportunity for alteration or duplication.

Card or Badge Exchange:

- a. In this system, two items contain identical photographs but different background colors, or one item has an overprint. One is presented at the entrance to a specific area and exchanged for the other, which is carried or worn while in that area. Individual possession upon issuance is only in the area, to decrease the possibility of forgery or alteration.
- b. This method provides extra security by having both photographs identical. In this type of system, the second badge or card is kept in the security area and never leaves the area.

Multiple Card or Badge:

- a. Instead of having specific markings on the ID card or badge denoting permission to enter various restricted areas, the multiple card or badge system makes an exchange at the entrance to each security area within the installation. Exchange cards or badges are kept at each area for only those individuals who have the appropriate card or badge. By virtue of the localized and controlled exchange requirements, this is the most secure and effective system.
- b. Card and badge data are identical and must be so to allow comparisons.

Enforcement Measures:

The most vulnerable link in any identification system is its enforcement. Perfunctory performance of duty by the security forces in comparing the bearer with the card or badge may weaken or destroy the effects of the most elaborate system. Positive enforcement measures should be prescribed to insure effective operation of the personnel and identification system. These should include, but not be limited to the following:

- a. Security personnel designated for duty at entrance control points should be chosen for their alertness, quick perception, tact, and good judgment.
- b. Formalized, standard procedures for conducting assemblies, posting, and relief of personnel, and frequent inspection of personnel on post at irregular times are effective means to preclude posting of unqualified personnel and perfunctory performance of duty.
- c. A uniform method of handling or wearing security ID cards or badges should be prescribed. If carried on the person, the card must be removed from the wallet or other container and handed to security personnel. A badge should be worn in a conspicuous position to expedite inspection and recognition from a distance.
- d. Entrances and exits of restricted areas should be arranged so that arriving and departing personnel are forced to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control of entrance and exit.
- e. Artificial lighting at the control points should be arranged so that it illuminates the arriving and departing personnel and should be of sufficient intensity to enable security personnel to compare and identify the bearer with the ID card or badge.
- f. Enforcement of access control systems rests primarily on the installation security forces. However, it is essential that they have the full cooperation of the employees, who should be educated and encouraged to assume this security responsibility. Employees should be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to particular zones, employees should report movement of individuals to unauthorized zones.

- g. Identification card and badge racks or containers used at control points for an exchange system should be positioned so they are accessible only to guard personnel.
- h. A responsible custodian should be appointed by competent authority to accomplish control procedures, turn in, recovery, or expiration of security ID cards and badges. The degree of compromise tolerable in the identification system is in direct proportion to the degree of security required or indicate

Visitor Identification And Control:

- a. Physical security precaution against pilferage, espionage, and sabotage requires screening, identification, and control of visitors. Visitors are generally in the following categories:
 - (1) Persons with whom every installation or facility must have dealings in connection with the conduct of its business, such as representatives of suppliers, customers, licensors or licensee, insurance inspectors or adjusters, government inspectors (national, state, and local), service industry representatives, contractors, employees, etc.
 - (2) Individuals or groups who desire to visit an installation or facility for a purpose not essential to, or necessarily in furtherance of, the operations of the installation or facility concerned. Such visits may be desired, for example, by business, educational, technical, or scientific organizations and individuals or groups desiring to further their particular interests.
 - (3) Individuals or groups specifically sponsored by government agency organizations such as foreign nationals visiting under technical cooperation programs and similar visits by US nationals.
 - (4) Individuals and groups who the government generally encourages but does not specifically sponsor, because of the contribution they make to economic and technical progress or to defense production in the United States and/or in friendly nations.
 - (5) Guided tour visits to selected portions of installations in the interest of public relations.
- b. Arrangements for identification and control of visitors may include the following:
 - (1) Positive methods of establishing the authority for admission of visitors, as well as any limitations relative to access.
 - (2) Positive ID of visitors by means of personal recognition, visitor permit, or other identifying credentials. The employee, supervisor or officer in charge should be contacted to ascertain the validity of the visit.
 - (3) Availability and use of visitor registration forms and records that will provide a record of identity of the visitor, time and duration of his visit, and other pertinent control data.
 - (4) Availability and use of visitor ID cards or badges. Such identification media should be numbered serially and indicate the following: bearer's name; area(s) to which access is authorized; escort requirements, if any; time limit for which issued; signature (or facsimile). photograph, if desired and available. procedures which will insure supporting personal identification in addition to check of visitor cards or badges at restricted area entrances.
 - (6) Procedures for escorting visitors having limitations relative to access through areas where an uncontrolled visitor, even though conspicuously identified, could acquire information for which he is not authorized. Foreign national visitors should be escorted at all times.
 - (7) Controls which will recover visitor ID cards or badges on expiration, or when no longer required.
 - (8) Twenty-four hour advance approval when possible. Where appropriate, the installation should prepare an agenda for the visit and designate an escort officer.

Security Personnel At Entry and Exit Points:

The security manager responsible for these individuals must insure that the personnel:

- a. Are alert, perceptive, tactful, and capable of exercising sound judgment in executing their duties and responsibilities.

b. Conduct frequent, irregular checks of their assigned areas during periods of inactivity (holidays, weekends, and after-duty hours).

Tab 2: Vehicle Access Control

Critical Questions:

- What person, staff, or unit is responsible for the vehicular access control plan?
- What forces are assigned to man the vehicle access points?

Considerations:

- What vehicles are allowed on base?
- Are there changes to this plan based on the THREATCON?
- How often is this system changed?
- What system will be used to identify installation vehicles?
- Will this be a visual decal, a verbal exchange, or ID check?
- Who will activate the changes during the THREATCON Status?
- If additional forces are required, from where will they come?
- Who has the roster for registered vehicles?
- What process has been established for checking additional vehicles?
- What vehicles are allowed into what areas?
- Where is parking for employees?
- Where is parking for visitors?
- Where is parking for deliveries?
- Are military working dogs employed for vehicle inspection?
- Are guards armed?
- What ROE policy is in effect?
- Is a mechanism in place to preclude entry through the egress point (reverse-entry attempts)?
- Where are warning signs posted?
- If in OCONUS are translators available?

Enclosure 1: Vehicle Control Tools

Vehicle Control

- a. All privately owned/visitor-operated motor vehicles on the installation should be registered with the provost marshal or the installation physical security office. Requirement to display a tag or decal should be IAW Installation requirements.
- b. Vehicles belonging to visitors should be identified by a temporary decal or identification media different from permanent registration to permit ready recognition by security personnel.
- c. When authorized vehicles enter or exit a restricted area, each must undergo a systematic search, including, but not limited to, the following areas: interior, engine compartment, external air breathers, top of vehicle, battery box, cargo compartment, and undercarriage.

Truck and Railroad Car Control

- a. Movement of trucks and railroad cars into and out of installations or facilities should be supervised and each inspected to prevent the entry or removal of unauthorized persons or materiel. Inspectors should be especially watchful for explosives or incendiaries.
- b. Truck and railroad entrances should be controlled by locked gates when not in use, and should be under security supervision when unlocked or opened for passage.
- c. Identification cards or badges should be issued to operators of trucks and railroad engines to insure proper identification and registration of those entering and leaving the area. Such cards or badges should permit access only to specific loading and unloading areas.
- d. All conveyances entering or leaving a protected area should be required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and vehicle contents should be carefully examined. The security check should include: Appropriate entries in security log, date, operator's name, description of load, time entered and departed. License check of operator. Verify seal number with shipping document and examine seal for tampering.
- e. Incoming trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas. Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated restricted areas to discharge or pick up cargo. Escorts should be provided when necessary.

Tab 3: Mail and Package Controls

Critical Questions:

- What person, staff, or unit is responsible for mail and package control?
- What procedures should be integrated into the overall access control plan?

Considerations:

- What improvements will be made during increased THREATCON?
- Who will make those improvements?
- Where are the regulations for admission of materials and supplies?
- What special controls on delivery of supplies to restricted areas exist?
- What are the regulations or special controls on delivery of supplies to restricted areas?
- Are military working dogs employed for package inspection?
- How are classified shipments to be handled?
- What procedures are in place for delivery of personal items?
- What technological solutions are available to assist mail and package control?
- What procedures are in place for classified materials?
- What agreement is in place with the local postal system?
- How does the local postal system get mail onto the installation normally?
- How does the local postal system get mail onto the installation during increased THREATCON?
- What information has been given to dependents on mail screening at home?

Enclosure 1: Package Control Tools:

Package Control

- a. A good package control system helps prevent or minimize pilferage, sabotage and espionage. Only packages with proper authorization should be permitted into restricted areas without inspection.
- b. A positive system should be established to control movement of packages, materiel, and property into and out of the installation.
- c. A package checking system, using Individual Property Pass or a similar form, may be used at the entrance gate for the convenience of employees and visitors. When practicable, inspect all outgoing packages except those properly authorized for removal. When 100 percent inspection is impractical, conduct frequent unannounced spot checks.

Property Controls

- a. Property controls must not be limited to packages carried openly; but must include control of anything that could be used to secret property or materiel of any type.
- b. Persons should not be routinely searched except in unusual situations. When they are, it should be only in accordance with published command directives.

Enclosure 2: Letter And Package Bomb Recognition Checklist (Tool)

The following information is useful in detecting the presence of letter or package bombs sent through US and international mails. While by no means complete or foolproof, letters and packages exhibiting the characteristics below should be considered as potential Improvised Explosive Devices (IEDs).

WEIGHT

- weight unevenly distributed
- heavier than usual for its size
- heavier than usual for its postal class

STAMPS

- more than enough postage

POSTMARK

- foreign from an unusual city

THICKNESS

- for medium size envelopes, the thickness of a small book
- not uniform or has bulges
- for large envelopes, bulkiness, an inch or more in thickness

WRITING

- foreign writing style
- misspelled words
- marked "air mail," "registered," "certified," or "special delivery" certified," or "special delivery"

ADDRESS

- marked "personal," "private," or "eyes only"
- confidential"
- no return address
- poorly typed or handwritten address
- hand printed
- title for the recipient incorrect
- addressed to a high-ranking recipient by name, title, or department

ENVELOPE

- peculiar odor
- oil stains
- inner sealed enclosure
- excessive sealing material
- wire, string, or foil sticking
- ink stains

RIGIDITY

- springiness
- greater than normal, particularly along its center length

(From DOD 0-2000.12-H.)

Appendix 9: Barriers

Purpose :

The Barrier Plan should include pedestrian, vehicle, and visual barriers to control, deny, impede, delay and discourage access to restricted and non-restricted areas by unauthorized persons. This plan should be maintained by the proper security forces to ensure employment of the proper measures at all times.

The plan should:

- Define the perimeter of restricted areas.
- Establish a physical and psychological deterrent to entry as well as providing notice that entry is not permitted.
- Optimize use of security forces.
- Enhance detection and apprehension opportunities by authorized personnel in restricted and non-restricted areas.
- Channel the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

Background:

Physical barriers delay, but can rarely be depended upon to stop a determined intruder. Therefore, to be effective, such barriers must be augmented by security force personnel or other means of protection. In determining the type of barrier required, the following should be considered:

- Physical barriers will be established around all restricted areas. The type of barrier to be used will be determined after a study of local conditions. The barrier or combination of barriers used must afford an equal degree of continuous protection along the entire perimeter of the restricted area. When a section or sections of natural or structural barriers (or the lack thereof) provide a lesser degree of protection, other supplementary means to detect and assess intrusion attempts must be used.
- In cases of a high degree of relative criticality and vulnerability, it may be necessary to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 30 feet (9.14 meters) for optimum protection and control. Two lines of barriers will only be used either in conjunction with an intrusion detection system between the fences or on the inside fence, or some other form of alarm system and a security force capable of immediate response. The use of two barriers alone provides little extra protection beyond a few seconds of delay to a determined intruder and may actually be counter productive in identifying the location of high risk items.
- The perimeter boundaries of all installations or separate activities will be either fenced or walled and posted to establish a legal boundary. This defines the perimeter, provides a buffer zone, facilitates control and makes accidental intrusion unlikely. It is important that consultation be made with local authorities to ensure that posting of barriers in areas of concurrent or proprietary jurisdiction complies with local or state trespass laws.
- In establishing any perimeter or barrier, consideration must be given to providing emergency entrances and exits in case of fire. However, openings will be kept to a minimum consistent with the efficient and safe operation of the facility and without degradation of minimum security standards.
- Water boundaries present special security problems. Such areas should be protected by material or structural barriers, and posted. In addition to barriers, patrol craft should be used at activities or installations whose waterfronts contain critical assets, restricted areas, or which are otherwise essential to the mission of the installation or activity. In inclement weather, such patrols cannot provide an adequate degree of protection and should be supplemented by increased waterfront patrols.

