AIR FORCE HANDBOOK 10-222, VOLUME 3
1 May 2008

CIVIL ENGINEER GUIDE TO EXPEDITIONARY FORCE PROTECTION

DEPARTMENT OF THE AIR FORCE

This Page Intentionally Left Blank

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE HANDBOOK 10-222, VOLUME 3
1 May 2008
Certified Current 27 May 2011
Operations

CIVIL ENGINEER GUIDE TO EXPEDITIONARY FORCE PROTECTION

ACCESSIBILITY: This publication is available on the e-Publishing website at http://www.e-publishing.af.mil for downloading and ordering.

RELEASABILITY: There are no releasability restrictions.

OPR: HQ AFCESA/CEXX

Certified by: HQ AF/A7CX
(Colonel Donald L. Gleason)
Pages: 97

Supersedes: AFH 10-222V3
1 June 1997

This handbook supports force protection training outlined in AFI 10-210, *Prime Base Engineer Emergency Force (BEEF) Program*. It describes expeditionary force protection tactics, techniques, and procedures (TTPs) Air Force (AF) civil engineers can use to protect critical assets including personnel, facilities and equipment during deployments. It is applicable to active duty, Air National Guard, and Air Force Reserve engineers. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMTs 847 from the field through Major Command (MAJCOM) publications/forms managers. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) at https://afrims.amc.af.mil. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This publication has been substantially revised and must be completely reviewed. This revision incorporates the latest force protection tactics, techniques, and procedures used by civil engineers deployed in expeditionary environments. It includes antiterrorism guidance and standards from the most recently published unified facilities criteria (UFCs) and addresses the civil engineer's role in supporting integrated base defense (IBD).

Chapter 1— INTRODUCTION. 7

1.1. Overview. 7

1.2. Force Protection Defined. 7

1.3. Elements of Force Protection. 8

1.4. Operations Security (OPSEC). 8

1.5. Force Protection Condition (FPCON) System. 9

Table 1.1. Force Protection Conditions. 9

1.6. Terrorist Threat Levels. 10

Table 1.2. Terrorist Threat Levels. 10

1.7. Training. 11

Figure 1.1. Levels of Antiterrorism Training. 11

Chapter 2—COMBATING TERRORISM. 12

2.1. Overview. 12

Figure 2.1. Berm Construction. 12

2.2. Antiterrorism. 13

2.3. Counterterrorism. 13

2.4. Threat Assessment. 14

2.5. Criticality Assessment. 15

2.6. Vulnerability Assessment. 15

2.7. Risk Management. 16

2.8. Random Antiterrorism Measures (RAMs). 16

Chapter 3—FORCE PROTECTION PLANNING. 17

3.1. Overview. 17

Figure 3.1. Force Protection Planning. 17

3.2. Force Protection Plan. 18

3.3. Resource Constraints. 18

3.4. Site Selection. 19

3.5. Site Layout. 19

3.6. Unified Facilities Criteria. 21

Table 3.1. Levels of Protection – New and Existing Buildings. 23

Table 3.2. Levels of Protection – Expeditionary and Temporary Structures. 24

Table 3.3. Standoff Distances for New and Existing Buildings. 26

Figure 3.2. Standoff Distances – Controlled Perimeter. 27

Figure 3.3. Standoff Distances – No Controlled Perimeter. 27

Figure 3.4. Parking and Roadway Control for Existing Buildings—Controlled Perimeter. 28

Figure 3.5. Parking and Roadway Control for Existing Buildings – No Controlled Perimeter. 28

Table 3.4. Standoff Distances and Separation for Expeditionary and Temporary Structures. 29

Figure 3.6. Standoff Distances and Separation for Expeditionary and Temporary Structures. 30

Chapter 4—PHYSICAL SECURITY. 31

4.1. Overview. 31

4.2. Aspects of Physical Security. 31

4.3. Perimeter Security. 32

Figure 4.1. Perimeter Security Measures. 32

Figure 4.2.Typical Barrier Plan. 34

Figure 4.3. Portable Barrier. 35

Figure 4.4. Drum Barrier. 35

Figure 4.5. Retractable Bollards. 36

Figure 4.6. Lift Plate Barricade System. 36

Figure 4.7. Sliding Gate. 36

Figure 4.9. Non-Retractable Bollards. 37

Figure 4.10. Steel Hedgehog Barrier. 38

Figure 4.11. Expedient Barrier - Equipment Tires. 38

Figure 4.12. Concrete Jersey Barrier. 38

Figure 4.13. Sand Bags. 39

Figure 4.14. HESCO Barriers. 39

Figure 4.15. Perimeter Fences and Barriers. 40

Figure 4.16. Grille Installed On Drainage Culvert. 41

Figure 4.17. Typical Entry Control Facility. 42

Figure 4.18. Entry Control Facility Zones. 44

Figure 4.19. Jersey Barriers Cabled Together. 45

Figure 4.20. Barriers Used to Form Serpentine Path. 46

Figure 4.21. Berms and Ditches. 47

Figure 4.22. Security Lighting and Intrusion Detection System. 48

Figure 4.23. Obscuration Screen on Perimeter Fence. 49

Figure 4.24. Observation Posts, Guard Towers, and Defensive Fighting Positions. 50

Table 4.1. HESCO Container Sizes and National Stock Numbers. 51

Figure 4.25. Illustration of Different Sizes of HESCO Containers. 51

4.4. Internal Security. 52

Figure 4.26. Internal Security Measures. 52

Figure 4.27. Mass Notification System. 53

Figure 4.28. Expeditionary Structures. 54

Figure 4.29. Blast and Fragmentation Hazard Zones. 55

Figure 4.30. Compacted Soil Revetment. 57

Figure 4.31. Fragmentation Retention Film. 58

Figure 4.32. Example of Compartmentalization. 59

Figure 4.33. Predetonation Screening. 60

Figure 4.34. Revetments. 61

Figure 4.35. Personnel Protective Shelter. 62

Figure 4.36. Expeditionary Power Plant. 63

Figure 4.37. Burying Utility Lines. 64

Figure 4.38. Camouflage Netting Being Applied. 65

Figure 4.39. Contractors Providing Power Support - Camp Taji (Iraq). 66

Chapter 5—INTEGRATED BASE DEFENSE (IBD). 67

5.1. Overview. 67

5.2. Essential Capabilities of IBD. 67

Figure 5.1. Essential Capabilities of Integrated Base Defense. 68

Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION. 72

Attachment 2—BASELINE FPCON MEASURES. 86

Attachment 3—SITE SELECTION AND LAYOUT CONSIDERATIONS. 93

Chapter 1

INTRODUCTION

1.1. Overview. Force Protection (FP) is an overarching concept that should not be used synonymously with Antiterrorism (AT). AT is a sub-element of combating terrorism, which is a subset of the broader FP concept. FP is inherent to command and must be a commander's top priority at all times. This handbook provides guidance on implementing FP measures in the expeditionary environment. Many of the references listed throughout this handbook are For Official Use Only (FOUO) publications. Planners should gain access to these publications and download them to secure media to ensure they are available throughout all phases of deployments.

1.2. Force Protection Defined. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines FP as "actions taken to prevent or mitigate hostile actions against Department of Defense (DOD) personnel and their families, resources, facilities, and critical information." This protection is necessary to ensure the force is fit and capable of applying decisive and overwhelming force at the right place and time to achieve US objectives. Concern for the health and welfare of the force must always be paramount. FP efforts must be geared towards coordinated and synchronized offensive and defensive measures which enable effective employment of forces while simultaneously degrading opportunities for the enemy. The DOD definition excludes actions to defeat the enemy or protect against accidents, weather, or disease as elements of force protection. Air Force Doctrine Document (AFDD) 2-4.1, *Force Protection*, states that the AF views FP as an integrated application of offensive and defensive actions to deter, detect, preempt, mitigate, or negate threats against USAF air and space operations and assets based on an acceptable level of risk. Key to the AF view of FP is the protection of its people. It is important to note that the AF considers prevention of accidents, along with protection against various forms of disease, especially those induced through hostile action, to also be elements of FP.

1.3. Elements of Force Protection. Force protection includes efforts designed to prevent attacks on DOD assets and interests and minimize the effect of any attacks. It is unrealistic to assume every DOD asset can be protected. For this reason, plans and preparations to recover from an attack must be focused on enabling the mission to continue and restoring confidence throughout the unit and local population.

1.3.1. **Deterrence**. Seek to deter incidents by discouraging terrorists from planning against, targeting, or attacking DOD interests. Measures civil engineers can take include placing barriers and roadblocks, strategically locating assets, and ensuring sufficient standoff to reduce the chances of an attack.

1.3.2. **Countermeasures**. Commanders employ an appropriate mix of countermeasures, both active and passive, to prevent terrorists from attacking DOD assets. A description of these countermeasures and their application are outlined in Air Force Tactics, Techniques, and Procedures (AFTTP) 3-10.1, *Integrated Base Defense*.

1.3.3. **Mitigation**. Commanders employ the full range of active and passive measures such as hardening and sidewall protection to lessen the impact of terrorist events against DOD assets.

1.3.4. **Recovery**. Commanders design plans to recover from the effects of a terrorist incident while continuing the mission. Air Force emergency management procedures are outlined in AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*.

1.4. Operations Security (OPSEC). OPSEC is a key element of FP and must be integrated into all aspects of military operations to identify critical information, which may be vulnerable to being collected and used by adversaries to harm personnel or destroy mission-critical assets. Once an analysis of vulnerabilities is complete, OPSEC measures must be implemented for each vulnerability identified. Refer to AFI 10-701, *Operations Security*, and JP 3-13.3, *Operations Security,* for additional information on OPSEC measures.

1.5. Force Protection Condition (FPCON) System. The FPCON system standardizes threat identification, recommended preventive measures and responses to terrorist threats against US personnel and facilities (**Table 1.1**). FPCON *measures* are actions taken to deter and/or prevent terrorists from conducting an attack. FPCON measures incorporate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal protection to personnel and assets and should be tailored to a specific site. FPCONs should not be confused with threat levels. Threat levels are the result of threat assessments and are used to assist in determining local FPCONs. The objective is to ensure an integrated approach to terrorist threats. Baseline FPCON levels and measures are listed in DOD Instruction (DODI) 2000.16, *DOD Antiterrorism (AT) Standards*. **Attachment 2** contains examples of FPCON measures civil engineers may implement during increased FPCON levels.

Table 1.1. Force Protection Conditions.

Normal	A general global threat of possible terrorist activity exists and warrants a routine security posture. At a minimum, access control will be conducted at all DOD installations and facilities.
Alpha	Increased general threat of possible terrorist activity against personnel or facilities. Nature and extent of the threat are unpredictable. FPCON Alpha measures must be capable of being maintained indefinitely.
Bravo	Increased or more predictable threat of terrorist activity. Sustaining FPCON Bravo measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.
Charlie	An incident occurs or intelligence is received indicating some form of terrorist action or targeting of personnel or facilities is likely. Prolonged implementation of FPCON Charlie measures may create hardship and affect the activities of the unit and its personnel.
Delta	Applies in the immediate area where a terrorist attack has occurred or when intelligence is received indicating that terrorist action against a specific location or person is imminent. This FPCON is usually declared as a localized condition. FPCON Delta measures are not intended to be sustained for an extended duration.

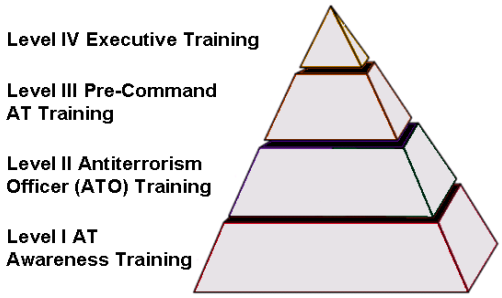
1.6. Terrorist Threat Levels. Terrorist threat levels reflect an intelligence assessment of threats against US personnel and interests in foreign countries. The Defense Intelligence Agency (DIA) sets the DOD terrorism threat level in a particular country, region, or locale. It is based on continuous intelligence analysis of several factors such as a terrorist group's existence, operational capability, intentions, activity, and the operational environment. Geographic combatant commanders also set terrorist threat levels for specific personnel, family members, units, and installations within their areas of responsibility using definitions established by the DIA. Terrorist threat levels should not be confused with FPCONs set by commanders that affect the local security posture. Threat level assessments are provided to senior leaders to help determine local FPCONs. Terrorist threat levels should also not be confused with threat conditions associated with the National Homeland Security Advisory System. **Table 1.2** describes the different threat levels and combination of factors used to determine each threat level. Additional sources on terrorist threat levels include DODI 2000.16; DOD O-2000.12-H (FOUO), *DOD Antiterrorism Handbook;* JP 3-07.2*, Joint Tactics, Techniques, and Procedures for Antiterrorism;* and AFI 10-245, *Air Force Antiterrorism (AT) Standards.*

Table 1.2. Terrorist Threat Levels.

Low	No group is detected or the group's activity is non-threatening.
Moderate	Terrorists are present but there are no indications of anti-US activity. The operating environment favors the Host Nation/US
Significant	Anti-U.S. terrorists are present and attack personnel as their preferred method of operation or a group uses large casualty-producing attacks as their preferred method but has limited operational activity. The operating environment is neutral.
High	Anti-U.S. terrorists are operationally active and use large casualty- producing attacks as their method of operations. There is a substantial DOD presence and the operating environment favors the terrorist. An incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely.

1.7. Training. Training is essential to establishing an effective FP program. DOD Instruction 2000.16 specifies minimum AT training requirements. To enable commanders to make the most effective decisions possible, personnel at all organizational levels should receive specialized FP training. The current FP training for DOD personnel consists of four levels (**Figure 1.1**). Level I training is an introduction to terrorism and terrorism operations and must be completed by military, DOD civilians, and family members prior to deployment. It includes topics such as personal protective measures, terrorist surveillance techniques, improvised explosive devices, and kidnapping and hostage survival tactics. Level I training is available on the DOD Antiterrorism website located at https://atlevel1.dtic.mil/at. DOD O-2000.12-H and JP 3-07.2 are additional sources that can be used to conduct Level I training. Level II training is a resident course designed to prepare officers and NCOs to serve as advisors to unit commanders on FP matters. Level III training is part of the O5/O6 level pre-command course. Level IV training includes a senior commander/executive-level seminar. Refer to AFI 10-245 to obtain training sources for levels II through IV.

Figure 1.1. Levels of Antiterrorism Training.



Chapter 2

COMBATING TERRORISM

2.1. Overview. Combating terrorism within DOD encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of chemical, biological, radiological, or nuclear materials or high-yield explosive devices. Where counterterrorism is offensive, antiterrorism is defensive. Antiterrorism focuses on defensive measures taken to reduce the vulnerability of individuals and property to terrorist acts. Air Force civil engineers are relied upon to implement antiterrorism and counterterrorism measures, such as fence and berm construction (**Figure 2.1**), particularly in expeditionary environments where the threat level is high due to ongoing military operations.

Figure 2.1. Berm Construction.

2.2. Antiterrorism (AT). AT refers to defensive measures taken to reduce the vulnerability of personnel, facilities, and equipment to acts of terrorism. As stated earlier, AT should not be used as a synonymous term with Force Protection. Rather, AT is a sub-element of combating terrorism, which is a subset of the broader FP concept. The AT program must be a collective, proactive effort focused on detecting and preventing terrorist attacks, preparing to defend against attacks, and responding to consequences of terrorist incidents. In the expeditionary environment, three key areas where civil engineers contribute significantly to AT are: (1) ensuring sufficient standoff between identified threats and mission-critical assets, (2) perimeter security, and (3) mitigation of blast and fragmentation effects through facility hardening and other means. Reference JP 3-07.2 and AFI 10-245 for additional details on AT standards and procedures.

2.3. Counterterrorism. Counterterrorism refers to offensive measures taken to prevent, deter, and respond to terrorism. US counterterrorism policy is based upon four principles: (1) the government makes no concessions to or agreements with terrorists; (2) terrorists must be brought to justice for their crimes; (3) states that sponsor terrorists and terrorism must be isolated and pressured so as to force a change of behavior; and (4) the counterterrorism capabilities of countries allied with the US, and those requiring assistance in fighting terrorism, must be bolstered. Civil engineers contribute to counterterrorism efforts in many ways similar to those actions taken to support antiterrorism efforts (i.e., ensuring effective standoff, placing barriers, etc). To support counterterrorism efforts, civil engineers also assist security forces in establishing a defense in-depth capability (also called a layered defense) as part of the Integrated Base Defense (IBD) concept. These efforts provide additional deterrence and increases the time needed for security forces to respond and neutralize threats in the event of an attack. **Chapter 5** provides more details on civil engineer roles in IBD.

2.4. Threat Assessment. The threat assessment is the process used to conduct an analysis and develop an evaluation of a potential threat. It is usually conducted by intelligence personnel such as the Air Force Office of Special Investigations (AFOSI). All available information concerning enemy activities is analyzed to determine if personnel and/or critical assets might be targeted. The analysis includes factors such as a terrorist group's existence, capability, intentions, history, and targeting as well as the security environment within which friendly forces operate. DODI 2000.16 contains guidance on conducting threat assessments.