Enclosure 1: Barrier Tools

1. Does the fenced portion of the installation/ restricted area barrier meet minimum specifications for security fencing?
 - a. Is it of chain link (cyclone) composition?
 - b. What gauge wire?
 - c. Is the mesh opening no larger than two inches?
 - d. Are reinforcing wires interwoven at top and bottom of fence?
 - e. Is the bottom of the fence within two inches of solid ground?
 - f. Is the top guard strung with barbed wire (or barbed tape/razor edge) and angled outward away from protected site and upward at a 45 degree angle?
2. Does the activity provide for security force inspection of the security barrier, including clear zones, at least once per month? Are deficiencies noted and are remedial actions promptly effected?
3. If masonry wall is used, does it meet minimum specifications for security fencing?
4. If building walls, floors and roofs form a part of the barrier, do they provide security equivalent to that provided by a chain link fence?
5. Are all openings properly secured?
6. If a building forms a part of the barrier, does it present a potential penetration hazard at the point of juncture with the perimeter security fence?
7. If a body of water forms any part of the barrier, are additional security measures provided?
8. Are openings such as culverts, tunnels, manholes for sewers and utility access, and sidewalk elevators that permit access to the installation and restricted area properly secured?
9. Are all portals in perimeter barriers guarded or secured?
10. Do gates and/or other entrances in perimeter barriers exceed the number required for safe and efficient operation?
11. Are all perimeter barrier portals equipped with secure locking devices? Are they locked when not in use?
12. Do all gates provide protection equivalent to that provided by the barrier of which they are a part?
13. Are barrier gates and/or other entrances which are not in active use locked and frequently inspected by guards or other personnel?
14. Are locks to all gates, active and inactive, rotated at least annually?
15. Does the security officer provide adequate protection and accountability of keys to security barrier entrances? If not, specify responsible individual or office.
16. Are keys to barrier entrances issued to other than installation personnel?
17. Are automobiles permitted to park within clear zones?
18. Are prescribed clear zones maintained on both sides of the restricted area barriers?
19. If clear zone requirements cannot be met, have compensatory security measures been implemented? Have waivers or exceptions been obtained or initiated for obstacles within clear zones that are not considered cost effective to relocate?
20. Are lumber, boxes or other extraneous material allowed to be stacked against or adjacent to the barrier or within established clear zones?
21. Are adequate interior all-weather security roads provided for the use of security patrol vehicles?
22. If security patrols or other security activities along the perimeter have been changed since the last survey, specify the change.
23. Have any additional barriers been installed or has any relocation thereof been accomplished since the last survey? If so, briefly describe:
24. Does any relocated function, newly designated restricted area, physical expansion, or other factor indicate necessity for installation of additional barriers or additional perimeter lighting? If so, briefly explain what action has been taken or is planned.

Specific standards for protective barriers can be found in FM 19-30, Chapter 5 (Army).

Specific standards for protective barriers can be found in AFI 31-101, Chapter 7, Pages 49 through 52 (Air Force).

Specific standards for protective barriers can be found in DOD 2000.12-H,

Tab 2: Pedestrian Barriers

Critical Questions:

- What person, staff, or unit is responsible for the pedestrian barriers?
- What type of information regarding pedestrian barriers should be integrated into the overall barrier plan?

Considerations:

- How many acknowledged pedestrian access points are there?
- Are there other locations around the perimeter that a pedestrian could enter the facility?
- What type of barriers are currently in use?
- How many intrusions have occurred in the past year/month?
- Are there holes in the perimeter fencing?
- Are there waterways accessing the installation?
- What is the normal flow of pedestrian traffic?
- What is the current state of the guard force?
- Are access restriction signs posted?
- Are the signs translated into the local language?
- What mechanisms are in place to slow or reduce the flow of pedestrian traffic?
- What improvements will be made during increased THREATCON?
- Who will make those improvements?
- Where are barriers stored?
- How many barriers are currently on the installation?
- Have plans been developed to account for the number of barriers that will be needed during increased THREATCON?

Tab 3: Vehicle Barriers

Critical Questions:

- Who is responsible for the Vehicle barrier plan?
- What is the product that the responsible office will produce?

Considerations:

- Who plans for a vehicle barrier?
- What type of vehicle barrier is required?
- What type of vehicle barrier is available to the installation?
- What improvements will be made to the vehicle barrier plan under increased THREATCON status?
- Where will the material come from to make these changes?
- What forces will be assigned to implement improvements to the barrier plan?
- Where do you place the vehicle barrier?
- Who inspects the vehicle barrier?
- Who maintains the vehicle barrier?
- Who mounts the surveillance equipment on the vehicle barrier?
- What height are the barriers?
- What thickness of barrier?
- What type of topping will be placed on the barrier?
- What kind of paint on the vehicle barrier?
- When do you need a vehicle barrier (day/night)?
- When do you patrol the vehicle barrier?
- When do you check the vehicle barrier for maintenance?
- When do you replace sections or all of the vehicle barrier?
- Where do you place the sensors?
- Where do you put guards?
- Where can you build near a vehicle barrier?
- Where do you place lights?

Enclosure 1: Vehicle Barrier Tool

The following type of barriers should be considered when planning a vehicle barrier system.

Barrier Types

- Active Barrier Systems
- Passive Barrier Systems
- Fixed Barrier System
- Movable Barrier System
- Portable Barrier System
- Expedient Barrier System

To best utilize a vehicle barrier system many considerations should be analyzed before deploying barriers.

Vehicle Barrier Design Considerations

- Location
- Safety
- Reliability
- Maintainability
- Cost
- Active Barrier Operations
- Clear Zones
- Operating Environment
- Installation Requirements
- Operator Training
- Aesthetics

Tab 4: Fences

Critical Questions:

- Who maintains and plans improvements to the perimeter fence?
- Who inspects the fence?
- What type of fence is required?
- What information should be integrated into the overall AT/FP Plan?

Considerations:

- What type of system will be used on the top of the fence?
 - Single strand - vertical
 - degree Y configuration
 - Tension sensor
- What type of mesh is used in the fence?
- What type of anchoring system should be used in this terrain?
- What kind of paint is used on the fence?
- What type of stabilizers should be used on the fence?
- What gap is allowed at the bottom of the fence?
 - For earth
 - For asphalt
- What pattern attachment scheme is used on the fence?
- What type of reinforcement against cars (aircraft arresting wire) is used?
- When do the guards patrol the fence (day/night)?
- When should the fence be checked for maintenance?
- When should sections of the fence be replaced for preventive maintenance?
- Are noted deficiencies immediately corrected?
- Where is the fence placed in relation to roads buildings?
- Where are the sensors placed on the fence?
- Where are guards near the fence?
- Where are lights placed in conjunction with the fence?
- Where are clear zones needed?
- When are tandem fences needed?
- When electric fences are in use, have power considerations been evaluated?
 - Backup power
 - Vulnerability of power system
 - Warning Signs for the public
- When are walls to be used in lieu of fences?

Enclosure 1: Fence Design Tools

Fence Design Criteria: Four types of fencing authorized for use in protecting restricted areas are chain-link, barbed wire, concertina, and barbed tape. Choice of type depends primarily upon the degree of permanence of the installation, availability of materials, and time available for construction. Generally, chain-link fencing will be used for protection of permanent limited and exclusion areas. All four types of fencing maybe used to augment or increase the security of existing fences that protect restricted areas. Examples would be to create an additional barrier line, increase existing fence height, or provide other methods that add effectively to physical security.

a. Chain-link (Federal Spec. RR-F-191/1, Type I). Chain-link fence, including gates, must be constructed of 7-foot (approximately 2.13 m) material (6 foot or 1.83 m for controlled areas), excluding top guard. Fence heights for conventional arms/ammo security must be 6 feet for standard chain link, wire-mesh fencing. Chain-link fences must be of 9-gauge (.1508 inches or 3.77 mm) or heavier wire galvanized with mesh openings not larger than 2 inches (approximately 5.1 cm) per side, and a twisted and barbed selvage at top and bottom. It must be taut and securely fastened to rigid metal or reinforced concrete posts set in concrete. It must reach within 2 inches (5.1 cm) of hard ground or paving. On soft ground it must reach below the surface deeply enough to compensate for shifting soil or sand (OCE Guide Specification 02711). Security commensurate with FE-6 fence construction standards will be provided. Construction must be in accordance with specifications in Office, Chief of Engineers (OCE) drawing 40-16-10 (figure 11). For added resistance to climbing, optional top rail or taut wire may be omitted. Fencing may be painted with a nonreflective substance to reduce the glare to security forces. Weaknesses in the chain link fence occur as a result of weather (rusting) and failure to keep fencing fastened to the post which affects the desired tightness.

1. Barbed Wire. Standard barbed wire is twisted, double-strand, 12-gauge wire, with four-point barbs spaced an equal distance apart. Barbed wire fencing, including gates, intended to prevent human trespassing should not be less than 7 feet (2.13 m) high, excluding the top guard, and must be firmly affixed to posts not more than 6 feet (1.82 m) apart. The distance between strands will not exceed 6 inches (approximately 15.3 cm) and at least one wire will be interlaced vertically and midway between posts.

2. Concertina. Standard concertina barbed wire is a commercially manufactured wire coil of high-strength-steel barbed wire, clipped together at intervals to form a cylinder. Opened, it is 50 feet long and 3 feet in diameter. When used as the perimeter barrier for a restricted area, concertina must be laid between poles with one roll on top of another or in a pyramid arrangement (minimum of three rolls). The ends must be staggered or fastened together and the base wire picketed to the ground.

3. Barbed Tape (Mil Fed Spec. MIL-B52775A)

4. The barbed tape system is composed of three items--barbed tape, barbed tape dispenser, and concertina tape. These items were type classified "standard A type," 16 December 1965.

5. Barbed tape is fabricated from a steel strip (0.020 inches thick nominal) with a minimum breaking strength of 500 pounds. The overall width is 3/4 of an inch. The tape has 7/16-inch barbs spaced at 1/2 inch intervals along each side. Fifty meters of tape are wound on a plastic reel 8 3/4 inches in diameter and 1 inch thick. The finish is electro-galvanized 0.0001-inches thick on each side.

6. Barbed tape concertina consists of a single strand of spring steel wire and a single strand of barbed tape. The sections between barbs of the barbed tape are securely clinched around the wire. Each coil is approximately 37 1/2 inches in diameter and consists of 55 spiral turns connected by steel clips to form a cylindrical diamond pattern when extended to a coil length of 50 feet. One end turn is fitted with four bundling wires for securing the coil when closed and each end turn is fitted with two steel carrying loops. The concertina extends to 50 feet without permanent distortion and when released, can be retracted into a closed coil.

7. The handling of barbed tape requires the use of heavy barbed tape gauntlets instead of standard barbed wire gauntlets.
8. **Top Guard.** A top guard must be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or barbed tape along the top of a fence, facing outward and upward at approximately a 45-degree angle (figure 14). Top guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence at least 1 foot (approximately 30.5 cm). Three strands of barbed wire, spaced 6 inches (15.2 cm) apart, must be installed on the supporting arms. The number of strands of wire or tape may be increased when required. The top guard of fencing adjoining gates may range from a vertical height of 18 inches (45.7 cm) to the normal 45-degree outward protection, but only for sufficient distance along the fence to open the gate(s) adequately. Top fence rails should not be specified where protection is of utmost importance. Top rails will assist a climber. A bottom and top wire reinforcement should be used as a substitute (OCE-02711).
9. **Gates and Entrances.** The number of gates and perimeter entrances must be the minimum required for safe and efficient operation. Active perimeter entrances must be designed so that the guard force maintains full control. Semiactive entrances, such as infrequently used vehicular gates, must be locked on the inside when not in use. Gates and entrances, when closed, must provide a barrier structurally comparable to their associated barrier(s). Top guards, which may be vertical, are required for all gates.
10. **Type Field Perimeter Fence.** A combination of concertina fencing, developed in Vietnam, uses a double-barbed wire with five rolls of concertina between the fences. This fence has, in many situations, been used in place of chain link fence, and has been found to be most effective
11. **Tanglefoot Wire.** Barbed wire or tape may be used in appropriate situations to construct a tanglefoot obstruction either outside a single perimeter fence or in the area between double fences, to provide an additional deterrent to intruders. The wire or tape should be supported on short metal or wood pickets spaced at irregular intervals of 3 to 10 feet, and at heights between 6 and 12 inches. The wire or tape should be crisscrossed to provide a more effective obstacle. Depth of the field is governed by the space and materials available.

Appendix 10: Lighting

Purpose :

Lighting is an essential element of an integrated physical security program. During hours of darkness, protective lighting provides a means of continuing a degree of protection close to that maintained during daylight hours. This safeguard also has considerable value as a deterrent to thieves and vandals, and may make a potential terrorist operation directed at the installation more difficult. Protective lighting should enable guard force personnel to observe activities around or inside an installation without disclosing their presence. The purpose of this appendix is to provide measures to enhance the current lighting system on the system so that these measures can be integrated into the overall AT/FP Plan. This plan should be maintained by the proper security forces to ensure employment of the proper measures at all times.

Background:

Lighting is inexpensive to maintain, and when properly employed may reduce the need for security forces. It may also provide personal protection for forces by reducing the advantages of concealment and surprise for a determined intruder. Security forces thus relieved may be used to better advantage elsewhere. Adequate lighting for all approaches to an installation not only discourages attempted unauthorized entry, but also reveals persons within the area. However, lighting should not be used alone. It should be used with other measures such as fixed security posts or patrols, fences and alarms.

Critical Questions:

- Who is the responsible person(s), staff(s), or unit(s) for the lighting system?
- What information is included in the overall AT/FP Plan?
- What forces are assigned to the lighting system?

Considerations:

- What is the current status of the lighting system?
- What is the desired goal of the lighting system?
- What modifications/new starts are needed to achieve the end state? (This section should feed to an installation construction plan).
- What areas of the installation are being lit?
- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- Are the lights used to illuminate different things? (People vs Objects)
- Where will the lights be placed?
- Are lights needed in conjunction with the barriers? (Previous appendix)
- Who inspects/maintains the lighting system?
- Who mounts the surveillance equipment with the lights?
- What type of lights are being used?
- What type of beams and what color of beams do the lights have?
- What type of power source is being used?
- Is the power source constant?
- Is there a backup power source?
- Where is the power source located?
- Can the power source be accessed from outside the installation?
- Are the lights susceptible to counter measures?
- What type of mounting is required?
- Is there scheduled maintenance performed?
- Where do you put guards in conjunction with the lights?

Does the installation often have power blackouts, fluctuating or erratic voltages in the primary power source?

Tab 1: Lighting Tools

Types of Lighting:

- Continuous (Stationary Luminary)
 - Glare Protection Lighting
 - Controlled Lighting
- Standby Lighting (Stationary Luminary)
- Building Face Perimeters
 - Active Entrances
 - Semiactive or Inactive Entrances
- Moveable Lighting
- Emergency Lighting

Planning Considerations:

- Cleaning and replacement of lamps and luminaries, particularly with respect to costs and means (such as ladders) required and available.
- Advisability of including mercury and photoelectric controls. These may be desirable in a peacetime situation, but undesirable when a blackout is a possibility.
- The effects of local weather conditions on various types of lamps and luminaries.
- Fluctuating or erratic voltages in the primary power source.
- Requirement for grounding of fixtures and the use of a common ground on an entire line to provide a stable ground potential.
- Establishment of a ledger to maintain a burning-time (80 percent) record based on the life expectancy of the lamp. The ledger should contain as a minimum the following:
 - Type and wattage of lamp.
 - Area, facility, or utility pole used.
 - Date of insertion.
 - Program date (based on life expectancy) for extraction and where used.

PROTECTIVE LIGHTING CHECKLIST

- Is the perimeter of the installation and restricted area fencing provided adequate lighting?
- Does the protective lighting meet adequate intensity requirements?
- Are the cones of illumination from lamps directed downward and away from guard personnel?
- Is perimeter protective lighting used so that security force patrol personnel remain in comparative darkness?
- Are lights checked for proper operation at least once daily?
- Are defective lights and need for replacement of inoperative lamps reported immediately?
- Are repairs to lights and replacement of inoperative lamps effected immediately or in a reasonable time?
- Is additional protective lighting provided at active portals and points of possible unauthorized intrusion?
- Are gate guard houses provided with proper illumination?
- Does the activity have a dependable primary source of power for its protective lighting system?
- Does the activity have a dependable auxiliary (emergency) source of power for its protective lighting?
- Is the protective lighting system independent of the activity primary lighting or power system?
- Is the primary power supply for the protective lighting system protected?
- How is it protected?
- Are there provisions for standby or emergency protective lighting?
- Is the standby or emergency equipment tested at least monthly?
- Can the emergency backup power supply be rapidly switched into operation when needed?
- Is the emergency backup power supply self-starting?
- If not, what is the time delay between primary power loss and activation of secondary (emergency) power?
- Is the protective lighting emergency or stand-by power source located within a restricted area?
- Is parallel circuitry used in the wiring?

- Are multiple circuits used?
- If yes, are proper switching a-rearrangements provided?
- Are switches and controls properly located, controlled and protected?
- Are they weatherproof and tamper resistant?
- Are they readily accessible to security personnel?
- Are they located so that they are inaccessible from outside the perimeter barrier?
- Is there a centrally located switch to control protective lighting?
- When was the most recent activity lighting energy conservation opportunities (LECO) study conducted?
- When was the most recent installation/ restricted area protective lighting survey conducted?
- Is the protective lighting system designed and locations recorded so that repairs can be made rapidly in an emergency?
- Are materials and equipment in shipping and storage areas properly arranged to provide adequate lighting?
- If bodies of water form a part of the perimeter, is adequate lighting provided where deemed appropriate?

Appendix 11: On-Site Security Elements

Purpose :

Security force functions should be designed to detect/deter and defeat terrorism; prevent/deter theft and other losses caused by such things as fire, accident, sabotage and espionage; protect life, property and the rights of individuals; and enforce rules, regulations, and statutes. The listed functions will enhance the AT/FP posture of the installation. The on site security element of the AT/FP Installation Plan is integral to the efficient operations of the majority of the plan. The security element is critical to the increases in the THREATCON status. Therefore it is important that their tasks and responsibilities to be clearly defined and the command and control of these forces be understood throughout the installation. This should be entered as an annex to the AT/FP.

Background:

It is important that the commander or his designated representative instruct the security force in the extent and limitations of the commander's jurisdiction. Whether state or Federal law or both are applicable on a particular portion of a military installation or facility depends largely on the nature of jurisdiction.

The first line of defense against hostile acts at or on the installation is not elite counter-terrorist units, but those security force organic to the installation commander. The security force constitutes one of the most important elements of an activity's physical security program. Security forces normally perform duties that require higher degrees of training and experience such as: Security of restricted areas; security of specific sensitive areas; direct action in the event of hostilities towards Americans, supervisory or coordinated role with other military units or security agencies.

Critical Questions:

- What person or staff has overall responsibility for the installation's on-site security element?
- What forces are responsible for physical security?

Considerations:

- Where is the security unit located?
- What forces are identified as auxiliary to reinforce the primary unit?
- When was the last time the on-site security element was evaluated?
- Who established the on-site security element mission essential task list (METL)?
- When was the commander's intent for the on site security element updated?
- Who interfaces with the security elements?
- What changes (auxiliary security forces) will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- What is the alert notification procedure?
- Who is the on-site security member on the crisis management team?
- What specialized training does on-site security require?
- Who in the security forces was part of the plan development?
- When were the incident reaction plans rehearsed?
- What were the results of the after action report?
- What specialized equipment is needed?
- Who authorizes direct action by security force personnel?
- Who is the POC for the rules of engagement?
- Who coordinated with the SJA and IG for the ROE?
- Who insures the continuity of capabilities during an incident?
- What reserve element will be used?
- Who authorizes additional personnel?
- When are personnel re-evaluated?
- Who develops selection criteria?
- What training programs are available within DOD?

- What training programs are available with US Government / Foreign?
- What training is available from outside sources?
- When are no notice exercises and rehearsals conducted?
- Who developed the on-site security element METL?
- Who determines task/conditions/standards?
- What unique systems are located at the installation?
- Who provides specialized training for the unique systems?
- Where can the specialized training be conducted?
- What legalities exist with any special/unique training?
- Who insures that proper equipment is available for training and mission?
- Is there an Embassy located nearby?
- Has coordination been done with the RSO and local guard force for patrolling of residential areas?

Tab 1: On Site Security Elements Checklist

- Is the present security force strength and composition commensurate with the degree of security protection required?
- Are security force orders under constant review for currency and does the security officer conduct a total detailed review at least semi-annually?
- Do security force members have security clearances equivalent to the highest degree of security classification of the documents, material, etc., to which access may be required?
- Do civil service members of the security force meet the minimum qualifications of the Office of Personnel Management qualification standards?
- If a composite security force is used, is there a single separate supervising echelon for military and civilian elements?
- Are security force personnel inspected and briefed by a supervisor prior to being posted?
- Do supervisors inspect each post/patrol/ activity at least twice per shift?
- Does the activity maintain an organized and equipped Auxiliary Security Force (ASF)?
- Does the Auxiliary Security Force receive adequate training?
- Are there sufficient on-board active duty military personnel available who could be utilized by the host command to adequately staff the Auxiliary Security Force?
- Has consideration been given to employing alternate security measures such as intrusion detection systems, closed-circuit television, securing nonessential perimeter gates?
- Are there adequate visitor escort procedures established to preclude the use of security force personnel as escorts?
- Has liaison been established with local, state and Federal law enforcement agencies whereby early warning of threat situation will be provided?
- Are appropriate armed guards or DCS used for the shipment of highly classified material?
- Are adequate plans prepared as part of the station crisis management plan for augmenting the security force with additional personnel and equipment?
- If yes, is the post 24-hr/7-day week force strength?
- Do security adequate training provided? manning factor of 5.3 for a
- post used for determining security force personnel record or report
- their presence at key points in the installation by means of: portable watch clocks, central watch clock stations, telephones, two-way radio communications equipment, or other?
- Are guard assignments, times and patrol routes varied at frequent intervals to avoid establishing routines?
- Are quarterly exercises conducted using the Auxiliary Security Force? If yes, are adequate records and logs maintained on each exercise?
- Are periodic assessments of weapons and ammunition made to determine adequacy and are measures taken to change allowances as appropriate?
- Are contract guard personnel subject to a National Agency Check prior to performing duty?
- Are contract guard personnel performing under a classified contract cleared at a level equal to the material being protected?
- Does the command have an organized, trained and equipped Emergency Service Team?
- Is the EST under the operational control of the security officer?
- Is the EST drilled at least once each quarter using various scenarios?
- Is the EST comprised of only DOD and/or military members of the security department?
- Are EST applicants thoroughly screened for suitability as required, including psychological screening?

Appendix 12: Technology

Purpose :

The commander's designated planner(s) for AT should conduct a comprehensive analysis of the threat and physical security plan for the installation. Once planners formulate these reports, they should identify areas where technology, specifically Intrusion Detection System (IDS), could enhance the security posture. Other technologies to be considered are x-ray devices, closed-circuit televisions, sensors, and night vision devices.

Background:

DOD 5200.8-R encourages the use of technology and people to achieve a cost-effective, security system level of performance. Planners should bear in mind that cost-effective security systems designs use the minimum essential components to achieve the desired level of security; resource limitations and constraints mean that trade-offs will be required.

Intrusion detection systems play a vital part in the overall protection of military installations, activities, equipment and materiel assets. These systems detect through sound, vibration, motion, electrostatic and/or light beams. For an item to be secure, the system must focus upon detecting unauthorized individuals at the entry points (gate, door, or fence), area (buildings), and at a specific object (vault, file, or safe). It is important to remember that any security detection system, once activated, is useless unless it is supported by a prompt, quick reacting security force.

The purpose of IDS is to accomplish one or more of the following:

Economize - permit more economical and efficient use of manpower by requiring smaller mobile responding guard forces instead of larger numbers of personnel for patrols and fixed guard posts.

Substitute - use in place of other physical security measures which cannot be used because of safety regulations, operational requirements, appearance, layout, cost, or other reasons.

Supplement - provide additional controls at critical points or areas; provide insurance against human error; enhance the security force capability; provide the earliest practical warning to security forces of any attempted penetration of protected areas.

Critical Questions:

- Who is responsible for the IDS or other technology planning?
- What are the critical areas that need to be protected?
- How can the MEVAs be best protected?

Considerations:

- What is the criticality of the installation or facility?
- What is the mission of the installation/facility?
- What is the installation RDF status?
- What is the level of maintenance?
- What are the high-end equipment items?
- Who conducted an analysis of the installation?
- When was the last time that analysis was done?
- Where is the report?
- To whom was the report disseminated?
- When the threat increases, can a technological system be added to for minimal cost upgrade?
- When the threat decreases, can the upgraded portions be recovered and stored for future use?
- What will be savings in manpower?
- What are the savings of money over time?
- What is the response time for security forces?
- What special tactical training have they received?
- What special training have they received on the IDS?
- What is the extent of VIPs to the installation?

- Where is the most vulnerable location and how accessible is it to intruders?
- What security measures are presently in place?
- What assets are available to the installation?
- Where would infra-red lighting / acoustic sensors be most effective
- What security systems exist (fire alarms / lighting / fencing) for individual buildings?
- Are other forms of detection available?
- What systems, if any, are linked to local law enforcement?

Other Planning Factors:

The IDS that is determined, should be purchased and developed for each site with the capabilities to be modularized and built upon if the threat level were to increase.

Each system should be capable of operating from a standby power source to compensate for the vulnerability of power sources outside the installation. The time requirement for such capability must be evaluated in each case dependent upon such factors as alternate power supplies, maintenance support, and hours of active operation.