2.4.1. **Identifying the Threat**. The threat must be described in specific terms and should include the types of aggressors (i.e., terrorists, saboteurs, spies, extremist protestors, criminals, etc.) and the types of weapons, tools, and explosives likely to be used in an attack or an attempt to compromise a military asset. The threat identification should also include tactics likely to be used, such as stationary or moving vehicle bombs, bomb delivery via mail or supply shipments, airborne or waterborne contamination, forced or covert entry, standoff or ballistic weapons, visual surveillance, acoustic eavesdropping, and insider compromise. As an example, the threat might be described as a moving vehicle bomb consisting of a 4,000-pound vehicle containing a 500-pound explosive. Identifying the specific threat will help in determining asset vulnerability. This information can then be used by civil engineers to develop and implement protective measures to counter the specified threat.

2.4.2. **Planning for the Threat**. The threat level assigned to the country or region where a unit may be deploying will help to plan protective measures throughout all phases of deployments, including predeployment, initial beddown, sustainment, and redeployment. Upon notification of deployment, unit commanders should immediately contact their servicing AFOSI detachment and request a counterintelligence threat assessment. For planning purposes, UFCs 4-010-01, *DOD Minimum Antiterrorism Standards For Buildings*, and 4-020-01, *DOD Security Engineering Facility Planning Manual*, contain detailed information on expeditionary site layout and protective measures designed to mitigate the effects of attacks on expeditionary and temporary structures as well as existing structures.

2.5. Criticality Assessment. The criticality assessment is the process used to systematically identify key assets (i.e., personnel, equipment, stockpiles, buildings, etc.) deemed mission critical by commanders based on their importance to the mission or function. This assessment forms the basis for prioritizing assets requiring high levels of protection. It addresses the impact of temporary or permanent loss of key assets, installation infrastructure, or a unit's ability to perform its mission. The assessment considers resources needed (i.e., time, funding, capability, infrastructure support, etc.) to recover or reconstitute an asset to enable the mission to continue with minimum interruption. The commander appoints a team to conduct the assessment, taking into consideration all of the factors mentioned above, and produces a prioritized list of critical assets. Areas encompassing multiple critical assets are referred to as critical areas. Detailed information on conducting criticality assessments can be found in DOD O-2000.12-H and JP 3-07.2.

2.6. Vulnerability Assessment. Terrorists conduct surveillance of US assets to determine a target's suitability for attack. Terrorists look for weaknesses in FP measures and security procedures that provide opportunities to attack targets at their greatest vulnerability. A vulnerability assessment is an evaluation of the site to determine if key assets are provided the appropriate level of protection. Minimum standards are applied where a specific threat has not been identified. Higher levels of protection are provided where a specific threat has been identified. During the assessment, the terrorist threat, including likely tactics, must be analyzed to determine what assets are vulnerable to attack by what means. Vulnerabilities are gaps in protection for key assets. They are identified by considering tactics associated with certain threats and levels of protection designed to defeat these tactics. Vulnerabilities may involve inadequacies in intrusion detection systems (IDSs) and barriers, inadequate standoff distances, and building construction that cannot resist explosive effects at the established standoff distance. Where vulnerabilities are identified, protective measures must be implemented to counter them. DODI 2000.16 contains guidance on conducting vulnerability assessments. The Defense Threat Reduction Agency (DTRA) website, located at http://www.dtra.mil/, also contains a wealth of information and guidelines for conducting vulnerability assessments.

2.7. Risk Management. Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions to balance risk costs with mission benefits. This process is called a risk assessment. Risk assessments provide commanders with a method to assist them in making resource allocation decisions designed to protect their personnel and assets from possible terrorist threats in a resource-constrained environment. The risk assessment is based upon three critical components: threat, criticality, and vulnerability assessments. It is conducted after completing all other assessments. Any plan that does not start with these assessments will probably be too reactive and result in wasted efforts and resources. Once vulnerabilities are identified, commanders manage risk by developing strategies to deter terrorist incidents, employing countermeasures, and mitigating the effects and developing plans to recover from terrorist incidents. Civil engineers participating in the development of FP and AT plans should also participate in the risk assessment. The information collected during the risk assessment is critical to developing effective FP and AT plans. For more information on risk management, refer to AFTTP(I) 3-2.34, *Multi-service Tactics, Techniques, and Procedures for Risk Management*.

2.8. Random Antiterrorism Measures (RAMs). RAMs are random, multiple security measures that consistently change the look of a site's FP posture. RAMs introduce unpredictability into the site's overall force protection program. By randomly selecting and implementing FPCON measures at different levels, surveillance attempts by terrorists will be frustrated and difficult. It will be harder for them to predict certain actions or discern patterns or routines that may reveal vulnerabilities. Other security measures not normally associated with FPCONs (e.g., locally developed, site-specific) can also be employed randomly to supplement the basic FPCON measures already in place. A list of baseline FPCON measures can be found at **Attachment 2** of this handbook and in AFI 10-245 and DOD Instruction 2000.16. These measures must be exercised regularly and associated plans must be adjusted to correct any inadequacies.

Chapter 3

FORCE PROTECTION PLANNING

3.1. Overview. Force protection planning should be conducted throughout all phases of contingencies. (**Figure 3.1**). Key aspects of FP planning involving civil engineers include site selection and site layout. Most protective measures applied in the expeditionary environment will be focused on site work. Use the site survey to learn as much as possible about the deployed location. Acquire necessary equipment, tools, and materials to implement protective measures prior to deploying. Refer to UFC 4-020-01 when developing cost estimates for expeditionary construction. Once deployed, some items may be difficult if not impossible to obtain. To effectively address the requirements of both site selection and site layout, civil engineers must first be familiar with UFCs that address FP and AT standards. This chapter covers FP planning, site selection, site layout, and the criteria established to ensure minimum AT standards are met while conducting these activities. Guidance on attaining higher levels of protection when deemed necessary by commanders is also covered.

Figure 3.1. Force Protection Planning.

3.2. Force Protection Plan. The FP Plan consists of specific measures developed to protect personnel, facilities, and critical assets. It includes elements such as the threat assessment, threat level, vulnerability assessment, criticality assessment, risk assessment, and FPCON measures. The commander will usually establish a Force Protection Working Group to develop the FP Plan. Civil engineers should focus on the physical security and IBD aspects of the FP Plan. It should include elements that contribute to IBD and the protection of key assets such as site layout, barrier placement, berm construction, security lighting, backup power, water source protection, expedient hardening, and terrain modification. Absolute protection against terrorist activities is not possible. Therefore, protective plans and procedures must be based on the threat identified by intelligence personnel. Considering the threat, protective measures should strike a reasonable balance between the protection required, mission requirements, available manpower, and available resources. The FP Plan itself should not be an end state. The plan should be a living document that is constantly reviewed and revised as threats, resource requirements, and innovations cause changes in FP tactics.

3.3. Resource Constraints. Some of the resources needed to implement FP plans include time, manpower, materials, equipment, and funding. Resources can be committed to FP by the installation at anytime during the process of conducting the threat, vulnerability, or criticality assessments. The commitment of resources could also be delayed until all assessments are complete and an analysis of the risks (risk assessment) can be examined. However, commanders will most likely use risk management to allocate resources towards those assets found to be most vulnerable to the identified threat and that if damaged or destroyed, would have the most damaging effect on the mission. Although FP is inherently a top priority for all commanders, limited resources under certain circumstances during some stages of deployment may cause risks to be high until additional resources can be obtained. Civil engineers must be adamant and persistent in efforts to obtain additional resources needed to apply the most effective FP measures needed to counter threats identified by the intelligence community. Most of the efforts to obtain FP resources should be accomplished during the predeployment phase and reassessed immediately upon deployment.

3.4. Site Selection. Civil engineers should participate in the site survey and learn as much as possible about the region and specific location to assist in selecting a site suitable to beddown the expected population, weapon systems, support equipment, and other assets. These factors must be considered along with the need for standoff. Many expeditionary and temporary structures are composed of metal frames and fabric or wood frames and rigid walls. These types of structures are generally impractical to harden or retrofit. For this reason, standoff distance is the primary approach to FP in the expeditionary environment, which drives the need for larger sites. Space should be sufficient to allow for dispersal of certain functions and equipment and to provide the commander the flexibility to increase the beddown population and standoff distances if needed in response to higher threat levels. This is a good time to develop a list of equipment, tools, and materials needed to immediately implement protective measures upon arrival to the deployed site.

3.5. Site Layout. This is an extremely important process in FP planning. If the site layout is not well thought out, it could be very difficult and costly to rearrange assets to provide increased protection once beddown is complete. Site layout must be based largely upon the known threat to personnel, mission-critical assets, support facilities and equipment from each likely enemy tactic (i.e., standoff weapons, vehicle bombs, etc.). Some key planning aspects of site layout include standoff distances, orientation of facilities, layout of roads, entry control points, layered defense tactics, physical barriers, sidewall protection and facility hardening, dispersal, compartmentalization, observation posts, defensive fighting positions, and personnel bunkers. All of these areas will be covered in more detail in **Chapter 4**. **Attachment 3** contains some key FP elements to consider during site selection and site layout and can be used as a quick reference checklist. This list is not all-inclusive. Every deployment is unique and therefore presents unique challenges. The following paragraphs provide more details on site layout. While conducting site selection and site layout functions, use available geographical information system (GIS) tools to enhance FP plans. The data provided by GIS tools can be used to enhance survivability efforts and ensure minimum AT standards are met.

3.5.1. **Maximize Standoff Distance**. Putting maximum distance between personnel, critical assets, and potential threats is generally the easiest, most economical, and most effective FP strategy. Maximizing distance provides the flexibility to attain higher levels of protection to counter increased threats. Standoff distances differ for base camps with controlled perimeters and those without controlled perimeters. If a controlled perimeter does not exist, standoff distances will be greater. When standoff distances cannot be achieved, structures should be analyzed by an engineer experienced in blast resistant design. Install recommended hardening to mitigate potential blast effects.

3.5.2. **Provide Effective Building Layout**. Effective building layout and orientation can significantly limit terrorist surveillance capabilities and targeting opportunities. This is particularly important when areas directly outside of an installation are not under the installation's control. Ensure that the main entrance to a facility/structure does not face the perimeter or other uncontrolled vantage points with direct lines of sight. Structures can also be oriented in a manner that can reduce the amount of damage from a bomb detonation in the area. This is covered in more detail in **Chapter 5**.

3.5.3. **Provide Effective Road Layout**. Although roads are often designed to minimize travel time from one place to another, caution must be taken when planning roads that provide straight line access to key facilities and other critical assets. These types of access roads provide the ability for a vehicle to gain the speed necessary to breach protective barriers or crash through facilities. Roads should be designed to limit the maximum speed a vehicle can attain before the driver loses control or draws attention. This can be accomplished by designing sharp curves in the roads or using barriers to create a serpentine layout that forces the driver to negotiate a series of sharp turns. Any vehicle driver attempting to leave the road in order to gain speed towards a potential target risks the chance of early detection and response. Roads that approach key facilities should be parallel to the facilities, versus a perpendicular approach. Barriers, trees, and other methods can be used to reduce the ability of drivers to leave the road or have a direct line of sight to the facility from the road.

3.6. Unified Facilities Criteria. This section focuses on UFCs which prescribe antiterrorism standards for new, existing, temporary, and expeditionary structures. The Undersecretary of Defense established guidance for developing and maintaining unified facilities criteria for planning, design, construction, sustainment, restoration, and modernization of DOD facilities in MIL-STD-3007, *Department of Defense Standard Practice for Unified Facilities Criteria (UFC) and Unified Facilities Guide Specifications (UFGS)*. UFC and UFGS development is primarily a joint effort of the US Army Corps of Engineers (USACE), the Navy Facilities Engineering Command (NAVFAC), and the Air Force Civil Engineer Support Agency (AFCESA). UFC and UFGS are used by the military departments, the defense agencies and the DOD field activities for planning, design, construction, sustainment, restoration and modernization of facilities, regardless of funding source. These publications can be located at the Whole Building Design Guide (WBDG) website at http://dod.wbdg.org. These publications can also be downloaded from the USACE Protective Design Center (PDC) website at https://pdc.usace.army.mil. This site also hosts open forums where users can post questions and collaborate on the latest protective designs and antiterrorism guidance.

3.6.1. **Standards**. Minimum DOD AT standards for new and existing inhabited facilities and expeditionary and temporary structures are outlined in UFC 4-010-01. The standards established by this guidance are intended to minimize the possibility of mass casualties in facilities where no known terrorist activity currently exists. Since it would be cost-prohibitive to design facilities that address every conceivable threat, the standards are designed to provide an appropriate level of protection for all personnel at a reasonable cost. Each DOD component may set more stringent AT building standards to meet the specific threats in its area of responsibility. CENTAF, AFSOUTH, USAFE, and PACAF have supplemental instructions regarding FP construction standards. Contact the theater-level A7/CE planner for more information. Where more stringent local standards apply, detailed descriptions of the levels of protection are provided in UFC 4-020-01.

3.6.2. **Levels of Protection**. Levels of protection relate to the degree to which assets (i.e., personnel, facilities, equipment, etc.) are protected based on known and specified threats such as vehicle-borne improvised explosive devices (VBIEDs), rockets, artillery and mortars. The primary strategy to achieve an appropriate level of protection is to maximize available standoff to keep potential or known threats as far away from personnel, inhabited facilities, equipment, and other critical assets as possible. However, if space is inadequate to achieve appropriate standoff distances, hardening and blast mitigation techniques must be applied to achieve an acceptable level of protection based on the asset's criticality and the threat. Primary gathering facilities (i.e., dining facilities, billeting, recreation facilities, etc.) should be hardened, if practicable, or provided some type of blast and fragmentation protection, including overhead cover and compartmentalization. Unless adequate planning is done to obtain the needed space to achieve appropriate standoff in high-threat environments where expeditionary assets are employed, personnel can be highly vulnerable to an attack. This potential vulnerability drives the need for larger sites. In addition, hardened structures, such as bunkers and foxholes with overhead cover, should be provided in the immediate proximity of all areas where personnel live and work. Selecting levels of protection for all key and critical assets involves a tradeoff for acceptable levels of risk. There are different standards for new and existing buildings and expeditionary or temporary structures. **Tables 3.1** and **Table 3.2**, excerpted from UFC 4-010-01, contains *qualitative* descriptions of potential damage to buildings and structures at different levels of protection that may be applied. **Table 3.1** applies to new and existing buildings and **Table 3.2** applies to expeditionary and temporary structures. Detailed *quantitative* descriptions of the levels of protection can be found in UFC 4-020-02 (FOUO), *Security Engineering Facilities Design Manual*.

Table 3.1. Levels of Protection – New and Existing Buildings.

Level of Protection	Potential Building Damage/Performance [2]	Potential Door and Glazing Hazards[3]	Potential Injuries
Below AT Standards [1]	Severe damage. Progressive collapse likely. Space in and around damaged area will be unusable.	Doors windows will fail catastrophically and result in lethal hazards (high hazard rating).	Majority of personnel in collapse region suffer fatalities. Potential fatalities in areas outside of collapsed area likely.
Very Low	Heavy damage - Onset of structural collapse, but progressive collapse is unlikely. Space in and around damaged area will be unusable.	Glazing will fracture, come out of the frame, likely to be propelled into the building, with potential to cause serious injuries (low hazard rating). Doors may be propelled into rooms, posing serious hazards.	Majority of personnel in damaged area suffer serious injuries with a potential for fatalities. Personnel in areas outside damaged area will experience minor to moderate injuries.
Low	Moderate damage – Building damage will not be economically repairable. Progressive collapse will not occur. Space in and around damaged area will be unusable.	Glazing will fracture, potentially come out of the frame, but at a reduced velocity; does not present a significant injury hazard (very low hazard rating). Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel in damaged area suffer minor to moderate injuries with the potential for a few serious injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience minor to moderate injuries.
Medium	Minor damage – Building damage will be economically repairable. Space in and around damaged area can be used and will be fully functional after cleanup and repairs.	Glazing will fracture, remain in the frame and result in a minimal hazard consisting of glass dust and slivers (minimal hazard rating). Doors will stay in frames, but will not be reusable.	Personnel in damaged area potentially suffer minor to moderate injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience superficial injuries.
High	Minimal damage. No permanent deformations. The facility will be immediately operable.	Glazing will not break (no hazard rating). Doors will be reusable.	Only superficial injuries are likely.

Notes:
1. This is not a level of protection and should never be a design goal. It only defines a realm of more severe structural response and may provide useful information in some cases.
2. For damage/performance descriptions for primary, secondary, and non-structural members, refer to UFC 4-020-02.
3. Glazing hazard levels are from ASTM F 1642.

Table 3.2. Levels of Protection – Expeditionary and Temporary Structures.

Level of Protection	Potential Structural Damage	Potential Injury
Below AT Standards (Note)	Severe damage. Frame collapse/massive destruction. Little left standing	Majority of personnel in collapse region suffer fatalities. Potential fatalities in areas outside of collapsed area likely.
Very Low	Heavy damage. Major portions of the structure will collapse (over 50%). A significant percentage of secondary structural members will collapse (over 50%).	Majority of personnel in damaged area suffer serious injuries with a potential for fatalities. Personnel in areas outside damaged area will experience minor to moderate injuries.
Low	Moderate damage. Damage will be unrepairable. Some sections of the structure may collapse or lose structural capacity (10% to 20% of structure)	Majority of personnel in damaged area suffer minor to moderate injuries with the potential for a few serious injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience minor to moderate injuries.
Medium	Minor damage. Damage will be repairable. Minor to major deformations of non-structural members and non-structural elements. Some secondary debris will be likely, but the structure remains intact with collapse unlikely.	Personnel in damaged area potentially suffer minor to moderate injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience superficial injuries.
High	Minimal damage. No permanent deformation of primary and secondary structural members or non-structural elements.	Only superficial injuries are likely.
Note: This is not a level of protection and should never be a design goal. It only defines a realm of more severe structural response and may provide useful information in some cases.		