At each installation the type of technology selected is intended to meet a specific type of problem. Factors to be considered in selecting the appropriate components/systems include but are not limited to the following:

- Location and response time capability of security forces
- Availability of security forces
- Value of facility, material, or the sensitivity of classified material to be protected
- Area environment, to include building construction, sound levels inside and outside, and climate
- Communications and electrical interference
- Operational hours of the installation or facility
- Specific target to be protected

A consideration of these factors readily indicates the advisability of obtaining technical data to assist in making a wise selection. Often, more than one type of sensor, or even system is necessary to give adequate protection for an area or structure.

While there are a variety of commercially manufactured and militarily procured systems designed to detect approach or intrusion, the security arena is changing on an almost daily basis. Therefore the commander should identify a section or individual to monitor the market for emerging technologies so that the installation can respond to any changes in the security profile. When the unique event or permanent change in the profile takes place, this section or individual should be able to identify the special technology required to keep the security profile at its necessary level. Useful items to observe the technology changes are:

Trade Shows

Conferences / Seminars

Defense Journals

US Government training programs

DOD training programs

Commercial training programs

Foreign Government training programs

Membership to Security organizations

Specific standards for intrusion detection can be found in FM 19-30, Chapter 7 (Army).

Specific standards for intrusion detection can be found in AFI 31-101, Chapter 8, Pages 59 through 62 (Air Force).

Specific standards for intrusion detection can be found in DOD 2000.12-H, Chapter 8, Paragraph E, Page 8-9 (DOD).

An intrusion detection system checklist can be found in FM 19-30, Appendix O, Page 399.

Appendix 13: Training

Purpose :

Commanders and civilian managers have a continuing responsibility to insure that personnel receive comprehensive security awareness briefings. The objective is to develop the installation security awareness to such a degree that the organization presents a very strong security profile. In so doing it becomes a significantly less vulnerable target.

Security awareness and personnel protection programs are to increase awareness to the possible threat of terrorism. The commander's designee for anti-terrorism programs should inform all DOD personnel including dignitaries, civilian employees, and dependents of the general threat, as well as the perceived threat level in the general area of the installation or area of operation of any activity. To assist the designated POC, the training is organized around; Individual Training, Unit Training, and Installation Training Awareness. Once planners have prepared the installation training plan, they should integrate it into the AT/FP Plan.

Background:

All military personnel and family members, as well as civilians connected with the military or US Government (including contract personnel) are potential victims of terrorist attacks and should take the proper security precautions. The most important measure is in educating persons who are likely targets in recognition of threat and taking appropriate actions to reduce their risk. Personal protection, education, and training must emphasize how to deny the opportunity for an attack or to elevate the risk to the attacker. The objective of personal protection is to use personal protection measures tailored to the level of the threat.

- Individual Training Programs: Individual training should consist of a program that makes the personnel aware that a threat is present and that they must be constantly aware that they, the installation personnel, are the commands first line of defense against the gathering intelligence on them. These classes include but are not limited to:
 - Terrorist Operations
 - Individual Protective Measures
 - Detecting Surveillance
 - Cultural Awareness
 - Reporting Procedures for Incidents
- Unit Training: Unit training should consist of the initial Individual Training and those programs as directed by service specific yearly training requirements. They should include but are not limited to:
 - Threat Updates
 - United States Current Affairs
 - Host Nation Current Affairs
 - Interrogation Techniques
 - Debriefing Techniques
- Installation Training Exercises: The installation directs the service specific training requirements for all tenant units. To insure that these training programs are effective and disseminated properly, the installation should conduct a series of exercise to monitor the training program's progress. They should include but are not limited to:
 - No notice inspection of training records
 - Field training exercises with a dedicated opposition intelligence gathering force
 - Unilateral low visibility exercises for the intelligence/counter intelligence divisions directed against units
 - Insure that a strong positive threat awareness briefing is prepared for every field exercise conducted

Critical Questions:

- What person, staff, or unit is responsible for the implementation of the installation's AT/FP education and training programs?
- How will the AT/FP education and training programs be implemented on the installation?

Considerations:

- How many service members on the installation are trained to level one or level two?
- How many level one personnel are on the installation?
- When was the last AT/FP installation exercise conducted?
- How does the installation assess the adequacy of training for dependents?
- How old are the training materials on the installation?
- What schools/courses are available for security professionals?
- How often do installation HRPs travel?
- How often does the installation receive HRPs?
- When HRPs arrive do they remain on the installation?
- How often do HRPs go to local authorities?
- Who coordinates with local authorities for special activities(celebrations, displays, VIP visits)?
- What is the current status of training?
- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- Is there a historical data base of incidents in your area of operation?
- Is there a review panel to insure that DOD and installation requirements are met?
- Who is the training director and/or special instructor cadre?
- Is there a "train the trainer" program on the installation?
- How often is training conducted?
- When was the last time a training program was conducted?
- What education programs are taught by local law enforcement personnel?

Tab 1: Security Education Program

Security programs, information awareness campaigns and planning efforts are useless without an effective security education program. Security education is a participatory program requiring the support of the entire installation (including civilian personnel, contractors, family members and tenant units). DODI 2000.14 outlines policy and procedures accorded the education process for the Department of Defense. For Civilian Contractor personnel working/living abroad, this is augmented by the Department of State Overseas Security Advisory Council publication "Emergency Planning Guidelines for American Businesses Abroad."

A good Security education program consists of (but is not limited to):

- Individual Training (Level I)
- Unit/Ship Training (Level II)
- Command Level Training (Level III)
- Executive Level Training (Level IV)
- Security Awareness Campaign
- Area of Responsibility (Geographic) Specific Training/Information for Assigned, Exercise or Temporary Duty Personnel
- Installation Response/Preparedness Leader/Manager Coordination Drills and Verification Exercises
- Installation Personnel, Facilities Security Exercises (scenario and THREATCON driven)
- Mass Casualty, First Responders Drills

A comprehensive security education program must view security as part of operations, training, quality of life and health, morale and welfare activities. In addition, it must not only be concerned with physical security measures but crime prevention, pilferage, operational security as well as personnel security and the collection, analysis and reporting of intelligence information relating to domestic and international terrorism incidents.

Responsibility for the education program does not stop at the physical parameters of the installation/base but by close coordination and association with local law enforcement officials, includes the military population in the community at large.

Steps to be taken by installation security manager in creating a comprehensive Installation Security Program of Instruction/Course of Instruction[POI/COI]:

- Ensure Installation Security Managers attend the *Terrorism on Military Installations and/or Bases Course*
- Identify populations at the various levels to receive training
- Identify resource personnel to assist in the formulation of the program (personnel identified in this group should also be considered for inclusion into the Threat Working Group):
 - Staff Judge Advocate
 - Chaplain
 - Special/Community Services Officer
 - Safety Officer
 - Public Affairs Officer
 - Installation Chief Medical Officer
 - Explosive Ordnance Disposal
 - Tenant Unit Commanders
 - Criminal/Special Investigations Officer
 - Installation/Base Operations/Intelligence staff officer
 - Local Police, Emergency Services/Medical Managers
 - Commercial Contractors Representatives
 - AAFES/NAVEX/DECA Representatives

- Identify high-risk personnel, high risk positions that must attend the *Individual Terrorism Awareness Course* at the JFK Special Warfare Center and School at Fort Bragg, NC. (JFK SWCS)
- Identify requirements for other specialty training through DODI 200014
- Identify the total security posture of the installation.
- Identify and clarify the aims and objectives of the programs.
- Identify the tools and resources needed to execute the programs. This includes certification that instructors are qualified to provide training
- Identify and disseminate to tenant units trends from recent inspections (within or without the installation) that affect the conduct and direction of educational programs.
- Ensure a system is in place to provide pre-travel, pre-deployment briefings that are AOR specific. This includes, when necessary, classified briefings and special briefings for high-risk areas.

The following courses are DOD mandatory, standardized, Level I training topics,.

- Introduction to Terrorism
- Terrorist Operations
- Individual Personnel Protection Measures
- Terrorist Surveillance Techniques
- Hostage Survival
- Explanation of Threat Level
- Recent AOR Updates for area of travel, to be provided to installations by geographical CINCs, which will include a current threat brief (including the availability of classified information) and AOR specific requirements.

Tab 2: Personal Protective Measures Against Terrorism

Any member of the Department of Defense, not just senior leaders, can become a target for terrorists. The purpose of this appendix is to provide general guidance to DOD members and their families on how to avoid acts of terrorism, as well as to provide basic instructions in the event DOD personnel become victims of a terrorist attack. Attitude toward security is most important. Although some of these precautions are applicable overseas, you can decrease your chances of becoming a terrorist target, as well as those of your family members, by taking the precautions listed in this appendix. Therefore, it is highly recommended you share this information with every member of your family. It is also suggested that you and your family review these precautions on a regular basis.

At All Times:

- Encourage security awareness in your family and discuss what to do if there is a security threat.
- Be alert for surveillance attempts or suspicious persons or activities, and report them to the proper authorities.
- Trust your gut feelings.
- Vary personal routines whenever possible.
- Get into the habit of checking in, to let your friends and family know where you are or when to expect you.
- Know how to use the local phone system.
- Always carry telephone change.
- Know the emergency numbers for local police, fire, ambulance, and hospital.
- Know the locations of civilian police, military police, government agencies, US Embassy, and other safe locations where you can find refuge or assistance.
- Avoid public disputes or confrontations. Report any trouble to the proper authorities.
- Know certain key phrases in the native language such as "I need a policeman," "Take me to a doctor," "Where is the hospital?" and "Where is the police station?"
- Set up simple signal systems to alert family members or associates that there is a danger. Do not share this information with anyone not involved in your signal system.
- Carry identification showing your blood type and any special medical conditions.
- Keep a minimum of a 1-week supply of essential medication on hand at all times.
- Keep a low profile. Shun publicity. Do not flash large sums of money.
- Do not unnecessarily divulge your home address, phone number, or family information.
- Watch for unexplained absences of local citizens as an early warning of possible terrorist actions.
- Keep your personal affairs in good order. Keep wills current, have powers of attorney drawn up, take measures to ensure family's financial security, and develop a plan for family actions in the event you are taken hostage.
- Do not carry sensitive or potentially embarrassing items.

At Home:

- Have a clear view of approaches to your home.
- Install strong doors and locks.
- Change locks when you move in or when a key is lost.
- Install windows that do not allow easy access.
- Never leave house or trunk keys with your ignition key while your car is being serviced.
- Have adequate lighting outside your house.
- Create the appearance that the house is occupied by using timers to control lights and radios while you are away.
- Install one-way viewing devices in doors.
- Install intrusion detection alarms and smoke and fire alarms.
- Do not hide keys or give them to very young children.
- Never leave young children at home alone.
- Never admit strangers to your home without proper identification.
- Use off street parking at your residence, if at all possible.

- Teach children how to call the police, and ensure that they know what to tell the police (name, address, etc.).
- Avoid living in residences that are located in isolated areas, on one-way streets, dead-end streets, or cul-de-sacs.
- Avoid residences that are on the ground floor, adjacent to vacant lots, or on steep hills.
- Carefully screen all potential domestic help.
- Do not place your name on exterior walls of residences.
- Do not answer the telephone with your name and rank.
- Personally destroy all envelopes and other items that reflect personal information.
- Close draperies during periods of darkness. Draperies should be opaque and made of heavy material.
- Avoid frequent exposure on balconies and in windows.
- Consider owning a dog to discourage intruders.
- Never accept unexpected package deliveries.
- Don't let your trash become a source of information.

While Traveling:

- Vary times and routes.
- Be alert for suspicious-looking vehicles.
- Check for suspicious activity or objects around your car before getting into or out of it. Do not touch your vehicle until you have thoroughly checked it (look inside it, walk around it, and look under it).
- Know your driver.
- Equip your car with an inside hood latch and a locking gas cap.
- Drive with windows closed and doors locked.
- Travel with a group of people--there is safety in numbers.
- Travel on busy routes; avoid isolated and dangerous areas.
- Park your car off the street in a secure area.
- Lock your car when it is unattended.
- Do not routinely use the same taxi or bus stop. NOTE: Buses are preferred over taxis.
- If you think you are being followed, move as quickly as possible to a safe place such as a police or fire station.
- If your car breaks down, raise the hood then get back inside the car and remain there with the doors locked and the windows up. If anyone offers to assist, ask the person to call the police.
- Do not pick up hitchhikers.
- Drive on well-lit streets.
- Prearrange a signal with your driver to indicate that it is safe to get into the vehicle. Share this information only with persons having a need to know.
- Safeguard car keys at all times.
- Screen chauffeurs or permanently assigned drivers. Develop a simple system for the driver to alert you to danger when you are picked up. Share this information only with persons having a need to know.
- Lock your car, especially at night, and check and lock your garage when you park there overnight.
- Park in well-lighted areas if you must park on the street.
- Always fasten seat belts, lock doors, and close windows when driving or riding in a car.
- Be alert for surveillance and be aware of possible danger when driving or riding in a car.
- Drive immediately to a "safe haven" when surveillance is suspected; do not drive home.