3.6.3. **Standoff Distances**. The primary objective of design and site layout strategy is to keep potential threats as far away from personnel and critical assets as possible. Maximizing available standoff distance is the most cost-effective solution for mitigating the effects of blasts and provides the capability to increase distances to counter increased threats or achieve higher levels of protection. Due to different types of construction, standoff distances vary for new or existing buildings and expeditionary or temporary structures.

3.6.3.1. **New and Existing Buildings**. The standoff distances shown in **Table 3.3** and illustrated in **Figure 3.2** through **Figure 3.5** were extracted from UFC 4-010-01. The applicable explosive weights (kg/pounds of TNT) indicated in the table must be obtained from UFC 4-010-02 (FOUO). The standards were developed for a wide range of conventionally constructed buildings. As prescribed by UFC 4-010-01, the distances listed under the "Minimum Standoff Distance" column of **Table 3.3** must be provided except where doing so is not possible. For new buildings, standoff distances of less than those indicated are not allowed. For existing buildings, the UFC states that lesser standoff distances may be allowed where the required level of protection can be achieved through analysis of blast effects, building hardening, or other mitigating construction or retrofit. This is done only when achieving minimum standoff distances may not be possible.

3.6.3.2. **Expeditionary and Temporary Structures**. The standoff distances shown in **Table 3.4** and illustrated in **Figure 3.6** apply to expeditionary and temporary structures. These standoff distances were developed for TEMPER Tents, Southeast Asia (SEA) Huts, General Purpose Shelters, and Small Shelter Systems. The applicable explosive weights (kg/pounds of TNT) indicated in the table must be obtained from UFC 4-010-02 (FOUO). An "*" in **Figure 3.6** indicates the standoff distance varies by type of construction and that an analysis of the structure by an engineer experienced in blast-resistant design is required. Hardening will be applied as necessary to mitigate the effects of explosives indicated. If the geographic combatant commander determines a higher level of protection is required based on a known threat and an analysis of vulnerability and criticality assessments, refer to UFC 4-020-01. This manual outlines methods for achieving higher levels of protection.

Table 3.3. Standoff Distances for New and Existing Buildings.

Location	Building Category	Standoff Distance Requirements			
		Applicable Level of Protection	Conventional Construction Standoff Distance	Minimum Standoff Distance[1]	Applicable Explosive Weight [2]
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Billeting and High Occupancy Family Housing	Low	45 m [3] (148 ft.)	25 m [3] (82 ft.)	I
	Primary Gathering Building	Low	45 m [3] [4] (148 ft.)	25 m [3] [4] (82 ft.)	I
	Inhabited Building	Very Low	25 m [3] (82 ft.)	10 m [3] (33 ft.)	I
Parking and Roadways within a Controlled Perimeter	Billeting and High Occupancy Family Housing	Low	25 m [3] (82 ft.)	10 m [3] (33 ft.)	II
	Primary Gathering Building	Low	25 m [3] [4] (82 ft.)	10 m [3] [4] (33 ft.)	II
	Inhabited Building	Very Low	10 m [3] (33 ft.)	10 m [3] (33 ft.)	II
Trash Containers	Billeting and High Occupancy Family Housing	Low	25 m (82 ft.)	10 m (33 ft.)	II
	Primary Gathering Building	Low	25 m (82 ft.)	10 m (33 ft.)	II
	Inhabited Building	Very Low	10 m (33 ft.)	10 m (33 ft.)	II

Notes

1. Even with analysis, standoff distances less than those in this column are not allowed for new buildings, but are allowed for existing buildings if constructed/retrofitted to provide the required level of protection at the reduced standoff distance.
2. See UFC 4-010-02 for the specific explosive weights (kg/pounds of TNT) associated with designations I, II, III. UFC 4-010-02 is FOUO.
3. For existing buildings, see UFC 4-010-01 for additional options.
4. For existing family housing, see UFC 4-010-01 for additional options.
5. Refer to UFC 4-010-01 for definitions necessary for application of this table.

Figure 3.2. Standoff Distances – Controlled Perimeter.

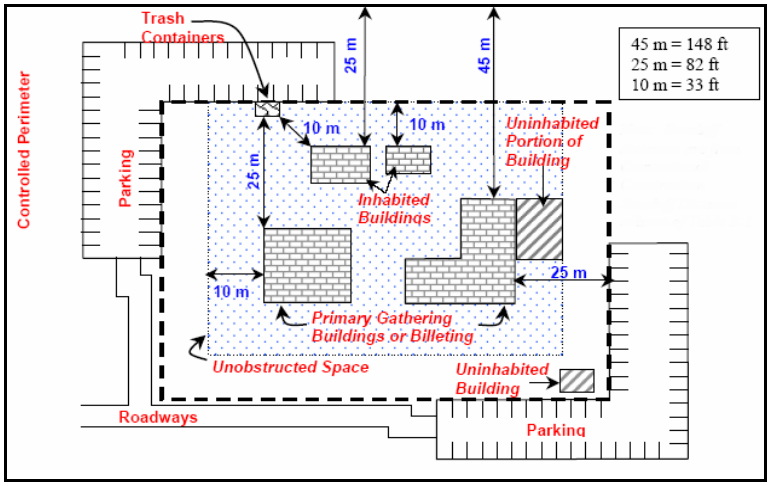


Figure 3.3. Standoff Distances – No Controlled Perimeter.

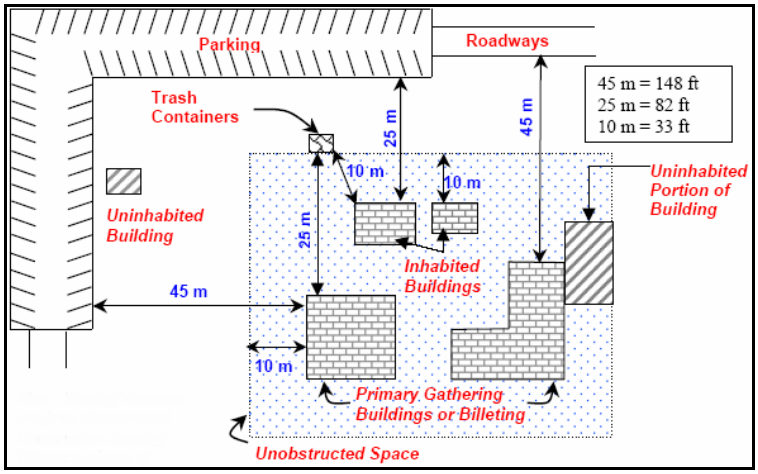


Figure 3.4. Parking and Roadway Control for Existing Buildings – Controlled Perimeter.

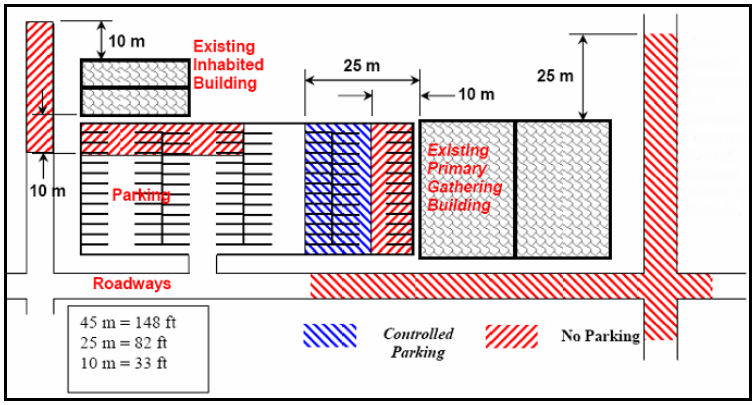


Figure 3.5. Parking and Roadway Control for Existing Buildings – No Controlled Perimeter.

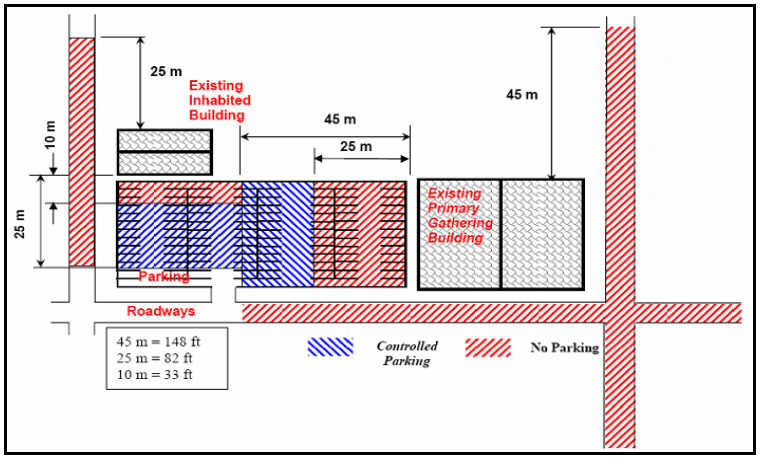


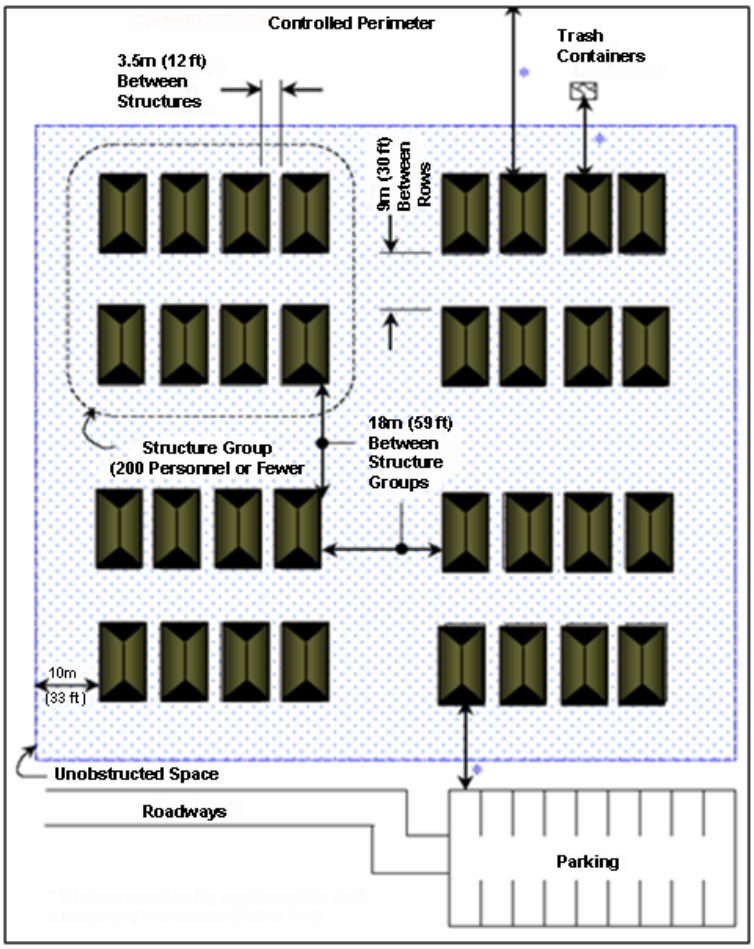
Table 3.4. Standoff Distances and Separation for Expeditionary and Temporary Structures.

Location	Structure Category	Standoff Distance or Separation Requirements			
		Applicable Level of Protection	Fabric Covered Structures[1]	Other Expeditionary and Temporary Structures[1][2]	Applicable Explosive Weight (TNT) [3]
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Billeting	Low	31 m (102 ft.)	71 m (233 ft.)	I
	Primary Gathering Structure	Low	31 m (102 ft.)	71 m (233 ft.)	I
	Inhabited Structure	Very Low	24 m (79 ft.)	47 m (154 ft.)	I
Parking and Roadways within a Controlled Perimeter	Billeting	Low	14 m (46 ft.)	32 m (105 ft.)	II
	Primary Gathering Structure	Low	14 m (46 ft.)	32 m (105 ft.)	II
	Inhabited Structure	Very Low	10 m (33 ft.)	23 m (75 ft.)	II
Trash Containers	Billeting	Low	14 m (46 ft.)	32 m (105 ft.)	II
	Primary Gathering Structure	Low	14 m (46 ft.)	32 m (105 ft.)	II
	Inhabited Structure	Very Low	10 m (33 ft.)	23 m (75 ft.)	II
Structure Separation[4]	Separation between Structure Groups	Low	18 m (59 ft.)	18 m (59 ft.)	III[5]
	Separation between Structure Rows	Low	9 m (30 ft.)	9 m (30 ft.)	III [5]
	Separation between Structures in a Row	Very Low	3.5 m (12 ft.)	3.5 m (12 ft.)	III[6]

Notes

1. See Appendix A of UFC 4-010-01 for a description of these structure types.
2. For container structures, Appendix B in UFC 4-010-01 applies.
3. See UFC 4-010-02 for the specific explosive weights (kg/pounds of TNT) associated with designations I, II, III. UFC 4-010-02 is FOUO.
4. Applies to Billeting and Primary Gathering Structures only. No minimum separation distances for other inhabited structures.
5. Explosive for building separation is an indirect fire (mortar) round at a standoff of half the separation distance.

Figure 3.6. Standoff Distances and Separation for Expeditionary and Temporary Structures.



Chapter 4

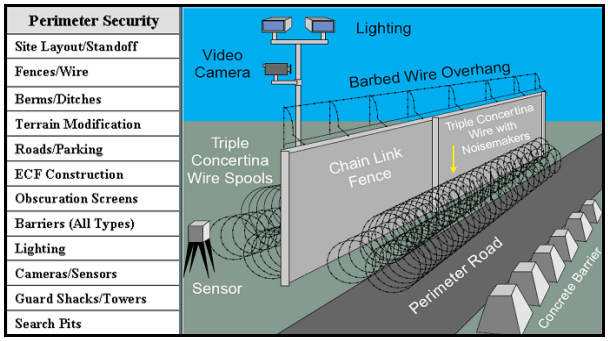
PHYSICAL SECURITY

4.1. Overview. A key element of FP is physical security. DOD 5200.8-R defines physical security as measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard these assets from espionage, sabotage, damage, and theft. This chapter provides guidance and considerations for implementing protective measures designed to eliminate threats or mitigate the effects of an attack against personnel and critical resources. In the absence of a specific threat, the minimum DOD FP standards in UFC 4-010-01 are applied.

4.2. Aspects of Physical Security. Physical security is built on the foundation that baseline security and preparedness postures are established based on the local threat, site-specific vulnerabilities, identification of critical assets, and employment of available resources. Physical security focuses on physical measures and procedures designed to safeguard assets from likely aggressors. As discussed earlier, plans for implementing these physical security measures begin far in advance of the deployment (including site selection and site layout planning) and continue throughout all phases of the deployment, including initial beddown, sustainment, and redeployment. Key physical security tasks civil engineers will perform include the implementation of protective measures designed to stop potential aggressors and mitigate the impact of an attack on personnel and other critical resources. This requires, among many other things, that security personnel be capable of detecting and identifying an aggressor as far in advance of an attack as possible. Civil engineers team with security forces to design and implement physical measures that will provide this early detection capability. The two broad areas of physical security that civil engineers might dedicate the majority of time and resources in expeditionary environments include perimeter security and internal security. This chapter focuses on these two aspects of physical security.

4.3. Perimeter Security. One of the most important FP tasks civil engineers are involved with during the initial stages of deployment and beddown is establishing perimeter security. Working with security forces, civil engineers must help establish a continuous physical barrier which clearly defines the physical limits of the site to prevent unauthorized access. **Figure 4.1** illustrates some aspects of perimeter security that should be addressed. This usually involves constructing fences, concertina wire, installing perimeter lighting, constructing berms and ditches, placing barriers, and assisting with the installation of security cameras. Also key is ensuring both a primary and backup source of power is available in the event systems requiring power are disrupted by intentional or unintentional damage. Clear zones, which are those areas beyond the perimeter, must be kept free of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to penetrate perimeter security. In addition, secure any structures originating from outside the perimeter, such as utility ducts, drainage culverts, concrete trenches, and storm drains. This can be done using screens and grates. Locks should be installed on manhole covers. Intrusion detection sensors can be used along with surveillance equipment to provide greater security. The next few paragraphs address how barriers, perimeter fences, entry control facilities, berms and ditches, lights and sensors, obscuration screens, and observation posts can be employed in the expeditionary environment.

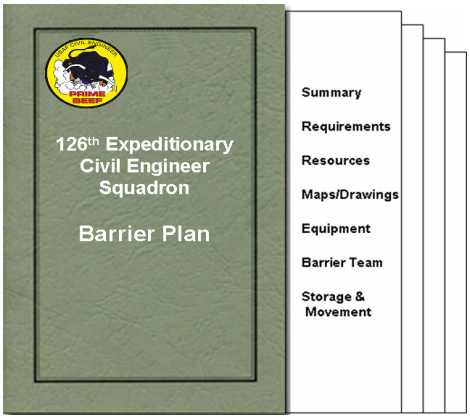
Figure 4.1. Perimeter Security Measures.



4.3.1. **Barriers**. One of the most important aspects of establishing effective physical security is the ability to employ barriers. Barriers are used to maintain standoff distances, establish boundaries, limit and control pedestrian and vehicular flow and access, channel movement in certain directions and to certain points, obstruct line-of-sight views from outside the perimeter, protect key facilities and mission-critical assets, and compartmentalize areas within primary gathering buildings. Civil engineers are largely responsible for employing barriers as part of the physical security element of FP.