Air Travel Security:

- Use military aircraft whenever possible.
- Avoid travel through high-risk areas; use foreign flag airlines and/or indirect routes to avoid such areas.
- Do not use rank or military addresses on tickets, travel documents, hotel reservations, or luggage.
- Select a window seat on aircraft because they offer more protection and are less accessible to hijackers than are aisle seats.
- Select a seat in the midsection of the aircraft because it is not one of the two usual areas of terrorist activity.
- Do not discuss your US Government affiliation with any other passengers.

- Consider using a tourist passport when traveling in high-risk areas; if you use a tourist passport, store your official passport, identification card, travel orders, and other official documents in your carry-on bags.
- Also, if you normally wear a military ring; e.g., Service or academy, consider leaving it at home or pack it in your checked baggage.
- Do not carry classified material unless it is mission-essential.
- Use plain civilian luggage; avoid using B-4 bags, duffel bags, and other military-looking bags.
- Remove all indications of your rank and any military patches, logos, and decals from your luggage and briefcase.
- Do not carry official papers in your briefcase.
- Travel in conservative civilian clothing.
- Do not wear military-oriented organizational shirts or caps or military-issue shoes or glasses.
- Also, avoid obvious American clothing such as cowboy boots and hats as well as American-logo T-shirts.
- Cover visible US-affiliated tattoos with a long-sleeved shirt.
- If possible, check your baggage with the airport's curb service.
- Adjust your arrival at the airport to minimize waiting time, be alert for any suspicious activity in the waiting area, and proceed immediately to the departure gate.

Hostage Defense Measures:

- Survive with honor--this is the mission of any American hostage.
- If your duties may expose you to being taken hostage, make sure your family's affairs are in order to ensure their financial security.
- Make an up-to-date will and give appropriate powers of attorney to your spouse or to a trusted friend. Concern for the family is a major source of stress for persons in kidnap or hostage situations.
- If you are taken hostage and decide not to resist, assure your captors of your intention to cooperate, especially during the abduction phase.
- Regain your composure as quickly as possible after capture, face your fears, and try to master your emotions.
- Take mental note of the direction, time in transit, noise, and other environmental factors that may help you identify your location.
- Note the numbers, names, physical characteristics, accents, personal habits, and rank structure of your captors.
- Anticipate isolation and terrorist efforts to confuse you.
- Try to mentally prepare yourself for the situation ahead as much as possible. Stay mentally active.
- Do not aggravate your abductors; instead, attempt to establish a positive relationship with them. Do not be fooled by a friendly approach--it may be used to get information from you.
- Avoid political or ideological discussions with your captors; comply with their instructions, but maintain your dignity.
- Do not discuss or divulge any classified information that you may possess.
- Exercise daily.
- Read anything you can find to keep your mind active.
- Eat whatever food is offered to you to maintain your strength.
- Establish a slow, methodical routine for every task.
- When being interrogated, take a simple, tenable position and stick to it. Be polite and maintain your temper. Give short answers, talk freely about nonessential matters, but be guarded when the conversation turns to substantial matters.
- If forced to present terrorist demands to authorities, in writing or on tape, do only what you are told to do. Avoid making a plea on your own behalf.
- Be proud of your heritage, government, and military affiliation, but be careful that your behavior does not antagonize your captors.
- Affirm your faith in basic democratic principles.

In the event of a rescue attempt:

- Drop to the floor.
- Be quiet and do not attract your captors' attention.
- Wait for instructions.
- Rescue forces will initially treat you as one of the terrorists until you are positively identified as friend or foe.
- This is for your security. Cooperate, even if you are initially handcuffed.
- Once released, avoid making comments to the news media until you have been debriefed by the proper US authorities.

Appendix 14: Weapons of Mass Destruction

WMD is beyond the scope of this AT/FP Planning tool. Provided below are rudimentary planning considerations. A separate WMD Planning Template is to be published.

Purpose :

Recent changes in the international availability of Chemical and, to a lesser extent, Biologic agents increase the possibility of WMD. This appendix will assist in preparing a plan for WMD and in integrating it into the AT/FP Plan.

Background:

The threat of WMD terrorism is different than the threat of "NBC" use on a battlefield. As events in Tokyo (1995 Sarin attack), New York City (1993 World Trade Center), and Oregon (1984 salmonella bacterium attack) indicate the use of chemical and biologic agents in a terrorist attack are not only possible, but have been planned and executed. While these attacks have had varying success it is undeniable that they have terrorized millions.

While the fielded U.S. Military is educated, trained, and equipped to operate in a "NBC" environment, the rear areas and (not-deployed) forces are less so. To a terrorist looking to terrorize the U.S. installations make inviting targets. Many areas on the installation naturally tend to congregate unprotected people. Examples of this are the PX, movie theater, and Parade Deck. The installation commander should prepare to mitigate the effects of WMD terrorism.

Critical Questions:

- Who is the responsible person, staff, or unit for the WMD planning?
- What analysis products must be produced/for what purpose?
- What forces are assigned WMD detection/protection/decontamination responsibilities?

Considerations:

- What changes will be made during increased THREATCON status to respond to the WMD threat?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?

WMD Threat Assessment:

- What sources of information feed the Threat assessment?
- What is the current threat?
- What terrorist groups have used WMD before?
- What type of agents has been used?
- What methods of dispersal have been attempted?
- Training levels of personnel in assessment?

Contamination Avoidance:

- When was the last exercise that tested the contamination avoidance
- Early warning?
- Sensor development and testing?

Protection:

- What equipment is on hand?
- What protective gear is available to be issued?
- When was the last MOPP exercise?
- What was the results of the last MOPP exercise?
- What threat warning puts the installation in what posture (MOPP)?

Decontamination:

- What decontamination gear is available for hasty/deliberate decontamination?
- How large an area should the installation be prepared to decontaminate?

Medical Aspects:

- How many casualties can be expected?
- What are the threat agents?
- Where are the hospitals onbase/offbase?
- Where are the MOUs/MOAs that clearly lay out tasks and responsibilities?

Appendix 15: Information Operations

Purpose :

Information Operations is an emerging mission area that may involve terrorist operations. Terrorists may choose to strike at an informational source to terrorize an installation or DOD. The individual responsible for information operations should develop a plan for safeguarding information and integrate this plan into the overall AT/FP Plan.

Background:

Terrorist operations against informational assets are a growing concern. While the majority of attacks against DOD informational systems have been conducted for monetary gain or "hackers" looking for a thrill, it is possible that terrorists may seize upon this venue for future attacks. The safeguarding of information and even individual knowledge is a constant vigilance. The installation's infrastructure is normally very dependent upon informational sources for routine operations, base management, service member support, and educational/recreational activities. Attacks against several of these target sets could endanger human lives (e.g., hospital records, emergency systems, and air traffic control stations) while others would provide such disruption that the installation may be effectively terrorized.

Critical Questions:

- What person, staff, or unit is responsible for conducting defensive information operations?
- What documentation or program is to be produced?
- How will this program be implemented into the overall AT/FP Plan?

Considerations:

- What changes will be made during increased THREATCON status?
- What augmentation, if any, will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- What historical data is available that will provide method of operation analysis?
- What communications systems are critical to installation operations?
- Have these systems been disrupted before?
- Where are the critical nodes in the communications systems?
- Have there been hacker attempts against this installation?
- What types of information systems operated on the installation?
- When was the last Information Security (INFOSEC) survey conducted?
- Are the INFOSEC specialists current in INTERNET technology?
- Has the C2 system ever been disrupted?
- Who is the on duty response force for information operations threats?

Appendix 16: Airfields

Purpose :

If an airfield exists on an installation, this annex will provide the basic information and beginning point for the commander's designated person who has responsibility for the AT/FP security. Each installation will have unique and special requirements that must be considered beyond any checklist. This plan should be integrated into the overall AT/FP Plan.

Background:

Airfields and aviation assets may be considered prime targets by virtue of the operations conducted (fuel/heavy equipment/ammunitions/high dollar, sensitive items). Additionally airfields are at a disadvantage due to their size and accessibility. Therefore the security officer or AT/FP Planner should use the same planning considerations used for the overall AT/FP Installation Plan in designing the airfield security plan.

Critical Questions:

- Who is responsible for airfield security?
- What documentation or program will they be required to produce?
- How is this document integrated into the overall AT/FP Plan?

Considerations:

- Who controls entry?
- Where are the grid maps?
- Have the grid maps been distributed to all concerned?
- Where is the crisis center for the airfield?
- What intrusion detection system is in place?
- What cover and concealment exists in and around the airfield?
- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- Are there stationary and roving patrols?
- Are there static security posts?
- Is there an outer perimeter fence?
- What type of aircraft are used at the facility?
- How are aircraft secured?
- Where is fuel maintained?
- How is the fuel center secured?
- Where is major equipment critical to operations stored?
- How is the operations center secured?
- How is the command center secured?
- What are the special communications requirements?
- How are specialized security personnel selected (background investigations)?
- What training is needed?
- What special equipment is needed for security forces?
- How is cargo handled?
- Are host nation personnel or third country nationals employed for cargo transport?
- Who checks for foreign objects on the airfield?
- Where is the security forces' holding area in the event of incident?
- When was the last time the security forces rehearsed?
- Where is the nearest fire equipment?
- When was the last time the fire department was tested for airfield disaster?
- Who maintains the records for flight operations and maintenance?
- Where are all blue prints and construction plans maintained?

Tab 1: Airfield Tools:

Airfield Considerations:

1. General Information:

- a. Designation (Name and Number):
- b. Map Reference:
- c. Additional Information:

2. Airfield Data:

- a. Location:
- b. Description:
 - Dimensions/Capacity:
 - Surface:
 - Elevation:
 - Additional Information (General Description):
- c. Reference Points (Direction and Distance):
- d. Approach/Departure Quadrants and Slope:
- e. Recommended Approach/Departure Heading (Magnetic):
- f. Obstacles:
 - LZ Vicinity:
 - Within 5 Miles:
- g. All Known Air Traffic Control Points:
- h. ATC Requirements:
- i. Night Flight Characteristics:
- j. Additional Information (Medical, Weather):

3. Tactical Considerations:

- a. Vulnerabilities:
- b. Recommended Staging Areas:
- c. Ground Routes Available:
- d. Upload Points (Routes, Concealment, Cover):
- e. Emergency Touchdown (Closest Safe Area ingress/egress):
- f. Additional Information:

Appendix 17: Ports

Purpose :

If a port exists at an installation, this annex will provide the basic information and beginning point for the commander's designated person who has responsibility for the AT/FP security. Each installation will have unique and special requirements that must be considered beyond any checklist. A port facility should be evaluated as a system of systems. Therefore for the security officer or AT/FP Planner should use the same planning considerations used for the overall AT/FP Installation Plan in designing the port security plan. This plan should be integrated into the overall AT/FP Plan.

Background:

Port terminals must be protected due to their importance in logistic efforts to transport heavy materiel. Planning for a port must take into consideration many factors not considered in the planning of a land-locked installation.

Ports and terminals areas may include modern piers and warehouses, or may be unimproved beaches on which logistics operations are conducted. The waterside may be anything from a broad and deep harbor to a narrow and shallow river, either of which may be under constant terrorist observation. All of these elements contribute to problems especially attendant to physical security of port operations. The most critical difference to be considered in the development of port defenses is the "obstacle" - water. The water may create an ingress route directly to the assets being protected. Watersides may be turned into an advantage if the proper planning, training, and exercises accept the limitations and advantages offered by a water environment.

Critical Questions:

- What person, staff, or unit is responsible for the port terminal?
- What product is the responsible person, staff, or unit to produce?
- How will this product be integrated into the overall AT/FP Plan?
- What forces are to provide security?

Considerations:

- Where are the hydrosurveys of the port?
- Are current grid maps available?
- What type of operation is conducted at the port (roll-on, roll-off/logistics over the shore)?
- What changes will be made during increased THREATCON status?
- What forces will be required to accomplish these changes?
- What equipment, materials, and time will be needed to make these changes?
- How many ships can be loaded/off loaded at a time?
- Do they off load / load civilian or foreign ships or only US military?
- What security force training will respond?
- What special equipment is needed by security forces?
- Are divers employed for survey and evaluation of port facilities?
- How are security personnel selected for water security forces?
- Are the dock workers military or civilian?
- Are host nation or third country nationals employed at the port?
- How long is cargo maintained on-site prior to transport?
- How is the marshaling yard secured for cargo?
- Is land transportation required for cargo?
- Are military working dogs employed for cargo inspection?
- Where is vehicle control point?
- What kind of heavy equipment is required for loading / unloading?
- Is there perimeter security?
- Are there boat patrols available?
- Are there static guard positions and roving patrols?

- Are there vehicle patrols?
- What special equipment is required for security forces?
- Where are the flammable materials maintained?
- Where is the Navy EOD team located?