4.3.1.1. **Barrier Plan**. Developing and implementing a barrier plan is a critical FP function for civil engineers. The barrier plan (**Figure 4.2**) outlines exactly how barriers will be employed continuously or during periods of heightened alert. A prioritized list of key facilities and critical assets to be protected forms the basis for the plan. This list should have already been developed during the threat, vulnerability, criticality, and risk assessments. The barrier plan should summarize the number and types of barriers employed as well as additional requirements, employment locations, if and where barriers will be prepositioned, their intended purpose (i.e., traffic control, perimeter security, etc.), and resources and equipment needed to move or relocate and install the barriers when needed (i.e., anchors, cables, forklift, trailer, etc.). Civil engineers work closely with security forces to identify resources needed to adequately protect key facilities and assets. Some installations may preposition key assets and employ them upon heightened alert or during periods of increased threat. In the expeditionary environment, limited resources may not allow for maintaining barriers in storage or prepositioned status for heightened alert. Barriers may need to be continuously employed to provide protection in high-threat environments. This determination is made on site. A dedicated barrier team should be appointed, trained, and exercised regularly.

Figure 4.2. Typical Barrier Plan.



4.3.1.2. **Types of Barriers**. There are many barrier designs that can be used for a variety of purposes (i.e., pedestrians, vehicles, weapons, etc.) and various types of structures and natural features that can be used as barriers (i.e., trees, mountains, water, wood, concrete, etc.). Barriers are categorized as either active (containing moving parts) or passive (non-moving parts). It is important not to confuse the different types of barriers available with the purpose for which the barrier is being used or will be used. For example, some barriers may be used to mitigate the effects of blast and/or fragmentation in the event of an attack and may sometimes be referred to as blast or fragmentation barriers. These are passive-type barriers. A variety of passive barriers can be found in the expeditionary environment (i.e., bitburg barrier, jersey barrier, Alaska barrier, T-barrier, HESCO barrier, etc.). Some active barriers commonly found in the expeditionary environment include bollards and arm barrier gates. Barriers can be further characterized as moveable (may require heavy equipment), fixed (permanently installed), or portable. Portable barriers are normally used temporarily until either a moveable or fixed barrier system can be employed. The following paragraphs further explain the types of barriers and the purposes for which they are commonly used.

4.3.1.2.1. **Active Barriers**. Active barriers are either electronically controlled or manually operated to allow or restrict access to sites or certain areas within a site. Examples include barricades, retractable bollards, beams, and gates. Active barriers are normally employed at entry and exit points to the site or at the entrance to a critical facility with a controlled perimeter. From a safety standpoint, active vehicle barriers are capable of causing serious injury or death, even when used for their intended purpose. This can be caused by equipment malfunction, inadvertent activation, or operator error. If using these types of barriers, make sure there are signs in place to alert vehicles to their presence (i.e., warning signs, lights, bright colors, etc.). In addition, these types of barriers should include backup power, emergency cutoff switches, and adequate lighting. **Figure 4.3** through **Figure 4.7** are examples of active barriers that can be used in the expeditionary environment.

Figure 4.3. Portable Barrier.

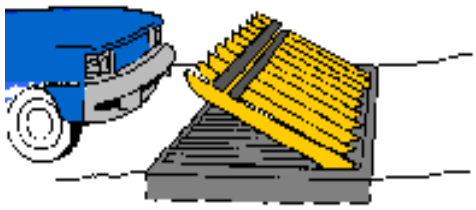


Figure 4.4. Drum Barrier.

Figure 4.5. Retractable Bollards.

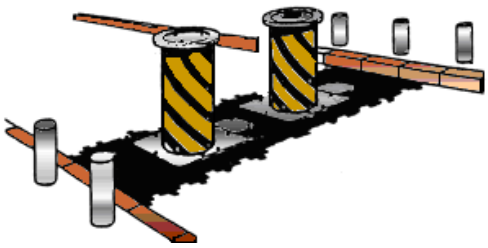


Figure 4.6. Lift Plate Barricade System.

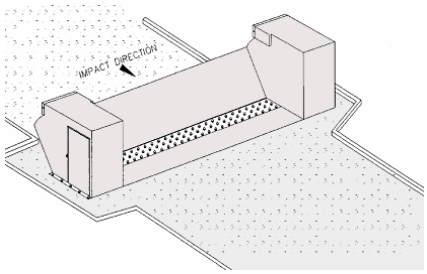
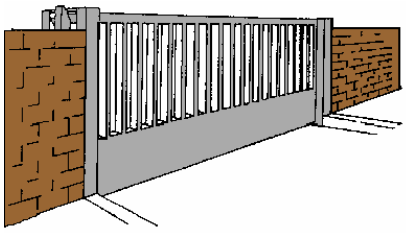


Figure 4.7. Sliding Gate.



4.3.1.2.2. **Passive Barriers**. Passive barriers have no moving parts and are designed to absorb energy upon impact and transfer that energy into the foundation. Examples include portable or permanent concrete structures, concrete bollards, posts, guardrails, ditches, and reinforced fences. Passive barriers along the perimeter or interior fence line should be designed to allow little or no penetration, especially if the available standoff distance is limited. Passive barriers are commonly found in the expeditionary environment, particularly if the contingency operation is of a limited duration. **Figure 4.9** through **Figure 4.14** are examples of passive barriers that can be used in the expeditionary environment. For additional details on different types of barriers, refer to UFC 4-022-02, *Selection and Application of Vehicle Barriers*, AFH 10-222, Volume 14, *Guide to Fighting Positions, Obstacles, and Revetments;* and the *Joint Forward Operations Base Force Protection Handbook*. This handbook can be located on the Joint Staff Antiterrorism Portal (ATEP) website at https://atep.dtic.mil (Non-classified Internet Protocol Router Network (NIPRNET)) or https://www.atep.smil.mil (Secret Internet Protocol Router Network; (SIPRNET)). You will need to submit an application to get authorization to access these secure sites.

Figure 4.9. Non-Retractable Bollards.

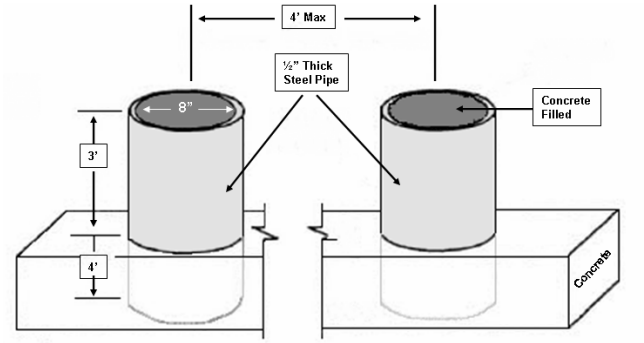


Figure 4.10. Steel Hedgehog Barrier.

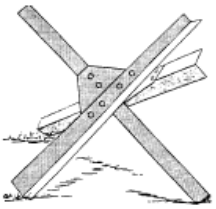


Figure 4.11. Expedient Barrier – Equipment Tires.

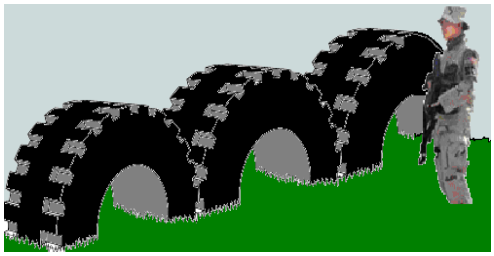


Figure 4.12. Concrete Jersey Barrier.

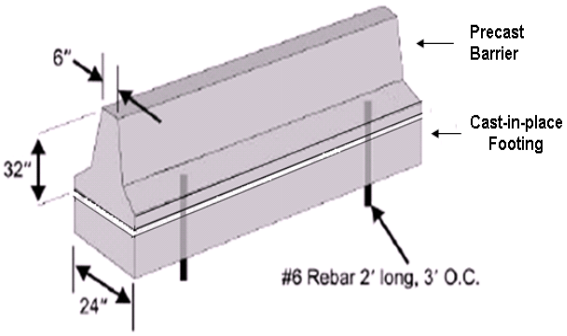


Figure 4.13. Sand Bags.

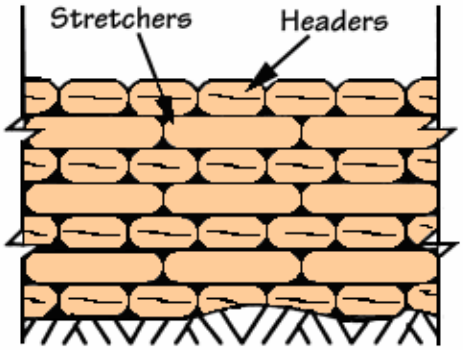
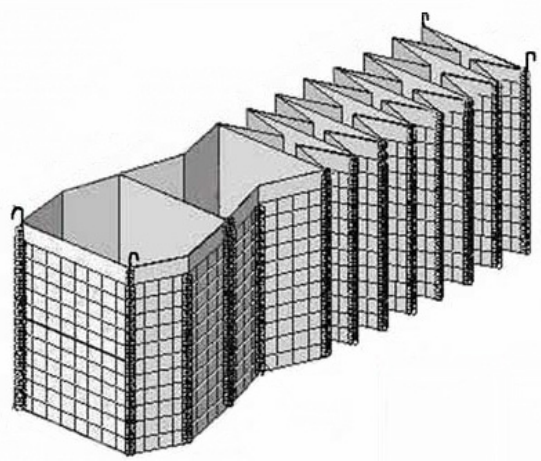


Figure 4.14. HESCO Barriers.

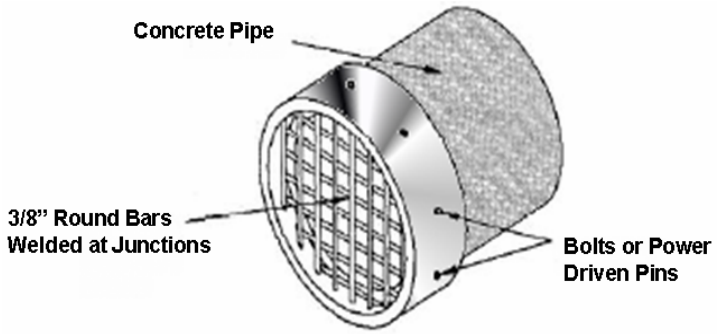


4.3.2. **Perimeter Fences**. Fences are used to define the boundary of a site or structure, direct and control the flow of traffic and establish clear zones. They are also used in conjunction with security lighting, intrusion detection systems, closed circuit television, and other means of integrating security. Chain link fences are antipersonnel barriers. They are cost-effective, usually readily available, and provide a moderate degree of protection. Chain link fences are more effective if reinforced with cable or topped with outriggers and razor wire or multiple strands of barbed wire (**Figure 4.15**). Since most fences can be easily penetrated by a moving vehicle, they are not considered vehicle barriers and will resist impact only if reinforced by barriers capable of absorbing the impact of moving vehicles. For additional details on security fencing, reference MIL-HDBK-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities* (will be replaced by UFC 4-022-03).

Figure 4.15. Perimeter Fences and Barriers.

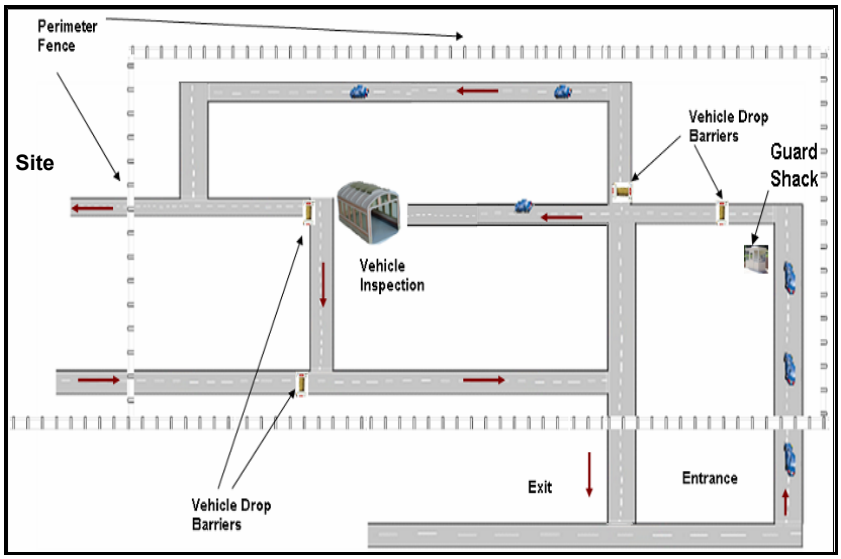
4.3.3. **Utility Openings**. Large utility openings, such as drainage pipes, culverts, vents, and ducts can provide an intruder with a means of entry or exit across a site's perimeter without triggering an alarm. These types of openings can also be used to conceal weapons or plant explosives. For these reasons, the number of culverts and other drainage pipes crossing a site's perimeter should be minimized. In addition, FP guidance states that these types of openings, having a cross-sectional area greater than 96 square inches and whose smallest dimension is greater than 6 inches, will be protected by securely fastened, welded bar grilles (**Figure 4.16**). As an alternative, these structures can be composed of multiple pipes with diameters of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. If grilles or pipes are installed in culverts or other drainage structures, ensure action is taken to compensate for the diminished flow capacity and increased maintenance that will be required. In addition, secure all manhole covers that could be accessed and used to cross the site's perimeter. For detailed information on securing these types of structures, refer to UFC 4-020-03FA*, Security Engineering: Final Design*. This document is FOUO and can be downloaded from the USACE's PDC website at https://pdc.usace.army.mil.

Figure 4.16. Grille Installed on Drainage Culvert.



4.3.4. **Entry Control Facility (ECF)**. The ECF is a physical boundary controlling vehicle access at the perimeter of the site. Some guidance may also refer to these boundaries as access control points (ACPs). The ECF is a security checkpoint at or outside the secured perimeter of an installation that allows for sufficient standoff from the perimeter to protected facilities and critical assets. Security personnel use the ECF to control vehicle access to the site using various methods such as guard shacks, vehicle barriers, and inspection points (**Figure 4.17**). Civil engineers team with security forces in determining the location and layout for ECFs and other structures needed to control vehicle access to the site. These determinations should be based on an intelligence assessment of the threat.

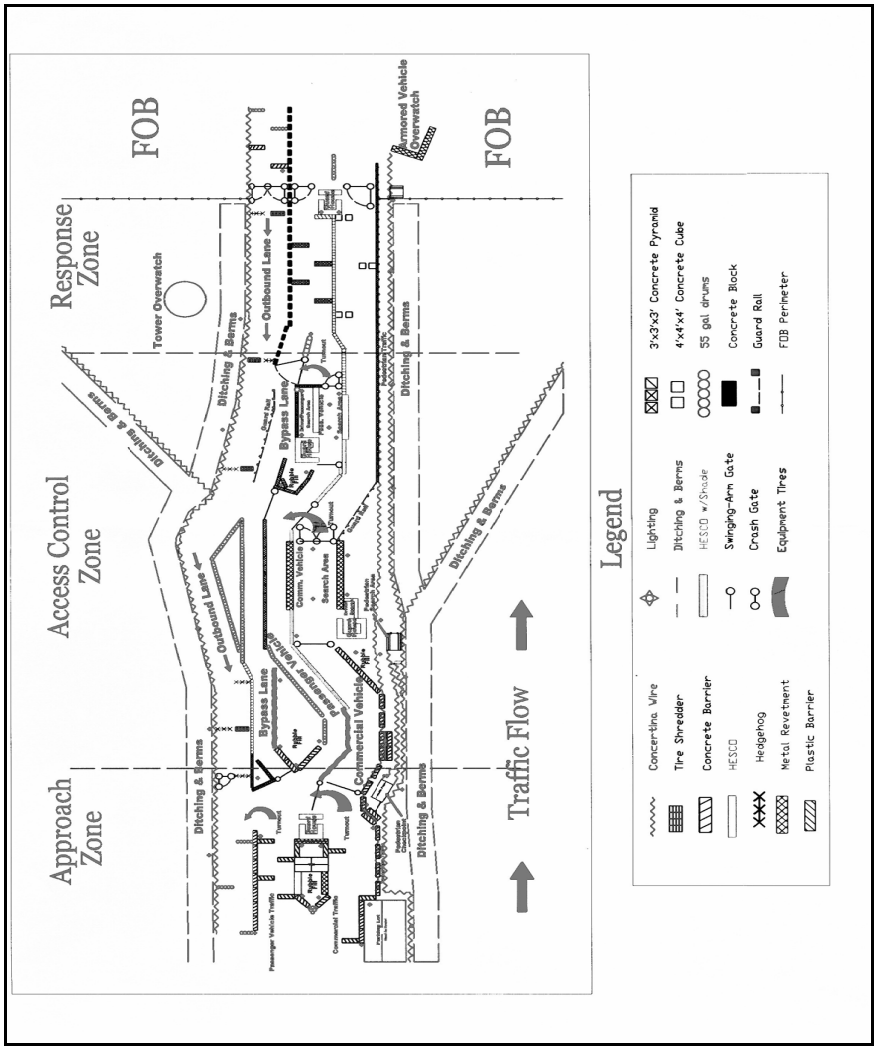
Figure 4.17. Typical Entry Control Facility.



4.3.4.1. **Location**. ECFs should be located to provide maximum standoff distance between the ECF and critical facilities and equipment. Minimum standoff distances are outlined in UFCs 4-010-01 and 4-010-02. The geographic combatant commander can increase these distances based on the known threat for a particular area. Always refer to the specific operational order to determine if prescribed standoff distances are more stringent than those outlined in UFCs.

4.3.4.2. **Layout**. The main ECF should be subdivided into zones and allow enough queue space to prevent vehicles waiting to enter the site from obstructing traffic on main roads (**Figure 4.18**). ECF zones consist of an approach zone, access zone, response zone, and safety zone. The approach zone is located at the interface between public roads and the site. Access zones comprise the main portion of the ECF. This is where guard facilities and vehicle inspection areas are located. Response zones extend beyond access zones to the final barrier or entry point. This is usually where security forces will set up an overwatch tower as a final denial point for vehicles attempting to gain unauthorized entry. Overwatch towers are hardened firing positions that provide coverage for vehicle entry, exit, and search areas. The safety zones include all techniques (fences, barriers, etc.) used to maintain an acceptable standoff distance between the ECF and critical assets. Vehicles approaching the site should be channeled through a maze of barriers that force drivers to decrease their rate of speed. Vehicles should be channeled into search pits to allow security personnel to search for and detect explosives. Search pits should be separated from local traffic by security fences and vehicles barriers and located outside of the minimum prescribed standoff distance. Civil engineers work closely with security and intelligence personnel in designing and siting vehicle search pits. Separate points of access to the site must be established for commercial trucks and delivery vehicles, outside the standoff distance, where they can be searched prior to gaining access. Detailed guidance for constructing ECFs can be found in UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*.

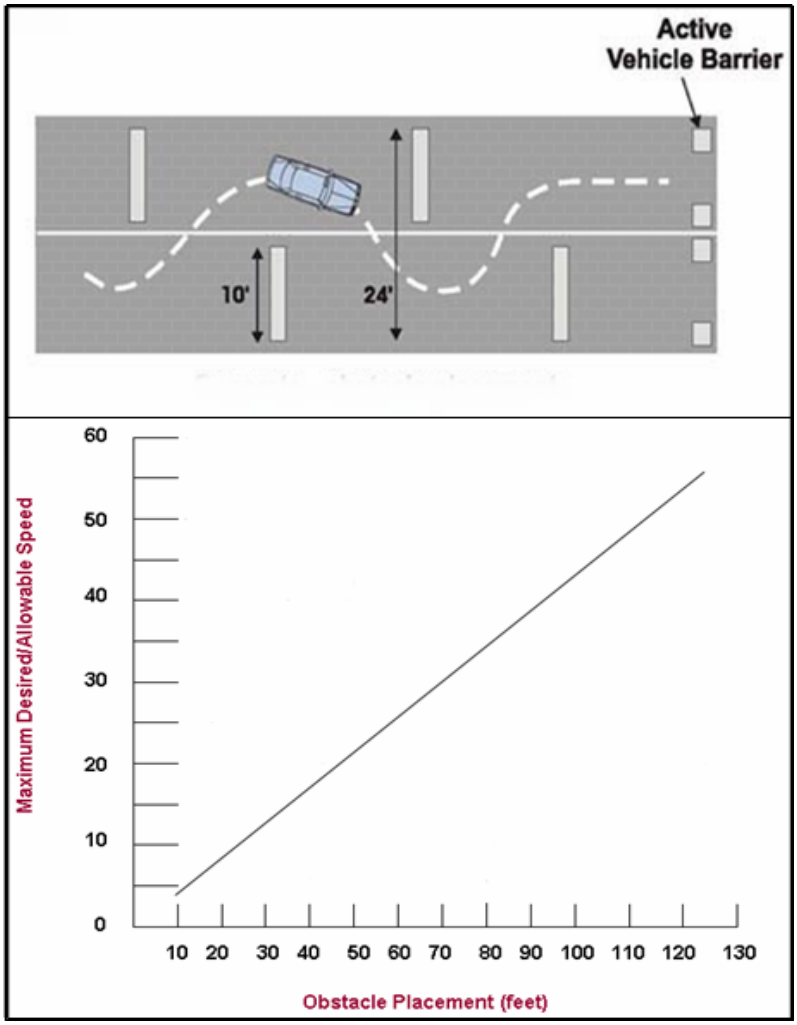
Figure 4.18. Entry Control Facility Zones.



4.3.4.3. **ECF Barriers**. ECF barriers are used to maintain control. They address the countermobility aspect of FP (preventing unauthorized vehicles from entering the site) and are set up to channel vehicles and pedestrians into or away from certain areas. The ECF is the point at which vehicles are either cleared or rejected from accessing the site and must be a strictly controlled area. ECF barriers define the boundaries and provide security personnel with a visual assessment of a driver's intent as a vehicle passes through certain zones and reacts to barriers employed to control path, speed, and direction. Barriers should be placed along main roads leading to the site from public roads to establish an approach zone and throughout the rest of the ECF to maintain control during the clearing process. Barriers should be anchored to the surface and/or cabled together to provide increased resistance to penetration attempts (**Figure 4.19**). To slow speeds of approaching vehicles, place barriers in a manner that produces a serpentine path drivers must negotiate to reach the entry point. Desired speeds can be controlled by placing barriers at certain distances apart. For example, to allow a maximum speed of 15 mph, place barriers 30 feet apart in an alternating pattern as depicted in **Figure 4.20**. Creating 90-degree turns also forces drivers to reduce speeds. A vehicle leaving these paths will draw attention and alert security personnel of a possible attempt to evade clearance procedures and gain unauthorized access to the site.

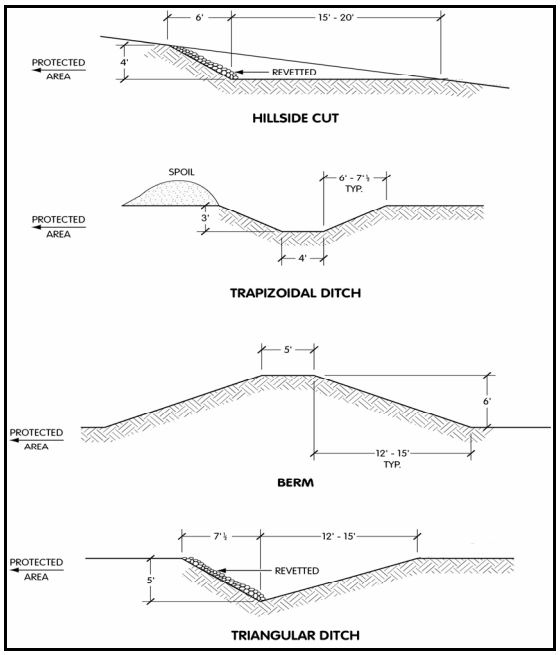
Figure 4.19. Jersey Barriers Cabled Together.

Figure 4.20. Barriers Used to Form Serpentine Path.



4.3.5. **Berms and Ditches**. Berms and ditches can be constructed around the site perimeter to slow or prevent vehicles from penetrating the restricted boundary (**Figure 4.21**). Triangular ditches and hillside cuts are relatively easy to construct and are very effective against a wide range of vehicles. Side hill cuts are variations of the triangular ditch adapted to side hill locations and have the same advantages and limitations. A trapezoidal ditch requires more construction time but is more effective in stopping a vehicle. With this type of construction, a vehicle will be trapped when the front end falls into the ditch and the undercarriage is hung up on the leading edge of the ditch. For additional information on constructing berms and ditches, reference AFH 10-222, Volume 14.

Figure 4.21. Berms and Ditches – Perimeter Security.



4.3.6. **Lighting and Sensors**. Security lighting allows personnel to observe areas around the perimeter, at entry control points, and throughout the site during hours of darkness without exposing themselves. It is best to use lighting that produces a glare upon individuals approaching a perimeter but does not illuminate and expose security personnel, guard houses, or observation posts. Avoid glare lighting if it will cause traffic hazards. Different types of terrain and surfaces required to be illuminated should be analyzed to determine the brightness of security lighting needed to ensure personnel can observe all areas in and around the site and as far outside the perimeter as possible. The site commander may require some areas to be void of lighting during certain times or at all times so as not to illuminate a potential target. To be more effective, security lighting can be combined with an IDS as shown in **Figure 4.22**. Numerous types of IDSs are currently being used in the expeditionary environment (microwave, passive infrared, active infrared, seismic, magnetic, motion detectors, closed circuit television, etc.). Certain factors determine the type of system to install, including site location, terrain, weather, manpower available for monitoring, etc. Regardless of the type of lighting or IDS used, provide emergency backup power. For more information on security lighting and IDSs, refer to the Illuminating Engineering Society of North America (IESNA) HB-9, *Lighting Handbook:* IESNA G-1-03, *Guide for Security Lighting for People, Property, and Public Spaces:* and UFC 4-020-04, *Electronic Security Systems*: *Security Engineering*.

Figure 4.22. Security Lighting and Intrusion Detection System.

4.3.7. **Obscuration Screens**. Perimeter obscuration screens are used to block direct lines of sight to sensitive areas or facilities from outside the perimeter of a site in an effort to reduce targeting opportunities from direct fire weapons. This can be done in various ways using trees, dense vegetation, chain link fences with slats, wooden fences, camouflage netting, earth berms, etc. Obscuration screens do not provide protection against direct fire weapons. Another type of screen, referred to as a predetonation screen, can be used for protection against these types of weapons. Predetonation screens are covered later in this chapter. Install facility obscuration screens on the side of facilities facing the perimeter of the site to reduce exposure. Obscuration screens can also be placed on perimeter fences to block lines of sight into the camp area **(Figure 4.23)**. When using obscuration screens, make sure personnel inside the site or facility are still able to see outside and observe any suspicious activities.

Figure 4.23. Obscuration Screen on Perimeter Fence.

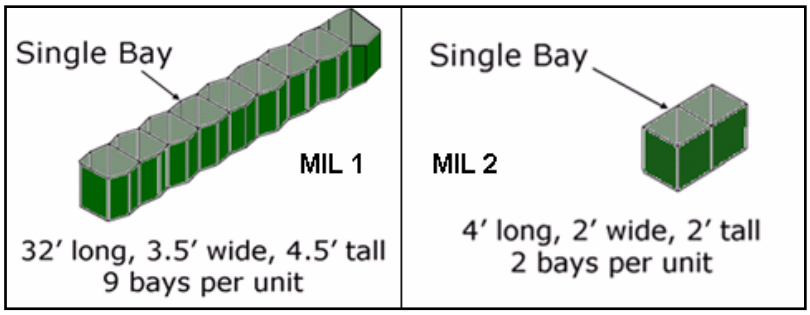
4.3.8. **Observation Posts, Guard Towers, and Defensive Fighting Positions**. Civil engineers must work closely with security forces personnel in siting and constructing hardened structures to be used for observation, overwatch, and defensive fighting (**Figure 4.24**). Some of the construction planning factors to be considered include: location, terrain, height, maximum number of personnel each structure is required to support, level of hardening, number of gun ports, heating, ventilation, and air conditioning requirements, plumbing requirements, lighting, electronic surveillance and communications equipment requirements, etc. These structures should be placed at least 30 feet inside the perimeter of the site and provide a clear view of the inner and outer clear zones and perimeter fence line. HESCO barriers (earth-filled containers) are commonly used in the expeditionary environment to construct various types of structures and sidewall protection. These containers come in various sizes and all have national stock numbers assigned (see **Table 4.1** and **Figure 4.25**). For details on constructing guard towers, observation posts, defensive fighting positions, and bunkers, reference the *Joint Forward Operations Base Force Protection Handbook* referred to earlier and AFH 10-222, Volume 14. Detail drawings and construction details for these types of structures can also be downloaded from the Theater Construction Management System (TCMS) website at http://www.tcms.net.

Figure 4.24. Observation Posts, Guard Towers, and Defensive Fighting Positions.

Table 4.1. HESCO Container Sizes and National Stock Numbers.

Unit	Height ft (m)	Width ft (m)	Length ft (m)	NSN (5680-99-xxx-xxxx)
Mil 1	4.5 (1.37)	3.5 (1.06)	32 (10)	835-7866 (Beige), 001-9396 (Green)
Mil 2	2 (0.61)	2 (0.61)	4 (1.21)	968-1764 (Beige), 001-9397 (Green)
Mil 3	3.25 (1.0)	3.25 (3.25)	32 (10)	001-9392 (Beige), 001-9398 (Green)
Mil 4	3.25 (1.0)	5 (1.5)	32 (10)	001-9393 (Beige), 001-9399 (Green)
Mil 5	2 (0.61)	2 (0.61)	10 (3.05)	001-9394 (Beige), 001-9400 (Green)
Mil 7	7.25 (2.21)	7 (2.12)	90 (27.7)	169-0183 (Beige), 126-3716 (Green)
Mil 8	4.5 (1.37)	4 (1.22)	32 (10)	335-4902 (Beige), 517-3281 (Green)
Mil 9	3.25 (1.0)	2.5 (0.78)	30 (9.14)	563-5649 (Beige), 052-0506 (Green)
Mil 10	7 (2.12)	5 (1.5)	95 (30.5)	391-0852 (Beige), 770-0326 (Green)

Figure 4.25. Illustration of Different Sizes of HESCO Containers.



4.4. Internal Security. The focus on internal security, from a civil engineer perspective, generally involves such tasks as facility hardening, dispersal, compartmentalization, revetment construction, bunker construction, and protection of utilities, to name a few (**Figure 4.26**). Existing facilities used in the expeditionary environment may need to be hardened to provide an acceptable level of protection from rockets, artillery, and mortars. In addition, expeditionary structures, bunkers, observation posts, and fighting positions must be constructed to support IBD objectives, covered in **Chapter 5**. The following are some basic concepts and techniques that can be used to provide some protection for existing and expeditionary structures. For construction details and different options that can be employed, refer to the *Joint Forward Operations Base Force Protection Handbook*.

Figure 4.26. Internal Security Measures.

Internal Security
Facility Hardening
Bunker Construction
Defensive Fighting Positions
Predetonation Screens
Window Protection
Asset Dispersal
Camouflage and Concealment
Compartmentalization
Protection of Utilities
Mass Notification Systems
Barriers (All Types)
Sidewalls and Revetments

4.4.1. **Mass Notification Systems**. Mass notification systems provide immediate notification to personnel during emergencies (**Figure 4.27**). Information can be relayed regarding FPCONs, imminent threats, attacks in progress, etc., and personnel can be directed to take certain response actions (i.e., take cover, evacuate, etc.). Civil engineers, especially Fire Emergency Services and Emergency Management, must work closely with security and communications personnel to install and maintain a site mass notification system with primary and backup power in the event the primary source of power is disrupted. Details on mass notification systems can be found in UFC 4-021-01, *Design and O&M: Mass Notification Systems*. Although there are many different systems available, the Giant Voice system is typically used in expeditionary environments. However, this system is generally not suitable for notifying personnel working or residing in permanent structures since the voice messages are usually unintelligible. In these instances, civil engineers work with security and communications personnel to develop alternative ways of providing mass notification.

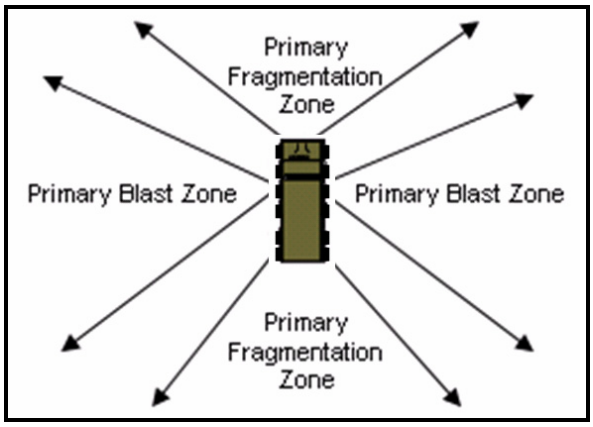
Figure 4.27. Mass Notification System.

4.4.2. **Facilities**. Achieving appropriate levels of protection for facilities most commonly used in the expeditionary environment, such as TEMPER tents and SEA Huts (**Figure 4.28**) can be very difficult. This is why standoff is particularly important in expeditionary environments. Personnel can be unusually vulnerable to certain threats during the initial stages of a deployment when the site is still somewhat austere, resources are limited, and access to permanently constructed facilities has not yet been negotiated. If US forces occupy existing permanent facilities offered by the host nation (HN), civil engineers may need to apply the standards outlined in UFC 4-010-01 for new and existing buildings (**Table 3.3**). Where more stringent local standards apply, or where local commanders dictate additional measures as a result of specific terrorist threats, these standards may be supplemented to achieve higher levels of protection. If increased levels of protection are warranted, detailed descriptions can be found in UFC 4-020-01. Also refer to AFH 10-2401, *Vehicle Bomb Mitigation Guide*, for recommendations on increasing protection against vehicle bombs. Both publications are FOUO and can be accessed under the USACE website at https://pdc.usace.army.mil. Follow the application instructions to obtain a userid and password. The following paragraphs present techniques that can be used in conjunction with standoff to mitigate the effects of blast/fragmentation on facilities in the expeditionary environment.

Figure 4.28. Expeditionary Structures.