Tab 1: Maritime Defensive Concepts

1. Joint Base on a Shoreline

The establishment of a base on a shoreline presents special advantages and challenges to those responsible for the functions inherent in the base's mission and for its defense. The advantages include the availability of the assets of more than one Service component for use by commanders in fulfilling their responsibilities. The special challenges may include the fact that facilities like ports and harbors are usually located in heavily populated areas. Command arrangements may be complicated by diverse purposes when multiple Service components use the same facilities. For example, the following installations may be in close geographical proximity:

- a. Army common-user water terminal;
- b. Support base for a MAGTF;
- c. Naval base supporting and sustaining fleet operations and/or naval coastal warfare operations, naval advanced logistic support site (ALSS), and naval forward logistic site (FLS); and
- d. Air Force base operating an aerial port of debarkation.

2. Command and Control

- a. The JFC designates the base commander, usually from the Service component with the dominant force on the installation.
- b. The JFC must designate the chain of command for security and defense, which may differ from the mission chain of command. In the case of multi-Service operations, each Service component facility may be designated a separate base as part of a base cluster commanded by the designated predominant Service commander. The base or base cluster may be directly subordinate to the joint headquarters, to a component commander, or to an area or functional commander. In the case of a large joint operation, the Army Material Command may have extensive ongoing contractor support operations (to open the port and remain throughout the operation as required). Command relationships must account for their presence and make allowance for any special protective measures. Examples of area or functional commanders are:
 - Marine force service support group commander;
 - Army transportation command commander, TAACOM commander, and ASG commander;
 - Naval coastal warfare commander, ALSS commander, and FLS commander;
 - Air Force component commander; and
 - Joint special operations component commander.

3. Defense Planning

- a. Potential Threats
 - Land-Based Attacks. Land threats to the base include all levels of threat discussed in the capabilities portion of the threat assessment.
 - Waterborne Attacks. Friendly naval forces and US Coast Guard are the primary defense against waterborne threats and should achieve naval superiority in the waters adjacent to the base. However, even if overall superiority is achieved, small enemy units may seek to interfere with base operations from seaward approaches.
 - Amphibious Raids. The enemy may attempt amphibious raids using watercraft and/or aircraft. Likely beaches, LZs, and insertion areas should be outposted, obstacles should be placed, and the mobile reserve employed to counter such raids.
 - Sea Mining. Enemy mining of the seaward approaches to the base can be conducted from surface vessels, by air, or clandestinely by submarines. Detection of such activity should be a priority effort for surveillance systems, patrol boats, and aircraft guarding the seaward approaches to the base.
 - Maritime Special Operations Forces. Determined, specially trained, organized, and equipped individuals or units can infiltrate ports, harbors, and bases near shore by swimming, scuba diving, high-speed surface craft, indigenous small boats, or miniature submersibles. They can damage vessels, port facilities, and base resources. Security

forces, both seaward and ashore, and their supporting surveillance systems must be prepared to locate and counter such threats.

b. Approaches to the Base. Appropriate security and surveillance forces, backed up by capable mobile reserve forces, must be designated to cover every possible avenue of approach. These approaches include:

- Beaches;
- Concealed water approaches (fjords, bayous);
- Rivers;
- DZs and LZs;
- Land approaches;
- Urban terrain and infrastructure (including underground water and sewage systems); and
- Piers, docks, and waterfront facilities.

c. Defense Forces

- Ground Defense Forces. Normally, the units operating the base facilities are the most common source of personnel and equipment to form a ground defense force. For especially critical facilities, dedicated defense forces such as Marine Corps security forces, Air Force security police, Army military police, or Marine Corps military police units may form the core of the ground defense effort.
- Air and Missile Defense. See Appendix C, "Air and Missile Defense."
- Navy and Coast Guard Organizations. The naval coastal warfare commander (NCWC) may form a port security and harbor defense group (PSHDGRU) to support defense efforts.
- The harbor defense commander (HDC) sets the boundaries for harbor defense for the PSHDGRU. Defense of the harbor is the responsibility of the HDC, and inland defense is the responsibility of the appropriate area or component commander designated by the JFC.
- Close coordination on mission priorities must be accomplished for naval coastal warfare units between the NCWC and base commander to avoid conflicts. On a larger scale, under the direction of the NCWC, the PSHDGRU may have OPCON of forces providing port security and harbor defense in more than one port and/or harbor. This may be particularly true along a coastline that has multiple ports in geographic proximity to each other. In this situation, the multiple ports may be designated a base cluster. The PSHDGRU will, through the NCWC, coordinate security operations with the appropriate area or functional commander. The PSHDGRU may possess some or all of the following capabilities.
- Mobile Inshore Undersea Warfare Unit. A mobile surveillance and detection unit that possesses surface radar, subsurface sonobuoy, swimmer detection and neutralization, and naval communications capabilities.
- Naval Explosive Ordnance Disposal (EOD) Detachment. This detachment provides ordnance handling and evaluation, special weapons and/or ammunition support, and mine detection and neutralization capabilities. This detachment also identifies mine and/or ordnance beaching areas for the port or harbor.
- Port Security Unit (PSU). This unit is provided by the US Coast Guard and is integrated into the Navy component in wartime or as allowed by law. The mission of a PSU is to conduct outside the continental US port security and/or harbor rear area operations in support of requesting combatant commanders. Port security elements include patrolling harbors and anchorages, maritime interdiction, surveillance, and the enforcement of exclusionary zones.
- Mine Countermeasures (MCM) Elements. These elements detect and destroy enemy mines in harbors, approaches, and sea lanes, using mine countermeasure aircraft and vessels. Because of the small number of MCM forces, control of these assets is normally determined by the Navy component commander.
- Mobile Diving and Salvage Unit (MDSU). The MDSU has the missions of underwater hull search and repair, channel clearance, vessel salvage, and pier and piling inspection and repair. The PSHDGRU commander can request this unit's support of base defense efforts from the NCWC when required.

- Naval Special Boat Unit (SBU) Detachments. SBU detachments are organized to conduct or support joint special operations and coastal patrol and interdiction with coastal and riverine craft. SBU detachments consist of various high-speed small craft up to the 175-foot ships of the Cyclone (PC-1) class. Most craft can mount crew-served weapons. When available and pending other priorities, the detachments can be requested to support base defense.

4. Planning Considerations

The following factors should be considered when planning the defense of a base on a shoreline.

- a. Type and nature of the threat.
- b. Protection for sea approach choke points.
- c. Tides and currents.
- d. Water clarity and depth.
- e. Pier clearance.
- f. Lighting.
- g. Use of patrol boats.
- h. Communications.
- i. Rail and highway entrances security.
- j. Air and missile defense measures.
- k. Security for individual vessels.
- l. Area damage control.

Appendix 18: Buildings

Purpose :

While the installation plan addresses overall security, the individual buildings and units that occupy those buildings are required to develop procedures for employment of AT/FP security measures for each individual building. Planners should ensure that all personnel are aware of the threat and proper individual security measures. They should conduct a vulnerability assessment of the building and employ proper security measures to upgrade the current security posture. They should plan for future upgrades (barriers, lighting, additional security guards) based on increased THREATCONs and integrate these measures into the overall AT/FP Plan.

A skilled and determined terrorist group can penetrate most office buildings. However, the presence and use of guards and physical security devices (e.g., exterior lights, locks, mirrors, visual devices) create a significant psychological deterrent. Terrorists are apt to shun risky targets for less protected ones. If terrorists decide to accept the risk, security measures can decrease their chance of success. Commanders should develop comprehensive building security programs and frequently conduct security surveys that provide the basis for an effective building security program. These surveys generate essential information for the proper evaluation of present security conditions and problems, available resources, and potential security policy. Being just one of the many facets in a complex structure, security policies must be integrated with other important areas such as fire safety, normal police procedures, work environment, and work transactions. The following information provides guidance when developing building security procedures.

- a. Buildings most likely to be terrorist targets should not be directly accessible to the public.
- b. Executive offices should not be located on the ground floor.
- c. Locate senior personnel at the inner core of the building. This affords the best protection and control of visitors and prevents people outside the building from obtaining visual surveillance.
- d. If building windows face public areas, reinforce them with bullet resistant materials and cover them with heavy curtains.
- e. Monitor access to executive offices with a secretary, guard, or other individual who screens all persons and objects entering executive offices.
- f. Place ingress door within view of the person responsible for screening personnel and objects passing through the door.
- g. Doors may be remotely controlled by installing an electromagnetic door lock.
- h. The most effective physical security configuration is to have doors locked from within and have only one visitor access door into the executive office area. Locked doors should have panic bars.
- i. Depending upon the nature of the organization's activities, deception measures such as a large waiting area controlling access to several offices can be taken to draw attention away from the location and function of a particular office.

Consider installing the following: security devices: burglar alarm systems (preferably connected to a central security facility), sonic warning devices or other intrusion systems, exterior floodlights, dead bolt locks on doors, locks on windows, and iron grills or heavy screens for windows. If feasible, add a 15- to 20-foot fence or wall and a comprehensive external lighting

Critical Questions:

- Who is responsible for the building security?
- How will the building security procedures be integrated into the overall AT/FP Plan?

Considerations:

- What is the purpose of the building?
- Who is the security manager?
- Has an AT/FP evaluation been conducted?
- Has an Individual Security Program been implemented?
- What is the threat to the installation?

- What tactics have been used in the past by these groups?
- What security systems are currently in use?
- Is the parking area an adequate distance from the building? If not, are measures identified for increased THREATCON status?
- Is there an access control system in place (parking/building)?
- What window treatments are in place or programmed?
- Is CCTV used for interior monitoring?
- Is CCTV used for monitoring the surrounding area?
- Where is the nearest fire fighting equipment?
- Are there duress buttons at key locations?
- Where should visitors park?
- Has furniture been selected to be fire retardant?
- Is there complete exterior lighting surrounding the building?
- Are there emergency power lights for the interior?
- What are the procedures for classified destruction?
- What are the ADP procedures?
- Have evacuation and other emergency plans been developed?

Tab 1: Mission Essential Vulnerable Asset (MEVA) Evaluation

This appendix identifies some potential MEVAs, and provides one manner a commander may use to preliminarily identify MEVAs at the installation. It is one of many “jump start” appendices in the template. It's use is not required to complete the plan.

The commander bears responsibility for determining the criticality of the installation's assets to successfully accomplish its mission, even if the threat inflicts casualties and destroys or damages assets. Upon completion of the Criticality Assessment, the installation commander will be able to determine MEVA.

MEVA may include:

- command headquarters
- computer center
- arms room
- communications center
- motor pool
- aviation complex
- any item(s) that will have an impact on the installation commander's mission.

By combining physical security system components into an integrated protection system (a “system of systems”), it is possible to achieve appropriate levels of protection for installation defense. Such systems can be prohibitively expensive if applied to each of the installation's facilities. Since resources are seldom unlimited, the Commander must establish physical security protection priorities based upon the MEVA.

The levels of priorities of protection include:

Level A: Assets, the loss, theft, destruction, or misuse of which will result in *Great harm to the strategic capability*.

Level B: Assets, the loss, theft, destruction, or misuse of which will result in *Grave harm the operational capabilities*.

Level C: Assets, the loss, theft, destruction, or misuse of which could *Impact upon the tactical capabilities*.

Level D: Assets, the loss, theft destruction or misuse of which could *Compromise the defense infrastructure*.

The commander should use all of the physical security expertise available. This expertise complements the technical knowledge in other staff areas. Sensitive equipment and/or complexes may require differing degrees and types of protection depending on the physical characteristics of each location, surrounding environment, and vulnerability to security hazards.

Tab 2: Area/Complex Physical Security Survey Tool

This physical survey identifies some potential MEVAs and supplies some considerations that may be applied to inclusion on the potential MEVA list. It is one of many “jump start” appendices in the template. Its use is not required to complete the plan.

1. Name of Building/Facility.
 - What is its use?
 - Who has access?
 - What security is currently in place?
 - (1) Active (personnel)
 - (2) Passive (physical means without immediate, continuing personnel oversight)
 - a. When was security tested last?
 - (1) Active
 - (2) Passive (the passive means by personnel)
 - b. Results of last security check.
 - (1) Active
 - (2) Passive (of the passive means by personnel)
 - c. Agency conducting security check(s).
 - d. Corrective action taken based on results/recommendations of last security check.
2. Blueprints.
 - a. Building(s)
 - b. Electrical
 - c. Plumbing
 - d. Heating/air-conditioning
 - e. Surrounding grounds (architectural drawings)
 - f. City prints of waterlines, sewage, gas
3. Critical buildings, components, substations, (refer to target analysis checklist)
4. Maps (no black and white reproductions).
 - a. 1:50,000 topographic
 - b. Tourist maps
 - c. City maps/Country maps
5. Mass Transit Systems.
 - a. Maps
 - b. Schedules
 - c. Terminals
 - d. Routes
 - e. Security
6. Police and Fire Departments.
 - a. Location
 - b. Schedules
 - c. Points of Contact
 - (1) Name
 - (2) Phone Number
 - d. Frequencies
 - e. Special Training.
 - (1) Currently trained special attention required for WMD/NBC capability, masks, detection, decontamination
 - (2) Required
 - f. List of available equipment
 - g. Last rehearsal and reaction time
 - h. Include phone procedures and a complete list of communications means with local hospitals, emergency rooms or clinics, hospital administrators.