4.4.2.1. **Orientation**. Buildings and structures can be oriented in a manner to help reduce the effects of blast on the structure. Tests have shown that structures laid out with the smaller dimension of the structure facing the direction of an anticipated blast (i.e., perimeter fence, ECP, etc.) receive less damage than they would if the larger dimension were facing the direction of an anticipated blast. Also, tests with vehicle bombs have shown that the primary blast field from the explosion tends to be outwards from both sides of the vehicle, while the primary fragmentation field tends to travel more to the front and rear of the vehicle (**Figure 4.29**). This information can be used to determine how best to orient facilities during site setup. If possible, doors and windows should be faced in a manner that does not provide a direct line of sight from outside the perimeter. If this is not possible, cover the windows and consider using obscuration screening to block visual access to the facility or structure. For more details on vehicle bombs and their effects on all types of structures, including expeditionary structures, refer to AFH 10-2401. This handbook also provides safe standoff distances to defeat and mitigate the effects of vehicle bombs.

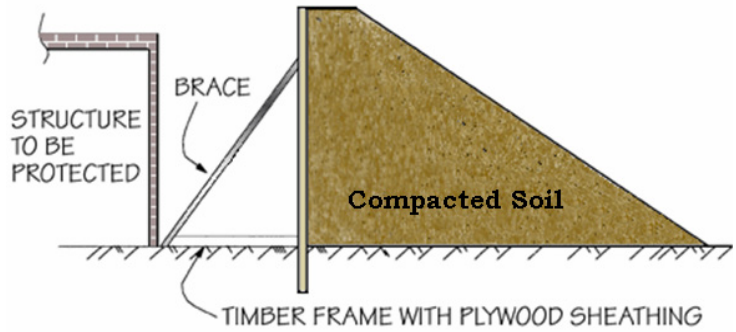
Figure 4.29. Blast and Fragmentation Hazard Zones.



4.4.2.2. **Clustering and Dispersal.** Making the determination to cluster or disperse assets can be based on several factors. Because each of these tactics has both positive and negative aspects, the planner will need to strike a careful balance between efficiency and survivability, with emphasis on survivability. Grouping high-risk activities and concentrating personnel and critical functions in a cluster can provide opportunities to maximize standoff distances, reduce the perimeter area, minimize access points, and create defensible space. Conversely, asset dispersal is often necessary due to the difficulty of hardening most temporary and expeditionary structures to mitigate the effects of indirect fire weapons. Dispersal is a form of passive defense that can be used to lessen the possibility that numerous critical assets could be damaged or destroyed in a single attack. This effort would be used in addition to other measures such as standoff distance, revetments, screening, and barriers. Asset dispersal, however, can have an isolating effect that reduces the effectiveness of existing security provisions, increases the complexity of emergency response, and creates less defensible space. The tradeoff between spreading out structures and equipment (past the minimum standoff distance) versus grouping them together will have to be analyzed. This is a risk management decision that must be made by the site commander after considering results of threat assessments, vulnerability assessments, criticality assessments, and recommendations from intelligence personnel, security forces, civil engineers, and other members of the staff. Regardless of where key assets are sited, CE must do everything possible to provide physical protection for these assets based on the identified threat. Reference AFH 10-222, Volume 1, *Guide to Bare Base Development*, for additional information on facility dispersal options.

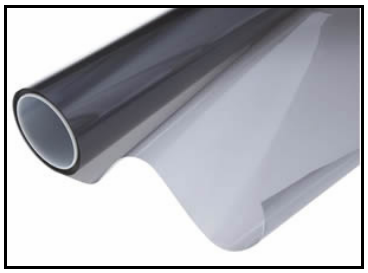
4.4.2.3. **Hardening**. Hardening the different types of temporary and expeditionary structures used during the initial phases of a military operation can be difficult or impractical. This is primarily due to the fact that these structures are designed to be mobile. These structures offer limited protection from threats when compared to permanent facilities constructed by conventional means. Some degree of protection can be achieved by hardening the outer perimeter of these types of structures. **Figure 4.30** is an example of a compacted soil berm being used to protect a structure. Earth-filled barriers such as berms, concertainer units, and sandbags can also be employed around expeditionary structures. Fragmentation barriers provide some degree of protection from impacting primary and secondary debris. These barriers work extremely well for fragment protection; however, they do not reduce blast damage significantly for conventional and expeditionary structures. Concrete barriers of sufficient height can be effective in stopping primary debris (debris from the weapon). However, barriers may also become secondary debris hazards (debris from the barrier itself) in the immediate area of an explosion, causing additional damage to the asset being protected. AFH 10-222, Volume 14 contains information on specific materials and techniques that can be used to harden facilities and other assets to provide some degree of protection.

Figure 4.30. Compacted Soil Revetment.



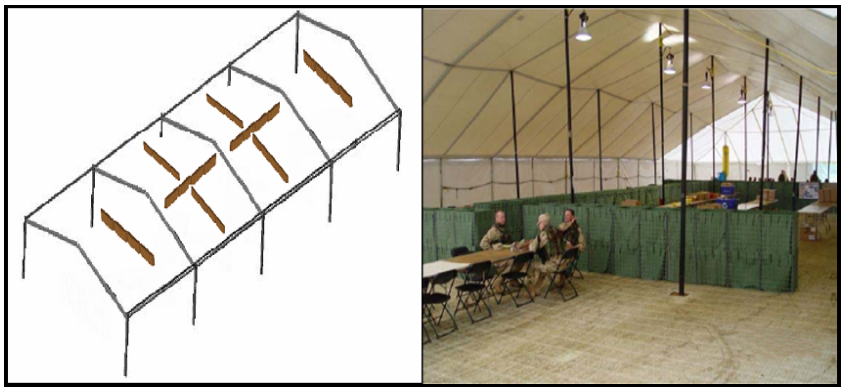
4.4.2.4. **Windows**. Window glass is usually the weakest part of a structure. Glass fragments caused by blasts can result in significant injuries. Although expeditionary structures usually do not contain glass windows, existing facilities occupied by US forces may in fact contain glass windows. If possible, these windows should be removed and the openings closed using plywood or some other protective material. If this is not possible, there are some methods that can be used to reduce hazards from broken glass. One of these is the installation of fragment-retention film (**Figure 4.31**). This is a plastic (polyester) sheet of film that is adhered to the glass with a special adhesive. This modification helps to keep the fragments caused by glass breakage together to prevent the fragments from flying throughout the area and causing severe injury and possibly death. Heavy drapes or a "catcher bar" (metal bar installed across the window) is also needed to prevent the large piece(s) of glass being held together by the retention film from flying through the room and causing blunt trauma injury. Engineering Technical Letter (ETL) 1110-3-501, *Windows Retrofit Using Fragment Retention Film with Catcher Bar System,* contains details on retrofitting windows using fragment retention film. An engineer trained to conduct an analysis that considers many factors (i.e., potential charge weight, standoff distance, size of glass pane, thickness and type of window glass, attachment of the pane to the window frame, and attachment of the frame to the structure) must determine if windows can be properly retrofitted. For this reason, use of protective film in the expeditionary environment should be a last resort. As stated earlier, it is preferable to just remove glass windows and replace them with plywood or some other material.

Figure 4.31. Fragmentation Retention Film.



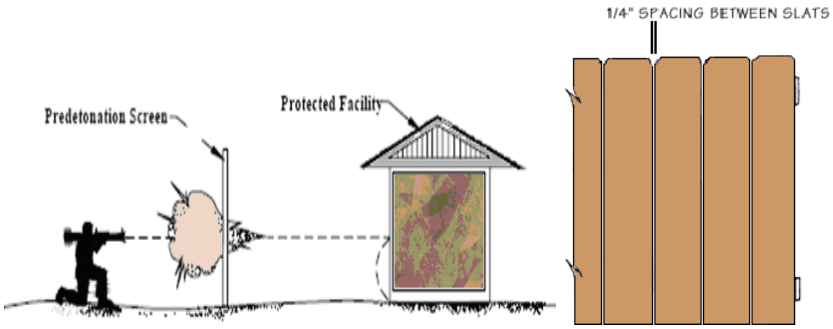
4.4.2.5. **Compartmentalization**. Compartmentalization is a technique used to reduce casualties in high population areas, such as dining and recreation facilities, as a result of fragmenting weapons detonating within the facility. It involves a series of interconnected walls designed to divide large areas of high occupancy into smaller protected areas to limit casualties from impacts of rockets, artillery, and mortars (**Figure 4.32**). Since the primary threat of a fragmenting weapon is its capability to generate fragmented projectiles, the objective of compartmentalization is to contain these fragmentation effects. Considering the weapons of concern in Iraq are the 120 mm mortar and 122 mm rocket, fragmentation effects pose a far more significant threat to compartment occupants than blast. Tests and analyses have shown that significant blast hazard will not generally extend beyond the compartment in which the weapon detonates. In addition to compartmentalization, fragmentation barriers must be constructed around the outside of the facility to mitigate blast and fragmentation from near misses. The minimum height for interior walls and exterior walls is 5 feet and 8 feet, respectively.

Figure 4.32. Example of Compartmentalization.



4.4.2.6. **Predetonation Screens**. A predetonation screen is a solid structure that is built and placed in front of a facility or other asset for the purpose of causing an anti-tank round to detonate before reaching its intended target, thereby dissipating its effects within the distance between the screen and the intended target (**Figure 4.33**). Predetonation screens may consist of wood fences, expanded metal mesh, or heavy woven-fiber fabric. Wood fences can be made of wood slats or plywood panels a minimum of 3/8-inch (9.4 mm) thick. If they are made of slats, the slats should be spaced no more than ¼-inch (6.4 mm) apart. Spaces in metal fabric screens must be 2 inches (50 mm) by 2 inches (50 mm) maximum and the fabric a minimum of 9 gauge (3.8 mm). The residual effects of a predetonated round on a building are more severe than the effects of a dudded round. After predetonation, the weapon's jet and the spent rocket engine from the rocket-propelled grenade continue past the screen. The screen should be located away from the wall at a standoff distance appropriate to the wall construction. For most materials, this is a minimum of 40 feet (10 m). However, it is best to consult UFC 4-020-03 for details on construction and standoff distances for predetonation screens.

Figure 4.33. Predetonation Screening.

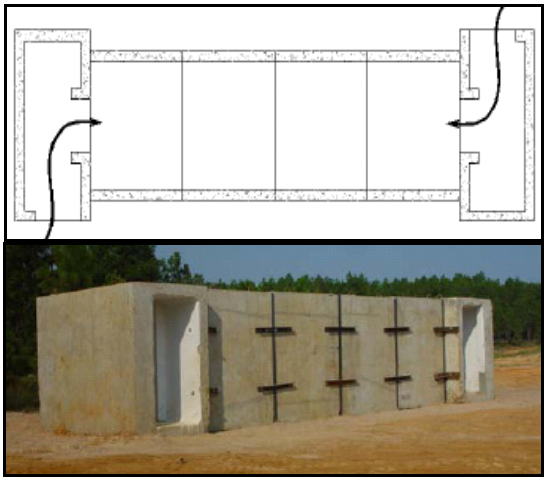


4.4.3. **Revetments**. Revetments are simply walls used to reduce the effects of blast or fragmentation on facilities and equipment resulting from near miss rockets, artillery, and mortars (**Figure 4.34**). They are used to protect parked aircraft or other high-value resources. These structures are also referred to as fragmentation or blast walls. Revetments can be constructed and configured in multiple ways for multiple purposes, using different materials. Engineers should identify revetment requirements through their servicing logistics function and the theater civil engineer staff. Refer to AFH 10-222, Volume 14 for construction details and an overview of the different types of revetments. The *Joint Forward Operations Base Force Protection Handbook* also contains information on different types of revetments.

Figure 4.34. Revetments.

4.4.4. **Personnel Protective Shelters**. Personnel must be able to quickly evacuate expeditionary-type structures in the event of an attack or when attacks are imminent. Protective structures with overhead protection should be sited strategically throughout deployed location, particularly near primary gathering buildings and where large numbers of personnel live and work (**Figure 4.35**). Once fortified with sandbags or enough soil cover, these shelters can provide protection against direct and indirect weapons fire. Sidewall barriers can be constructed using sandbags, earth-filled container structures, earth-filled wire mesh bastions, or concrete walls constructed by civil engineers. Sidewalls must be thick enough to resist direct fire weapons or a near miss from an indirect fire weapon. Covers must be capable of supporting the dead weight from sandbags or earth-filled containers. Only bunker designs approved by the USACE's Engineer Research Development Center should be constructed. Predetonation screens can also be placed above shelters to cause weapons to detonate upon impact, thereby reducing the effects upon the structure. More detailed information on personnel protective shelters can be found in AFH 10-222, Volume 14; the *Joint Forward Operations Base Force Protection Handbook*, the USACE's website, and the TCMS.

Figure 4.35. Personnel Protective Shelter.



4.4.5. **Utilities**. Vulnerability assessments should include the potential for aggressors to damage, destroy, or tamper with site utilities, particularly at those sites where utility lines actually cross the site perimeter. In addition to screening, sealing, and securing utility lines to prevent unauthorized access to the site, civil engineers must focus on providing redundant utility service, eliminating vulnerabilities identified in relation to the threat, and securing all utility production and distribution systems.

4.4.5.1. **Electrical Power**. Power plants are one of the most critical assets in the expeditionary environment (**Figure 4.36**). Protect power plant resources by using revetments, barriers, concertina or barbed wire (entanglements), camouflage, and berming. Depending on the population and size of the installation, power plant dispersal (having two or more plants established and interconnected) may be an option to ensure some degree of power generation capability remains after an attack. Also, power distribution cables should be buried 12-18 inches and spaced at least 6 inches apart. Position mobile electrical power generators near critical facilities and assets they support and harden them against attack. For details on power plant installation, see AFH 10-222, Volume 5, *Guide to Contingency Electrical Power System Installation.*

Figure 4.36. Expeditionary Power Plant.

4.4.5.2. **Water Production and Supply**. Water sources, water purification and distribution equipment, and water supplies must be kept under constant surveillance and tested frequently for contamination. Water transfer pipes can be tapped under pressure using hot-tapping tools, providing aggressors the opportunity to introduce contaminants into the water supply. Civil engineers must work closely with Bioenvironmental Engineering, Public Health, and Safety personnel to ensure water supplies are protected from intentional or unintentional contamination. Water sources must be guarded, water production equipment must be reveted, and water lines must be buried at the first opportunity (**Figure 4.37**). Roving patrols can establish surveillance points that can be used to alert personnel to the possibility of tampering. An emergency response plan should be developed in the event the water supply is contaminated. The plan should include a map indicating the location of all potential water sources, water production equipment, water storage areas, and alternative approaches to supplying safe water (i.e., boiling, special treatment, alternative water supply points, procedures for having bottled water brought in from other sources, etc.). For specific guidance on establishing and maintaining a potable water production capability during deployments, refer to AFI 10-246, *Food and Water Protection Program;* AFPAM 10-219, Volume 5, *Bare Base Conceptual Planning Guide*; and the US Army's Technical Bulletin (TB) MED 577, *Sanitary Control and Surveillance of Field Water Supplies.*

Figure 4.37. Burying Utility Lines.

4.4.6. **Camouflage and Concealment**. Camouflage and concealment are additional tactics used to enhance FP. All personnel should use whatever natural or artificial materials available to hide, blend, and disguise potential military targets. The key to camouflage is to alter the appearance of the asset being protected in a manner where it becomes part of the natural background. Natural cover could include materials such as trees, brush, grass, leaves, rocks or boulders. When using natural cover for concealment, be careful not to disturb the look of the natural surroundings. Use materials commonly found in the area where an asset is to be concealed. Also, natural cover, such as brush and leaves, will have to be changed whenever its appearance no longer looks natural and begins to change from that of its surroundings. Artificial cover could include burlap or netting applied to critical assets (**Figure 4.38**). Military assets can also be painted in a manner so that the asset blends in with the surrounding area. Camouflaging and concealing assets in a desert environment can be challenging. In the end, it is creativity and ingenuity that lead to effective disguises. Camouflage and concealment tactics should be used after hardening and cover are applied to the assets to be protected.

Figure 4.38. Camouflage Netting Being Applied.

4.4.7. **Contract Support**. Once hostilities level off and the initial beddown phase moves towards sustainment, contract support is available to implement and sustain base support operations (**Figure 4.39**). This capability allows military forces to focus more exclusively on achieving military objectives. The Air Force Contract Augmentation Program (AFCAP) is a contingency contract vehicle established as a force multiplier option to augment civil engineer and services capabilities during worldwide contingency planning and deployment operations. AFCAP can provide construction support at overseas locations and can support recovery operations after natural disasters, accidents, or terrorist attacks. The Navy's Global Contingency Construction (GCC) and Global Contingency Services (GCS) contracts are designed to provide worldwide construction and engineering services in response to natural disasters, military conflicts, humanitarian assistance, and a wide range of military operations unrelated to conflicts. The US Army Materiel Command (USAMC) support contract provides engineering, construction, and general logistic services. USAMC is supported by USACE for engineering and construction contract management and by the Defense Contract Management Agency for logistic services contract administration. Contact the MAJCOM Civil Engineer or HQ AFCESA for assistance in getting contract support.

Figure 4.39. Contractors Providing Power Support - Camp Taji (Iraq).

Chapter 5

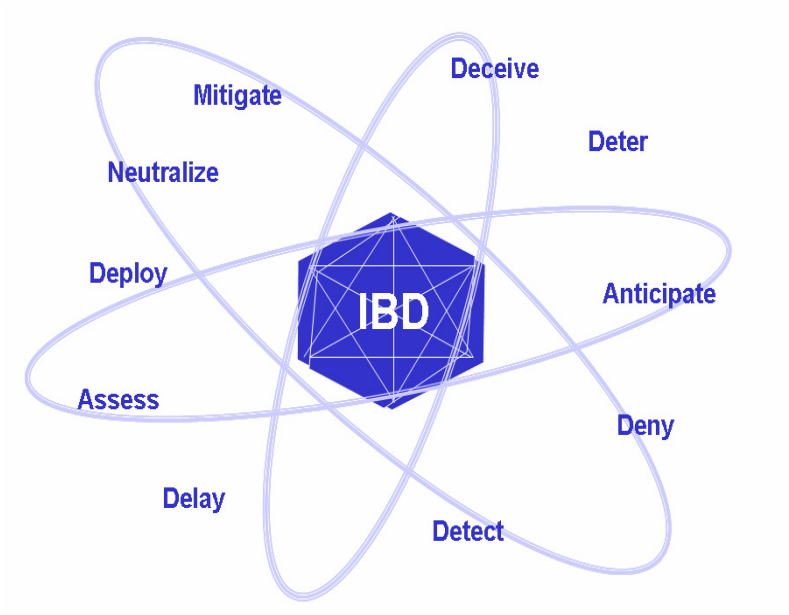
INTEGRATED BASE DEFENSE (IBD)

5.1. Overview. One of the most vital capabilities a base must have to counter threats, especially in an expeditionary environment, is the ability to apply an IBD concept. IBD is defined as the integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the FP battlespace to achieve local and area dominance in support of FP. The IBD battlespace encompasses airfields, priority resources, personnel cantonment areas, base facilities, and accommodation areas, and it extends beyond the physical perimeter. The objectives that guide IBD forces seeking to dominate the battlespace are to see first, understand first, and act first. The conditions influencing IBD are points in the operational spectrum defined by the strategic, operational, and tactical situations. While the methods used to achieve battlespace domination will vary depending on prevailing conditions, the enduring components for success are people and technology. This chapter outlines actions civil engineers must take to support effective application of the IBD concept.

5.2. Essential Capabilities of IBD. Essential capabilities for IBD are those actions deemed critical to successfully plan, program for, and execute combat support operations. They are shown in **Figure 5.1**. The application and methods through which the IBD essential capabilities can be achieved are variable. They depend on the prevailing threat, the operating environment, friendly forces available, rules of engagement, and other factors that characterize the battlespace. For additional information on IBD, refer to AFTTP 3-10.1.

5.2.1. **Assessment**. As stated in **Chapter 2**, an assessment of the threat, including vulnerability, criticality, and risk assessments, must be conducted to determine how best to employ defensive measures. This assessment is usually done by intelligence personnel with assistance from other functional areas, such as security forces and civil engineers. These assessments help to ensure effective application of limited FP resources. Otherwise, time and material could be wasted in an effort to provide total protection for every asset, which is not practical.

Figure 5.1. Essential Capabilities of Integrated Base Defense.



5.2.2. **Delay**. Forcing a delay in an adversary's actions increases the risks for the adversary and provides security personnel time to react and respond. Tactical guidance states that delay cannot be achieved unless there is depth to IBD. The obstacles and elements of security should be employed in layers, forcing the adversary to breach several layers of defense (active and passive) to reach a certain target. The concept of defense in depth does not rely on a single failure point, but rather employs different types of defenses and redundancies to ensure a nearly impenetrable perimeter. Early identification of a threat increases the capability to quickly make a determination of intent and neutralize the threat by applying multiple defensive measures. An example of layered defense would be the ECF zone concept covered in **Chapter 4**. The ECF is laid out in zones, where security personnel perform different functions. As vehicles move through the zones (approach, access, response, etc.), certain security measures are taken. An attempt to breach the ECF would be immediately noticeable and would give security personnel time to detect and react to the attempt and employ a range of measures to stop the vehicle, using deadly force if necessary in the response zone. Civil engineers work closely with intelligence and security personnel to determine how best to establish a layered defense and employ the techniques covered in **Chapter 3** and **Chapter 4** (i.e., site layout, perimeter security, internal security, etc.).

5.2.3. **Denial**. Denial is achieved by taking from the adversary the time, space, and means to conduct an attack. This can be done in many ways, such as blocking culverts and other potential avenues of approach, eliminating or modifying terrain that offers vantage points, employing barriers, constructing berms, ditches, and walls, and installing bollards or other types of vehicle barriers when and where they are needed. This element of IBD also includes all efforts to deny the adversary information through the use of existing security programs such as operations security, communications security, computer security, and information security (also referred to as OPSEC, COMSEC, COMPUSEC, and INFOSEC, respectively).

5.2.4. **Detection**. Detection can be enhanced by employing TTPs that allow us to become aware of an enemy's covert attempts. Several ways to enhance detection include the use of electronic surveillance systems, security lighting, chemical, biological, radiological, and nuclear detection equipment, and alarm systems. Also, constructing elevated observation posts provides security personnel with a clear view of all areas on the site and the surrounding clear zone. In addition, routine checks of critical equipment such as power and water production equipment, storage and distribution equipment, and the like are conducted to quickly uncover any evidence of tampering.

5.2.5. **Anticipation**. Anticipation involves determining options adversaries might take in order to be prepared to respond. Civil engineers employ and implement FP measures during site layout and site buildup based on the threat identified by the intelligence community; not just threats in general.

5.2.6. **Deterrence**. The goal of deterrence is to discourage adversaries from taking offensive action by making the consequences for their actions clear. In addition to consistent execution of RAMs, civil engineers support deterrence by employing obstacles and barriers, hardening facilities, and posting warning signs to make adversaries understand that a successful attack is unlikely.

5.2.7. **Deception**. The goal of deception is to distort the adversary's view and to mislead. Civil engineers support this element of IBD through the employment of decoys (when warranted) and the use of camouflage and other techniques to conceal critical assets. In addition, critical assets can be relocated throughout the site periodically to complicate an adversary's attempt to gain knowledge of military operations through surveillance.

5.2.8. **Mitigation**. Civil engineers use the results of intelligence analyses and guidance from intelligence and security forces in determining how best to mitigate the effects of an attack should aggressors breach defenses and attack a site or target. As covered earlier, mitigation is accomplished by maximizing standoff, providing effective site layout, hardening facilities where practical, constructing barriers, and using techniques such as window film and compartmentalization.

5.2.9. **Deployment**. Rapid response to an attack or an attempted breach of base defense measures must be second nature. Even personnel who are not considered first responders must be prepared to relocate to safer positions or augment first responders as needed. Roads may need to be blocked; power, ventilation, or water distribution systems may need to be temporarily shut-down or re-routed; or heavy equipment may be required to assist first re-sponders. There are many possible scenarios to IBD that will involve not only civil engineers, but every individual on the site or base. Deployment must be constantly rehearsed and exercised to be effective.

5.2.10. **Neutralization**. Neutralization involves all measures necessary to render the adversary or any other threats ineffective. First responders are heavily involved in efforts to neutralize threats to personnel, facilities, or key assets, but require support from all areas.

5.3. **Prescribed Forms:**

None.

5.4. **Adopted Forms:**

None.

KEVIN J. SULLIVAN, Lt Gen, USAF
DCS/Logistics, Installations and Mission Support

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 31-3, *Air Base Defense*, 28 December 2001

AFDD 2-4, *Combat Support*, 23 March 2005

AFDD 2-4.1, *Force Protection*, 9 November 2004

AFI 10-210, *Prime Base Engineer Emergency Force (BEEF) Program*, 24 July 2006

AFI 10-245, *Air Force Antiterrorism (AT) Standards*, 21 June 2002

AFI 10-246, *Food and Water Protection Program*, 4 December 2004

AFI 10-701, *Operations Security (OPSEC)*, 30 September 2005

AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007

AFMAN 10-2602, *Nuclear, Biological, Chemical, and Conventional (NBCC) Defense Operations and Standards*, 29 May 2003

AFMAN 37-123, *Management of Records*, 31 August 1994

AFPAM 10-219, Volume 5, *Bare Base Conceptual Planning Guide*, 1 June 1996

AFH 10-222, Volume 1, *Guide to Bare Base Development*, 1 February 2006

AFH 10-222, Volume 2, *Guide to Bare Base Assets*, 1 April 2006

AFH 10-222, Volume 5, *Guide to Bare Base Power Plant Installation*, 1 October 1998

AFH 10-222, Volume 14, *Guide to Fighting Positions, Obstacles, and Revetments*, 1 November 2000

AFH 10-2401, *Vehicle Bomb Mitigation Guide* (VBMG) (FOUO), 1 September 2006

AFTTP(I) 3-2.34*, Risk Management – Multi-service Tactics, Techniques, and Procedures for Risk Management*, 15 February 2001

AFTTP 3-10.1, *Integrated Base Defense*, 20 August 2004

TB MED 577, *Sanitary Control and Surveillance of Field Water Supplies*, December 2005

IESNA HB-9, *Lighting Handbook*, 1 December 2000

IESNA G-1-03, Guide for Security Lighting for People, Property, and Public Spaces, 1 March 2003

ETL 1110-3-501, *Windows Retrofit Using Fragmentation with Catcher Bar System*, 14 July 1999

MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Facilities*, 15 December 1993

MIL-HDBK-1013/10, Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities, 14 May 1993

MIL-STD-3007, *Department of Defense Standard Practice for Unified Facilities Criteria (UFC) and Unified Facilities Guide Specifications (UFGS)*, 15 February 2006

JP 1-02, *DOD Dictionary of Military and Associated Terms*, 12 April 2001

JP 3-07.2 (FOUO), *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 8 December 2004

JP 3-13.3, *Operations Security*, 29 June 2006

JP 3-34, *Joint Engineer Operations*, 12 February 2007

JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction*, 8 July 2004

JP 3-41, *Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management*, 2 October 2006

UFC 3-340-01, *Design and Analysis of Hardened Structures to Conventional Weapons Effects*, 1 June 2002

UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, 8 October 2003

UFC 4-010-02 (FOUO), *DOD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003

UFC 4-020-01, *DOD Security Engineering Facilities Planning Manual*, 1 March 2006

UFC 4-020-02FA (FOUO), *Security Engineering Concept Design*, 1 March 2005

UFC 4-020-03FA, *Security Engineering Final Design*, 1 March 2005

UFC 4-020-04, Electronic Security Systems: Security Engineering

UFC 4-021-01, *Design and O&M: Mass Notification Systems*, 20 September 2006

UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*, 25 May 2005 UFC 4-022-02, *Selection and Application of Vehicle Barriers*, 10 February 2005

DOD 2000-12, *DOD Antiterrorism Program*, 18 August 2003

DODI 2000.16, *DOD Antiterrorism (AT) Standards*, 2 October 2006

DODI 2000.21, *Foreign Consequence Management*, 10 March 2006

DOD O-2000.12-H (FOUO), *DOD Antiterrorism Handbook*, 9 February 2004

DOD 5200.8-R, *Physical Security Program*, 9 April 2007

Abbreviations and Acronyms

ACP—Access Control Point

AFCAP—Air Force Contract Augmentation Program

AFCESA—Air Force Civil Engineer Support Agency

AFDD—Air Force Doctrine Document

AFOSI—Air Force Office of Special Investigations

AFTTP—Air Force Tactics, Techniques, and Procedures

AOR—Area of Responsibility

AT—Antiterrorism

ATEP—Antiterrorism Enterprise Portal

COMPUSEC—Computer Security

COMSEC—Communications Security

CONEX—Container Express

DIA—Defense Intelligence Agency

DOD—Department of Defense

DODI—DOD Instruction

DTRA—Defense Threat Reduction Agency

ECF—Entry Control Facility

EM—Emergency Management

ETL—Engineering Technical Letter

FOUO—For Official Use Only

FP—Force Protection

FPCON—Force Protection Condition

GCC—Global Contingency Construction

GCS—Global Contingency Services

GIS—Geographic Information Systems

HN—Host Nation

IBD—Integrated Base Defense

IDS—Intrusion Detection System

IESNA—Illuminating Engineering Society of North America

INFOSEC—Information Security

ISO—International Organization for Standardization

JP—Joint Publication

MAJCOM—Major Command

MNS—Mass Notification System

NAVFAC—Naval Facilities Engineering Command

NIPRNET—Non-classified Internet Protocol Router Network

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PDC—Protective Design Center

RAM—Random Antiterrorism Measures; Rockets, Artillery, and Mortars

RDS—Records Disposition Schedule

SEA Hut—Southeast Asia Hut

SIPRNET—Secret Internet Protocol Router Network

TCMS—Theater Construction Management System

TB—Technical Bulletin

UFC—Unified Facilities Criteria

USACE—United States Army Corps of Engineers

UFGS—Unified Facilities Guide Specifications

USAMC—United States Army Materiel Command

VBIED—Vehicle-borne Improvised Explosive Device

WBDG—Whole Building Design Guide

WMD—Weapons of Mass Destruction

Terms

Access Control—Any combination of barriers, gates, electronic security devices, and/or guards used to deny entry to unauthorized personnel or vehicles.

Access Road—Any road (i.e., maintenance, delivery, service, emergency, etc.) that is necessary for the operation of a building or structure.

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 referred to as AT.

Antiterrorism Plan—An AT Plan is the specific measures taken to establish and maintain an AT Program.

Billeting—Any building or portion of a building, regardless of population density, in which 11 or more unaccompanied DOD personnel are routinely housed, including Temporary Lodging Facilities and military family housing permanently converted to unaccompanied housing. Billeting also applies to expeditionary and temporary structures with similar population densities and functions.

Building Hardening—Enhanced conventional construction that mitigates threat hazards where standoff distance is limited. Building hardening may also be considered to include the prohibition of certain building materials and construction techniques.

Building Separation—The distance between closest points on the exterior walls of adjacent buildings or structures.

Combating Terrorism—Combating terrorism within the DOD encompasses all actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts), counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), terrorism consequence management (preparation for and response to the consequences of a terrorist incident/event), and intelligence support (collection and dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, to include terrorist use of chemical, biological, radiological, nuclear materials or high-yield explosive devices (CBRNE).

Communications Security—Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, traffic-flow security, and physical security of COMSEC material.

Computer Security—Measures and controls that ensure security and availability of the information processed, stored, and transmitted by a computer.

Controlled Perimeter—A physical boundary at which vehicle access is controlled at the perimeter of an installation, an area within an installation, or another area with restricted access. A physical boundary will be considered as a sufficient means to channel vehicles to the access control points. At a minimum, access control at a controlled perimeter requires the demonstrated capability to search for and detect explosives. Where the controlled perimeter includes a shoreline and there is no defined perimeter beyond the shoreline, the boundary will be at the mean high water mark.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons or international terrorist activities.

Counterterrorism—Offensive measures taken to prevent, deter and respond to terrorism. Also called CT.

Criticality Assessment—Process used to systematically identify key assets (i.e., personnel, equipment, stockpiles, buildings, etc.) based on their importance to the mission or function and deemed mission critical by commanders.

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.

DOD Building—Any building or portion of a building (permanent, temporary, or expeditionary) owned, leased, privatized, or otherwise occupied, managed, or controlled by or for DOD. DOD buildings are categorized within these standards as uninhabited, inhabited, primary gathering and billeting.

Entry Control Facility—The entry point for all personnel, visitors, and vehicles to the site or installation. Also referred to as the entry control point (ECP) or access control point (ACP).

Expeditionary Structures—Structures intended to be inhabited for no more than one year. This group typically includes tents, Small and Medium Shelter Systems, Expandable Shelter Containers (ESC), International Organization of Standards (ISO) and Container Express (CONEX) containers.

Force Protection—Commander's program designed to protect service members, civilian employees, family members, facilities, information, and equipment in all locations and situations; accomplished through planned and integrated application of combating terrorism, physical security, operations security, and personal protective services and supported by intelligence, counterintelligence, and other security programs.

Force Protection Conditions (FPCONs)—A DOD-approved system standardizing the DOD and Military Services' identification of and recommended preventive actions and responses to terrorist threats against US personnel and facilities. The system is the principal means for a commander to apply an operational decision on how to protect against terrorism and facilitates inter-Service coordination and support for antiterrorism activities.

FPCON NORMAL—This condition applies when a general global threat of possible terrorist activity exists and warrants a routine security posture.

FPCON ALPHA—This condition applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of FPCON BRAVO measures. However, it may be necessary to implement certain measures from higher FPCON measures resulting from intelligence received or as a deterrent. Measures taken under this FPCON must be capable of being maintained indefinitely.

FPCON BRAVO—This condition applies when an increased or more predictable threat of terrorist activity exists. The measures in this FPCON must be capable of being maintained for weeks without causing undue hardship, affecting operational capability, and aggravating relations with local authorities.

FPCON CHARLIE—This condition applies when an incident occurs or intelligence is received indicating some form of terrorist action or targeting against personnel or facilities is likely. Implementation of measures in this FPCON for more than a short period probably creates hardship and affects the peacetime activities of the unit and its personnel.

FPCON DELTA—Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition.

Force Protection Working Group (FPWG)—The commander's cross-functional working group made up of wing and tenant units. Working group members are responsible for coordinating and providing deliberate planning for all antiterrorism/force protection issues. The FPWG should include representatives from relevant disciplines across the installation, including civil engineering, intelligence, AFOSI, security forces, public health, bioenvironmental, disaster preparedness, plans, communications, and other agencies as deemed necessary by commanders, including tenant units.