7. Medical.
 - a. Location
 - b. Size
 - c. Capacities
 - d. Security and date of last rehearsal
 - e. Reaction time to mass trauma and last rehearsal
 - f. Special assets (helicopter pad, vehicles, airfields, medical treatment)
8. Communications/Power Systems.
 - a. Main terminals/substations
 - b. Layout of complete grid system (electrical and phone)
 - c. Grid system central points/communications control points
 - d. Special capabilities (tract, tap, isolate)
9. Municipal Emergency Plans.
 - a. Function of each organization
 - b. Location of crisis action command post
 - c. Chain of command
 - d. Last rehearsal of emergency plans
10. Photos.
 - a. Aerial (N,S,E,W, and direct overhead)
 - b. Ground photo facing out to surrounding area
 - c. Ground photo facing into facility
 - d. Determine location of "unfriendly" government buildings, commercial/social action/political organization, and areas of known unrest
11. History of activity as it effects the current government (if OCONUS).
12. Potential of negative activity against current government (if OCONUS).
13. List of all agencies, officials, and government with any degree of responsibility and authority.
14. List of any commercial corporations or private citizens who have significant "power behind the throne" influence.
15. Identify staging areas for emergency reaction teams.

Tab 3: CARVER Target Analysis Tool

The following is an explanation of the CARVER targeting process. This process is used by US Special Operations Forces (SOF) in targeting adversary's installations. For that reason it is included as a tool to evaluate US installations from an adversarial point of view. For those familiar with the CARVER tool, it may be used in addition to or in lieu of the assessment process recommended in Annex A. It is one of many "jump start" appendices in the template. Its use is not required to complete the plan.

TARGET ANALYSIS PROCESS

This appendix explains CARVER, which is a SOF term. CARVER is used by Army Special Operations (ARSOF) personnel, Security Information Officers, and operational personnel throughout the ARSOF targeting and mission planning process to assess mission, validity, and requirements. It is also used in technical appreciation and target analysis. This appendix provides a step-by-step example of how to use CARVER.

CRITICALITY, ACCESSIBILITY, RECUPERABILITY, VULNERABILITY, EFFECT, AND RECOGNIZABILITY FACTORS

The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value. This value represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicate the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent.

CRITICALITY

Criticality means target value. This is the primary consideration in targeting. A target is critical when its destruction or damage has a significant impact on military, political, or economic operations.

Targets within a system must be considered in relation to other elements of the target system. The value of a target will change as the situation develops, requiring the use of time-sensitive methods respond to changing situations. For example, when one has few locomotives, railroad bridging may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces that require use of such bridges. Criticality depends on several factors:

- Time: How rapidly will the impact of the target attack affect operations?
- Quality: What percentage of output, production, or service will be curtailed by target damage?
- Surrogates: What will be the effect on the output, production, and service?
- Relativity: How many targets are there? What are their positions? How is their relative value determined? What will be effected in the system or complex "stream"?

Table 1 shows how criticality values are assigned on CARVER matrixes.

Table 1. Assigning criticality values.

CRITERIA	SCALE
Immediate halt in output, production, or service; target cannot function without it.	9-10
Halt within 1 day, or 66% curtailment in output, production, or service	7-8
Halt within 1 week, or 33% curtailment in output, production, or service	5-6
Halt within 10 days, or 10% curtailment in output, production, or service	3-4
No significant effect on output, production or service	1-2

ACCESSIBILITY

A target is accessible when an operational element can reach the target with sufficient personnel and equipment to accomplish its mission. A target can be accessible even if it requires the assistance of knowledgeable insiders. This assessment entails identifying and studying critical paths that the operational element must take to achieve its objectives, and measuring those things that aid or impede access. The adversary must not only be able to reach the target but must also remain there for an extended period. The four basic steps identifying accessibility are:

- Infiltration from the staging base to the target area.
- Movement from the point of entry to the target or objective.
- Movement to the target's critical element.
- Exfiltration.

Factors considered when evaluating accessibility include, but are not limited to:

- Active and passive early warning systems.
- Swimmer detection devices.
- Air defense capabilities within the target area.
- Road and rail transportation systems.
- Type of terrain and its use.
- Concealment and cover.
- Population density.
- Other natural or synthetic obstacles and barriers.
- Current and climatic weather conditions.

The analysis along each critical path to the target should measure the time it would take for the action element to bypass, neutralize, or penetrate barriers and obstacles along the way. Accessibility is measured in terms of relative ease or difficulty of movement for the operational element and the likelihood of detection. The use of standoff weapons should always be considered in such evaluations. Table 2 shows how accessibility values are assigned on CARVER matrices.

Table 2. Assigning accessibility values

CRITERIA	SCALE
Easily accessible, standoff weapons can be employed	9-10
Inside a perimeter fence but outdoors	7-8
Inside a building but on ground floor	5-6
Inside a building but on second floor or in basement; climbing or lowering required	3-4
Not accessible or inaccessible without extreme difficulty	1-2

RECUPERABILITY

A target's recuperability is measured in time; that is, how long will it take to replace, repair, or bypass the destruction of or damage to the target? Recuperability varies with the sources and type of targeted components and the availability of spare parts availability. Factors which should be considered when assessing recuperability include, but are not limited to, the availability of :

- On-hand equipment such as railroad cranes, dry docks, and cannibalization.
- Restoration and substitution through redundancies.
- On hand spares.
- Equivalent OB equipment sets that backup critical equipment or components, and the effects of economic embargoes and labor unrest.

Table 3 shows how recuperability values are assigned on CARVER matrices.

Table 3. Assigning recuperability values

CRITERIA	SCALE
Replacement, repair, or substitution requires 1 month or more	9-10
Replacement, repair, or substitution requires 1 week to 1 month	7-8
Replacement, repair, or substitution requires 72 hours to 1 week	5-6
Replacement, repair, or substitution requires 24 to 72 hours	3-4
Same day replacement, repair, or substitution	1-2

VULNERABILITY

A target is vulnerable if the adversary has the means and expertise to successfully attack the target. When determining the vulnerability of a target, the scale of the critical component needs to be compared with the capability of the attacking element to destroy or damage it. In general, the attacking element may tend to:

- Choose special components.
- Do permanent damage.
- Prevent or inhibit cannibalization.
- Maximize effects through the use of onsite materials.
- Cause the target to self-destruct.

Specifically, vulnerability depends on:

- The nature and construction of the target.
- The amount of damage required.
- The assets available; for example, personnel, expertise, motivation, weapons, explosives, and equipment.

Table 4 shows how vulnerability values are assigned on CARVER matrices.

Table 4. Assigning vulnerability values.

CRITERIA	SCALE
Vulnerable to long-range laser target designation, small arms fire, or charges of 5 pounds or less	9-10
Vulnerable to light anti-armor weapons fire or charges of 5 to 10 pounds	7-8
Vulnerable to medium anti-armor weapons fire, bulk charges of 10 to 30 pounds, or very careful placement of smaller charges	5-6
Vulnerable to heavy anti-armor fire, bulk charges of 30 to 50 pounds, or requires special weapons	3-4
Invulnerable to all but the most extreme targeting measures	1-2

EFFECT

The effect of a target attack is a measure of possible military, political, economic, psychological, and sociological impacts at the target and beyond. This is closely related to the measure of target criticality. The type and magnitude of given effects desired will help the adversary select targets and target components for attack. Effect in this context addresses all significant effects, whether desired or not, that may result once the selected target component is attacked. Traditionally, this element has addressed the effect on the local population, but now there are broader considerations. Effect is frequently neutral at the tactical adversarial level.

For example, the primary effect of the destruction of two adjacent long-range radar sites in an early warning system may be to open a hole in the system that is of sufficient size and duration to permit our adversary to launch a successful attack against the installation. Effects can also include:

- The triggering of countermeasures.
- Support or negation of PSYOP themes.
- Unemployment.

- Reprisals against the civilian populace.
- Collateral damage to other targets.

Possible effects can be speculative and should be labeled as such. Effects of the same attack may be quite different at the tactical, operational, and strategic levels. For example, the destruction of a substation may not affect local power supply but cuts off all power to an adjacent region. Table 5 shows how effect values are assigned on CARVER matrices.

Table 5. Assigning effect values.

CRITERIA	SCALE
Overwhelmingly positive effects; no significant negative effects	9-10
Moderately positive effects; few significant negative effects	7-8
No significant effects, neutral	5-6
Moderately negative effects, few significant positive effects	3-4
Overwhelmingly negative effects; no significant positive effects	1-2

RECOGNIZABILITY

A target’s recognizability is the degree to which it can be recognized by the adversary and his intelligence collection and reconnaissance assets, under varying conditions. Weather has an obvious and significant impact on visibility. Rain, snow, and ground fog may obscure observation. Road segments with sparse vegetation and adjacent high ground provide excellent conditions for good observation. Distance, light, and season must also be considered. Other factors that influence recognizability include the size and complexity of the target, the existence of distinctive target signatures, the presence of masking or camouflage, and the technical sophistication and training of the adversary. Table 6 shows how recognizability values are assigned on CARVER matrixes.

Table 6. Assigning recognizability values

CRITERIA	SCALE
The target is clearly recognizable under all conditions and from a distance; it requires little or no training for recognition	9-10
The target is easily recognizable at small-arms range and requires a small amount of training for recognition	7-8
The target is difficult to recognize at night in bad weather, or might be confused with other targets or target component; it requires some training for recognition	5-6
The target is difficult to recognize at night or in bad weather, even with small-arms range; it is easily confused with other targets or components, it requires extensive training for recognition	3-4
The target cannot be recognized under any conditions, except by experts	1-2

CARVER MATRIX

These CARVER factors and their assigned values are used to construct a CARVER matrix. For the adversary this is a tool for rating the desirability of potential targets and wisely allocating attack resources. For the installation commander, it is a tool to counter the adversary.

To construct the matrix, list the adversary's potential targets in the left column. For strategic level analysis, list the installation's systems or subsystems (electric power supply, rail system). For tactical level analysis, list the complexes or components of the subsystems or complexes selected by your MEVA analysis. (Figure 1 shows a sample matrix for a bulk electric power supply facility.)

As each potential target is evaluated for each CARVER factor, enter the appropriate targets have been evaluated, add the values for each potential target. The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets. Attack those targets with the highest totals first.

If additional men and/or munitions are available, allocate these resources to the remaining potential targets in descending numerical order. This allocation scheme will maximize the use of limited resources. Planners can use the CARVER matrix to present the installation's staff with a variety of adversary defeat options. With the matrix they can discuss the strengths and weaknesses of each COA against the installation's targeted facility.

An initial CARVER report and targeting folder that highlights gaps in the data may be prepared at this step. The folder is used to develop a detailed collection and reconnaissance and surveillance (R&S) plan

For Example: **THE INSTALLATION'S BULK ELECTRIC POWER SUPPLY**

POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
FUEL TANKS	8	9	3	8	5	6	41
FULE PUMPS	8	6	2	10	5	3	34
BOILERS	6	2	10	4	5	4	31
TURBINES	8	6	10	7	5	9	45
GENERATORS	4	6	10	7	5	9	41
CONDENSERS	8	8	5	2	5	4	34
FEED PUMPS	3	8	5	8	5	4	33
CIR. WATER PUMPS	3	8	5	8	5	4	33
GENERATOR STEP UP TRANSFORMER	10	10	10	9	5	9	53

Figure 1. Complete CARVER matrix.

Annex E: REFERENCES

- National Security Strategy of the United States, 1997.
- Report to the President: The Protection of United States Forces Deployed Abroad, Secretary of Defense, William J. Perry. September 15, 1996.

DEPARTMENT OF DEFENSE

- National Military Strategy of the United States, September 1997.
- DODD 2000.12, "DOD Combating Terrorism Program," September 15, 1996.
- DOD Instruction 2000.16, "DOD Combating Terrorism Program Standards," July 21, 1997.
- DOD 0-2000.12-H, "Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence," February 1993.
- DODD 5200.8, "Security of DOD Installations and Resources," May 1991.
- DODD 5200.8-R, "Physical Security Program," May 1991.
- DOD 5200 1-R, "Information Security Program," January 1997.

JOINT

- JP 1-01.1, "Compendium of Joint Publications," April 25, 1995.
- JP 1, "Joint Warfare of the Armed Forces of the United States," January 1, 1995.
- JP 0-2, "Unified Action of Armed Forces," February 24, 1995.
- JP 1-02, "DOD Dictionary of Military and Associated Terms," March 23, 1994.
- JP 2-0, "Joint Doctrine for Intelligence Support to Operations," May 5, 1995.
- JP 2-01.2, "Joint Doctrine and Tactics, Techniques, and Procedures for Counter-Intelligence Support to Operations," April 4, 1994.
- JP 3-0, "Doctrine for Joint Operations." February 1, 1995.
- JP 3-07, "Joint Doctrine for Military Operations Other Than War," June 16, 1995.
- JP 3-07.1, "Joint Tactics, Techniques, and Procedures for Foreign Intelligence Defense," December 30, 1993.
- JP 3-07.2, "Joint Tactics, Techniques, and Procedures for Antiterrorism."
- JP 3-07.3, "Joint Tactics, Techniques, and Procedures for Peace Keeping Operations," April 29, 1994.
- JP 3-07.5, "Joint Tactics, Techniques, and Procedures for Non-Combative Evacuation Operations," September 30, 1997.
- JP 3-07.7, "Joint Tactics, Techniques, and Procedures for Domestic Support Operations."
- JP 3-10, "Doctrine for Joint Rear Area Operations," February 26, 1993.
- JP 3-10.1, "Joint Tactics, Techniques, and Procedures for Base Defense."
- JP 3-11, "Joint Doctrine for Nuclear, Biological, and Chemical Defense," July 10, 1995.
- JP 3-54, "Joint Doctrine for Operations Security," August 22, 1991.
- JP 3-58, "Joint Doctrine for Military Deception," June 6, 1994.
- JP 4-04, "Joint Doctrine for Civil Engineering Support," September 26, 1995.
- JP 5-0, "Doctrine for Planning Joint Operations," April 13, 1995.
- JP 5-00.3, "Doctrine for the Joint Operation Planning and Execution System."
- JP 5-03.1, "Joint Operation Planning and Execution System Volume I: (Planning Polices and Procedures)," August 4, 1993.

US ARMY

- FM 19-30, "Physical Security," March 1979.
- FM 101-5, "Staff Organization and Operations," May 31, 1997.
- FM 7-98, "Operations in a Low Intensity Conflict," October 19, 1992.
- FM 3-4-1, "Multi-Service Procedures for NBC Defense of Fixed Sites, Ports, and Airfields," November 7, 1997.
- AR 190-13, "The Army Physical Security Program," October 30, 1993.
- AR190-11, "Physical Security of Arms, Ammunition, and Explosives," October 30, 1993.
- AR 525-13, "The Army Force Protection Program," November 1997.

- TC 19-16, "Countering Terrorism on US Army Installations," April 25, 1983.
- Special Operations and International Studies: Political-Military Analysis Handbook, United States Army, JFK Special Warfare Center, August 1990.

US AIR FORCE

- AF Doctrine Document 2-3, "Military Operations Other Than War," October 5, 1996.
- AF Manual 32-4005, "Personnel Protection and Attack Actions," October 1, 1995.
- AF Instruction 10-404, "Base Support Planning."
- AF Instruction 14-105, "Unit Intelligence Mission and Responsibilities."
- AF Instruction 31-101, Volume I, "The Air Force Physical Security Program," December 1996.
- AF Instruction 31-209, "The Air Force Resource Protection Program," November 10, 1996.
- AF Instruction 31-210, "The Air Force Antiterrorism Program," January 7, 1997.
- AF Instruction 31-301, "Air Base Defense," August 1, 1996.
- AF Handbook 31-223, "The Air Force Resource Protection Program," February 1, 1997.
- AF Pamphlet 10-219, "Contingency and Disaster Planning," December 1, 1995.
- AF Policy Directive 31-1, "Physical Security," August 1, 1995.
- AF Policy Directive 31-3, "Air Base Defense," March 2, 1995.
- AF Policy Directive 31-4, "Information Security," August 1, 1997.
- AF Policy Directive 31-5, "Personnel Security Program Policy," August 1, 1995.
- AF Policy Directive 31-6, "Industrial Security," July 1, 1995.
- AF Policy Directive 31-7, "Acquisition Security," March 2, 1993.

US NAVY

- OPNAVINST 3300.53, "Navy Antiterrorism Program," 1992.
- OPNAVINST 3000.54, "Protecting Navy Personnel from Terrorist Attack," 1992.
- OPNAVINST 5530.13b, "Protection of Arms, Ammunition, and Explosives."
- OPNAVINST 5530.14b, "Physical Security and Loss Prevention," December 21, 1988.
- SECNAVINST 3300.2, "Navy Combating Terrorism Program."
- SECNAVINST 5530.4a, "Naval Security Forces Ashore and Afloat."

US MARINE CORPS

- FMFM 7-14, "USMC Combating Terrorism," October, 1990.
- MCBHO 5500.12D, "Base Physical Security/Terrorism Counter Action Plan."
- MCO 3302.1B, "USMC Antiterrorism Program," June 3, 1992.

Annex F: GLOSSARY

aircraft piracy. Any seizure or exercise of control, by force or violence or threat of force or violence or by any other form of intimidation and with wrongful intent, of an aircraft within the special aircraft jurisdiction of the United States. (Approved for inclusion in the next edition of Joint Pub 1-02)

antiterrorism. Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts to include limited response and containment by local military forces. Also called AT. (DOD Directive 0-2000.12) (Approved for inclusion in the next edition of Joint Pub 1-02)

combating terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) taken to oppose terrorism throughout the entire threat spectrum. (DOD Directive 0-2000.12-H and Joint Pub 1-02)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs. (Approved for inclusion in the next edition of Joint Pub 1-02)

counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism. (DOD Directive 0-2000.12)

deterrence. The prevention from action by fear of the consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. (Joint Pub 1-02)

high-risk personnel. U.S. personnel and their family members whose grade, assignment, travel itinerary, or symbolic value may make them an especially attractive or accessible terrorist targets. (DOD Directive 0-2000.12)

hostage. A person held as a pledge that certain terms or agreements will be kept. (The taking of hostages is forbidden under the Geneva Conventions, 1949). (Joint Pub 1-02)

incident control point. A designated point close to a terrorist incident where crisis management forces will rendezvous and establish control capability before initiating a tactical reaction. (Approved for inclusion in the next edition of Joint Pub 1-02)

initial response force. The first unit, usually military police, on the scene of a terrorist incident. (Approved for inclusion in the next edition of Joint Pub 1-02)

installation. A grouping of facilities, located in the same vicinity, which support particular functions. Installations may be elements of a base. (Joint Pub 1-02)

installation commander. The individual responsible for all operations performed by an installation. (Approved for inclusion in the next edition of Joint Pub 1-02)

insurgency. An organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict. (Joint Pub 1-02)

insurgent. Member of a political party who rebels against established leadership. (Approved for inclusion in the next edition of Joint Pub 1-02)

National Command Authorities. The President and the Secretary of Defense or their duly deputized alternates or successors. Commonly referred to as NCA. (Joint Pub 1-02)

negotiations. A discussion between authorities and a barricaded offender or terrorist to effect hostage release and terrorist surrender. (Approved for inclusion in the next edition of Joint Pub 1-02)

open source information. Information of potential intelligence value (i.e., intelligence information) that is available to the general public. (Joint Pub 1-02)

operations center. The facility or location on an installation, base, or facility used by the commander to command, control, and coordinate all crisis activities. (Approved for inclusion in the next edition of Joint Pub 1-02)

operations security. A process of identifying critical information and subsequently analyzing friendly actions attendant to operations and other activities to:

- a. Identify those actions that can be observed by adversary intelligence systems.
- b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.
- c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Also called OPSEC. (Approved for inclusion in the next edition of Joint Pub 1-02)

physical security. That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (Joint Pub 1-02)

prevention. The security procedures undertaken by the public and private sector in order to discourage terrorist acts. (Approved for inclusion in the next edition of Joint Pub 1-02)

primary target. An object of high publicity value to terrorists. (Approved for inclusion in the next edition of Joint Pub 1-02)

proactive. Measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur. (Approved for inclusion in the next edition of Joint Pub 1-02)

revolutionary. An individual attempting to effect a social or political change through the use of extreme measures. (Approved for inclusion in the next edition of Joint Pub 1-02)

saboteur. One who commits sabotage. (Approved for inclusion in the next edition of Joint Pub 1-02)

secondary targets. Alternative targets of lower publicity value. Attacked when primary target is unattainable. (Approved for inclusion in the next edition of Joint Pub 1-02)

signal security. A generic term that includes both communications security and electronic security. (Joint Pub 1-02)

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

matters affecting the relations between a military force and civilian authorities and population, they may be considered as civil affairs agreements. (Approved for inclusion in the next edition of Joint Pub 1-02)

tactical security. In operations, the measures necessary to deny information to the enemy and to ensure that a force retains its freedom of action and is warned or protected against an unexpected encounter with the enemy or an attack. (Approved for inclusion in the next edition of Joint Pub 1-02)

terrorism. The calculated use or use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (DOD Directive O-2000.12) (Approved for inclusion in the next edition of Joint Pub 1-02)

terrorist. An individual who uses violence, terror, and intimidation to achieve a result. (Approved for inclusion in the next edition of Joint Pub 1-02)

terrorist groups. Any element regardless of size or espoused cause, which repeatedly commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives. (Approved for inclusion in the next edition of Joint Pub 1-02)

threat analysis. In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups that could target a facility. A threat analysis will review the factors of a terrorist group's existence, capability, intentions, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying probability of terrorist attack and results in a threat assessment. (Approved for inclusion in the next edition of Joint Pub 1-02)

threat and vulnerability assessment. In antiterrorism, the pairing of a facility's threat analysis and vulnerability analysis. (Approved for inclusion in the next edition of Joint Pub 1-02)

Annex G: ACRONYMS

AA&E - Arms Ammunition and Explosives
AAR - After Action Review
AC - Aircraft
ALSS - Advanced Logistic Support Site
ASF - Auxiliary Security Force
AT/FP - Antiterrorism/Force Protection
CI - Counterintelligence
CIA - Central Intelligence Agency
CINC - Commander in Chief
CJCS - Chairman of the Joint Chiefs of Staff
CM - Consequence Management
CMT - Crisis Management Team
COA - Course of Action
COMSEC - Communications Security
CONUS - Continental United States
CT - Counterterrorism
DIA - Defense Intelligence Agency
DOD - Department of Defense
DOJ - Department of Justice
DON - Department of the Navy
EEI - Essential Element of Information
EOD - Explosive Ordnance Disposal
FBI - Federal Bureau of Investigation
FLS - Forward Logistic Site
FRAGO - Fragmentary Order
HAV - Heavily Armored Vehicle
HAZMAT - Hazardous Material
HDC - Harbor Defense Commander
HN - Host Nation
HRP - High Risk Personnel
HUMINT - Human Intelligence
IAW - in accordance with
IDS - Intrusion Detection System
IED - Improvised Explosive Device
IG - Inspector General
IMINT - Image Intelligence
INFOSEC - Information Security
IO - Information Operations
IPB - Intelligence Preparation of the Battlefield
ISB - Internal Security Branch
JFK SWCS - John F. Kennedy Special Warfare Center/School
JIC - Joint Intelligence Center
JISE - Joint Intelligence Support Element
LAV - Lightly Armored Vehicle
LEA - Law Enforcement Agency
LOTS - Logistics Over the Shore
LZ - Landing Zone
MAGTF - Marine Air-Ground Task Force
MCM - Mine Countermeasures
MDSU - Mobile Diving and Salvage Unit
METL - Mission Essential Task List
MEVA - Mission Essential Vulnerable Asset

MILCON - Military Construction
MOA - Memorandum of Agreement
MOPP - Mission Oriented Protective Posture
MOU - Memorandum of Understanding
NATO - North Atlantic Treaty Organization
NBC - Nuclear, Biological, and Chemical
NCWC - Naval Coastal Warfare Commander
NMJIC - National Military Joint Intelligence Center
OCONUS - Outside the Continental United States
OPLAN - Operation Plan
OPORD - Operation Order
OPSEC - Operations Security
OSINT -Open Source Intelligence
PAO - Public Affairs Officer
PMO - Provost Marshal's Office
POC - Point of Contact
PSO - Personnel Security Officer
PSU - Port Security Unit
RA/M - Risk Assessment/Management
RAM - Random Antiterrorism Measures
ROE - Rules of Engagement
RORO - Roll On Roll Off
RSO - Regional Security Officer
SBU - Special Boat Unit
SIGINT - Signal Intelligence
SJA - Staff Judge Advocate
SOI - Standing Operating Instructions
SOP - Standing Operating Procedure
TAACOM - Transportation and Command Commander
TECHINT - Technical Intelligence
THREATCON - Threat Conditions
TSC - Tasks/Conditions/Standards
UN - United Nations
USA - United States of America
USAF - United States Air Force
USCENTCOM - United States Central Command
USDR - United States Defense Representative
USG - United States Government
USMC - United States Marine Corps
USN - United States Navy
VIP - Very Important Person
WAN - Wide Area Network
WMD - Weapons of Mass Destruction