Giant Voice System—A system typically installed as a base-wide system to provide a siren signal and pre-recorded and live voice messages. It is most useful for providing mass notification for personnel in outdoor areas, expeditionary structures, and temporary buildings. It is generally not suitable for mass notification to personnel in permanent structures because of the difficulty in achieving acceptable intelligibility of voice messages.

Improvised Explosive Device (IED)—Device fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to destroy, incapacitate, harass, or distract. It may incorporate military stores but is usually made from nonmilitary components.

Information Security—Protection of classified information stored on computers or transmitted by radio, telephone, or any other means.

Inhabited Building—Buildings or portions of buildings routinely occupied by 11 or more DOD personnel and with a population density of greater than one person per 40 gross square meters (430 gross square feet). This density generally excludes industrial, maintenance, and storage facilities, except for more densely populated portions of those buildings, such as administrative areas. The inhabited building designation also applies to expeditionary and temporary structures with similar population densities. In a building that meets the criterion of having 11 or more personnel, with portions that do not have sufficient population densities to qualify as inhabited buildings, those portions that have sufficient population densities will be considered inhabited buildings while the remainder of the building may be considered uninhabited, subject to provisions of these standards. EXAMPLE: a hangar with an administrative area. The administrative area would be treated as an inhabited building and the remainder of the hangar could be treated as uninhabited.

Integrated Base Defense—The integrated application of offensive and defensive action, both active and passive, taken across the ground dimension of the force protection (FP) battlespace to achieve local and area dominance in support of force protection.

Intelligence—Product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

Internal Security—Measures used to protect personnel or assets located on the interior of the base.

Level of Protection—The degree to which an asset is protected against injury or damage. This would include personnel and equipment. Levels of protection can be defined as low, medium, or high. For a low level of protection, the structure would be near collapse, a medium level of protection would result in a damaged but repairable structure, and a high level of protection would cause superficial damage to the structure. Selecting the level of protection means trading-off an acceptable level of risk.

Mass Notification System—A system that provides real-time information to all building occupants or personnel in the immediate vicinity of the building during emergency situations.

Obscuration Screen—A physical structure or some other element used to block the line of sight to a potential target.

Operations Security—An analytic process used to deny an adversary information - generally unclassified - concerning friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning processes or operations.

Passive Defense—Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative.

Perimeter Security—Elements that form the first line of defense for an installation. Elements include standoff, physical barriers, access control, entry control points, security lighting, hardened fighting positions and overwatch towers, intrusion detection and surveillance systems, and security forces.

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.

Predetonation Screen—A structure designed to protect a critical asset by causing a weapon to detonate prior to hitting the primary target, causing its effect to dissipate in the distance between the screen and the target.

Primary Gathering Building—Inhabited buildings routinely occupied by 50 or more DOD personnel. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building. For example, an inhabited portion of the building that has an area within it with 50 or more personnel is a primary gathering building for the entire inhabited portion of the building. The primary gathering building designation also applies to expeditionary and temporary structures with similar populations and population densities and to family housing with 13 or more family units per building, regardless of population or population density.

Proactive Measures—In antiterrorism, measures taken in the preventive stage of antiterrorism designed to harden targets and detect actions before they occur.

Random Antiterrorism Measures—Random, multiple security measures that consistently change the look of a site's force protection posture and introduce uncertainty into the site's overall force protection program. These measures make it difficult for terrorists t predict actions or discern patterns or routines.

Risk Management—The process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance risk costs with mission benefits.

Standoff Distance—A distance maintained between a building or portion thereof and the potential location for an explosive detonation.

Structure Group—A cluster of expeditionary or temporary structures consisting of multiple rows of individual structures with 200 or fewer DOD personnel.

Temporary Structures—Structures erected with an expected occupancy of three years or less. Typically includes wood frame and rigid wall construction and such things as Southeast Asia (SEA) Huts, hardback tents, ISO and CONEX containers, pre-engineered buildings, trailers, stress-tensioned shelters, Expandable Shelter Containers (ESC), and Aircraft Hangars (ACH).

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear. It is intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

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

Terrorism Threat Analysis—In antiterrorism, threat analysis is a continual process of compiling and examining all available information concerning potential terrorist activists by groups that could target a facility. A threat analysis will review factors of the presence of a terrorist group, operational capability, activity, intentions, and operating environment.

Threat Assessment—The process used to conduct a threat analysis and develop an evaluation of a potential terrorist threat; the product of a threat analysis for a particular unit, installation, or activity.

Terrorist Group—Any element, regardless of size or espoused cause that commits acts of violence or threatens violence in pursuit of its political, religious, or ideological objectives.

Terrorist Threat Level—Scale used by DOD intelligence agencies to describe the severity of a terrorist threat. Established by DIA and the geographic combatant commander; only applies to threats against DOD interests.

Unified Facilities Criteria—The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria and applies to the military departments, the defense agencies, and DOD field activities in accordance with USD(AT&L) memorandum dated 29 May 2002. UFCs will be used for all DOD projects and work for other customers where appropriate. UFCs are living documents and will be periodically reviewed, updated, and made available to users as part of the Services' responsibility for providing technical criteria for military construction. Headquarters, US Army Corps of Engineers (HQ USACE), Naval Facilities Engineering Command (NAVFAC), and the Air Force Civil Engineer Support Agency (AFCESA) are responsible for administration of the UFC system.

Vulnerability—The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information systems.

Vulnerability Assessment—A Department of Defense-, command-, or unit-level evaluation (assessment) used to determine how vulnerable an installation, unit, exercise, port, ship, residence, facility, or other assets might be to a terrorist attack. Identifies areas of improvement to withstand, mitigate, or deter acts of terrorism or other types of threats.

Weapons of Mass Destruction (WMD)—Weapons that are capable of a high order of destruction and/or of being used in such a manner as to destroy large numbers of people. Weapons of mass destruction can be high explosives or nuclear, biological, chemical, and radiological weapons, but exclude the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

Attachment 2

BASELINE FPCON MEASURES

A2.1. FPCON NORMAL. Applies when a general threat of possible terrorist activity exists but warrants only a routine security posture. Commanders employ Random Antiterrorism Measures (RAMs) during this and all FPCONs to enhance FP.

A2.2. FPCON ALPHA. Applies when there is a general threat of possible terrorist activity against personnel and installations, the nature and extent of which are unpredictable. These measures must be capable of being maintained indefinitely.

A2.2.1. At regular intervals, remind all personnel to be suspicious and inquisitive of any strangers on or near the site. Watch for suspicious packages or abandoned parcels, suitcases, etc.

A2.2.2. Secure and randomly inspect buildings, rooms, and storage areas not in regular use.

A2.2.3. Conduct random security spot checks of vehicles and persons entering facilities under the jurisdiction of the United States.

A2.2.4. Limit access points for vehicles and personnel commensurate with a reasonable flow of traffic.

A2.2.5. Identify critical assets and high occupancy buildings.

A2.2.6. Continue or introduce all FPCON NORMAL measures.

A2.2.7. Ensure all personnel are briefed on the threat, and remind them to be alert for and to report suspicious activities, such as the presence of unfamiliar personnel and vehicles, suspicious parcels, and possible surveillance attempts.

A2.2.8. Key personnel required to implement civil engineer FP measures should be placed on call.

A2.2.9. Conduct spot checks of vehicles, equipment, supplies and facilities.

A2.2.10. Conduct spot checks of water production equipment and supplies.

A2.2.11. Conduct spot checks of power production equipment and supplies.

A2.2.12. Conduct spot checks of heating, air conditioning, and ventilation equipment and supplies.

A2.2.13. Secure all hazardous material storage areas, particularly where large quantities are stored (i.e., hazardous material storage area, hazardous waste storage area, POL storage areas, etc.).

A2.2.14. Test communication procedures and verify key personnel can be contacted quickly if needed to implement additional protective measures.

A2.2.15. Train personnel on individual protective measures.

A2.2.16. Train and exercise personnel on how to react to an attack and where to take shelter (i.e., shelter in place, protective bunkers, etc.).

A2.2.17. Review all plans (i.e., barrier plans, dispersal plans, equipment surveillance plans, etc.) and identify resource requirements.

A2.2.18. Ensure personnel assigned to all emergency response teams are trained, on call, and capable of responding immediately.

A2.2.19. Consult with HN personnel if applicable, to verify any mutual support agreements.

A2.2.20. Review all higher FPCON measures and be prepared to implement measures of the next higher FPCON level.

A2.3. FPCON BRAVO. Applies when an increased and more predictable threat of terrorist activity exists. These measures must be capable of being maintained for weeks without causing undue hardship or extreme traffic delays, affecting operational capability, or aggravating relations with local authorities.

A2.3.1. Fully implement all measures of lower FPCON levels.

A2.3.2. Review contingency plans to ensure all resources required for implementation are available and all equipment is fully operational. Keep all personnel involved in implementing site contingency plans on call.

A2.3.3. As needed, erect and emplace barriers; construct berms, ditches, revetments, and predetonation screens; and install obscuration screening.

A2.3.4. Enforce control of entry into critical facilities, lucrative targets, and high-profile locations; and randomly search vehicles entering these areas. Particular scrutiny should be given to vehicles that are capable of concealing a large IED (i.e., cargo vans, delivery vehicles, etc.) sufficient to cause catastrophic damage to property or loss of life.

A2.3.5. Keep cars and objects (e.g., crates, trash containers) away from buildings to reduce vulnerability to bomb attacks. Apply this criterion to all critical and high-occupancy buildings. Consider applying to all inhabited structures to the greatest extent possible.

A2.3.6. Review current level of protection for all facilities (particularly primary gathering facilities and expeditionary structures) and critical assets; determine if levels of protection may need to be increased.

A2.3.7. Review standoff distances to ensure they meet minimum requirements, and consider the need to increase standoff distances.

A2.3.8. Consider centralized parking and implementation of barrier plans.

A2.3.9. Secure and periodically inspect all buildings, rooms, and storage areas not in regular use. At the beginning and end of each workday, as well as at random intervals, inspect the interior and exterior of all buildings for suspicious packages.

A2.3.10. Screen all mail packages to identify suspicious letters and parcels.

A2.3.11. Randomly inspect commercial and delivery vehicles.

A2.3.12. Randomly inspect water production, storage, and distribution equipment and lines for evidence of tampering or contamination.

A2.3.13. Patrol the site landscape looking for evidence of suspicious activity.

A2.3.14. Identify and brief personnel who may augment guard forces. Review specific rules of engagement including the use of deadly force.

A2.3.15. As deemed appropriate, verify identity of personnel entering all buildings.

A2.3.16. Review status and adjust as appropriate operations security, communications security, and information security procedures.

A2.3.17. Erect barriers/guard structures at entrances to airfields if needed.

A2.3.18. As appropriate, take actions to mitigate the threat of surface-to-air missiles or standoff weapons that can be delivered from beyond the airfield perimeter.

A2.3.19. Routinely inspect the perimeter fence and barriers to ensure there is no break in the fence line and that barriers have not been breached.

A2.3.20. Review all higher FPCON measures.

A2.4. FPCON CHARLIE. Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel and installations is imminent. Implementation of this measure for more than a short period may create hardship and affect the peacetime activities of the unit and its personnel.

A2.4.1. Fully implement all measures of lower FPCON levels.

A2.4.2. Recall additional required personnel. Ensure armed augmentation security personnel are aware of current rules of engagement and any applicable Status of Forces Agreements (SOFA). Review types of weapons and ammunition issued to augmentation security personnel. Heightened threats may require employment of different weapon capabilities.

A2.4.3. Be prepared to react to requests for assistance from both local authorities and other installations in the region.

A2.4.4. Limit access points in order to enforce entry control.

A2.4.5. Randomly search vehicles.

A2.4.6. Ensure or verify the identity of all individuals entering food and water storage and distribution centers, use sign-in and sign-out logs at access control and entry points, and limit or inspect all personal items.

A2.4.7. Initiate monitoring activity for chemical, biological, and radiological contamination as required. An alternate locally developed measure should be implemented when contractors are responsible for water supplies or when water is provided by local (non-DOD) sources or agencies.

A2.4.8. Increase standoff distances from sensitive buildings based on the threat. Implement barrier plan to hinder vehicle-borne attack.

A2.4.9. Increase patrolling of the installation/facility/unit including waterside perimeters, if appropriate. Be prepared to assist local authorities in searching for threatening actions and persons outside the perimeter.

A2.4.10. Protect all infrastructure deemed critical to the operational mission. Give special attention to and coordinate with local authorities regarding infrastructure located outside of the perimeter that may affect operations being conducted inside the perimeter.

A2.4.11. To reduce vulnerability to attack, consult local authorities about closing public (and military) roads and facilities and coordinate any other precautionary measures taken outside the installation perimeter.

A2.4.12. Randomly inspect suitcases, and briefcases, packages being brought onto the installation through access control points, and consider randomly searching them as they are taken off the installation.

A2.4.13. Review access procedures for all non-US personnel and adjust as appropriate. For airfields, consider terminating visitor access to the flight line and support facilities.

A2.4.14. Review all FPCON DELTA measures.

A2.5. FPCON DELTA. Applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, FPCON DELTA is declared as a localized warning and is not intended to be sustained for lengthy periods of time.

A2.5.1. Fully implement all measures of lower FPCON levels.

A2.5.2. Augment guards as necessary.

A2.5.3. Identify all vehicles within operational or mission support areas.

A2.5.4. Control facility access and implement positive identification of all personnel with no exceptions.

A2.5.5. Search all personally carried items (e.g., suitcases, briefcases, packages, backpacks) brought on site or into a facility.

A2.5.6. Make frequent checks of the exterior of buildings and of parking areas.

A2.5.7. Restrict all nonessential movement.

A2.5.8. Be prepared to barricade roads and facilities throughout the site and leading to the airfield, if necessary.

A2.5.9. Begin continuous monitoring for chemical, biological, and radiological contamination.

Attachment 3

SITE SELECTION AND LAYOUT CONSIDERATIONS

A3.1. Site Selection. It may not be possible to select sites that meet all requirements needed to implement effective force protection measures; nevertheless, a list of considerations should be developed and used during the site selection process. The following are examples of some elements that should be considered.

A3.1.1. Consider the threat throughout the entire site selection process.

A3.1.2. Consider minimum antiterrorism standards established by DOD and whether the site will support or inhibit efforts to attain and maintain antiterrorism standards.

A3.1.3. Consider force protection standards established by the geographic combatant commander and whether the site will support or inhibit efforts to attain and maintain these standards.

A3.1.4. Select a site that provides the opportunity to maximize standoff distances.

A3.1.5. Site beddown areas away from public roads and uncontrolled areas.

A3.1.6. Avoid areas where terrain features provide too many vantage points.

A3.1.7. Avoid areas that do not provide enough space to achieve sufficient standoff.

A3.1.8. Consider future need for additional space to support a population increase.

A3.1.9. Consider future need to increase standoff distances as a result of higher threat levels.

A3.1.10. Consider space needed for protective construction (i.e., bunkers, overwatch towers, defensive fighting positions, revetments, sidewall protection, blast and fragmentation barriers, vehicle barriers, perimeter barriers, etc.).

A3.1.11. Consider the need to establish a defense-in-depth posture for integrated base defense.

A3.1.12. Consider adjacent land use and direct lines of sight or access to the site.

A3.1.13. Consider the need to modify terrain outside of the established perimeter to provide clear zones and eliminate potential hiding places.

A3.1.14. Consider support needed from the local area (i.e., utilities, sanitation, indigenous materials, equipment, etc.) and how this will impact force protection efforts.

A3.1.15. Consider site elevation to ensure the elevation of the proposed site does not provide an advantage for potential aggressors (i.e., lines of sight, targeting opportunities, etc.).

A3.1.16. Consider the use of existing facilities and efforts needed to retrofit the facilities to meet minimum antiterrorism standards or standards established by the geographic combatant commander as a result of a known threat.

A3.1.17. Evaluate potential use of existing roads to enhance force protection efforts.

A3.1.18. Consider the need to establish separate ECPs for delivery vehicles.

A3.1.19. Consider the need for vehicle queue space and search pits.

A3.1.20. Consider the need to disperse key facilities and critical assets.

A3.1.21. Select a site that lends itself to establishing an effective controlled perimeter.

A3.1.22. Consider the need to bury utility lines.

A3.1.23. Consider the need to orient facilities to avoid direct line of sight from the perimeter.

A3.1.24. Consider the need to site high-value facilities and assets near the center of the site.

A3.2. Site Layout. Some key areas to consider during site layout include standoff distances, layered security, minimum and separate ECPs, redundant utilities, protection of all key assets, ammunition storage, hazardous material and hazardous waste storage, and protective shelters throughout the site. Maintain maps that indicate, in detail, where every asset will be placed and where all protective construction (i.e., revetments, bunkers, etc.) will take place. Following are some elements to consider during site layout.

A3.2.1. Use the threat assessment to determine how best to site facilities in relation to existing roads and the controlled perimeter.

A3.2.2. Consider minimum antiterrorism standards established by DOD when siting facilities and critical assets.

A3.2.3. Consider force protection standards established by geographic combatant commanders when siting facilities and critical assets.

A3.2.4. Maximize standoff distance between the controlled perimeter and inhabited buildings and other key assets.

A3.2.5. Limit entry control points to an absolute minimum, and establish a separate entry control points for trucks and delivery vehicles at an appreciable standoff distance from inhabited facilities, primary gathering buildings, and other key assets.

A3.2.6. Consider terrain, elevation, and space available when determining where to site the ECF. Include space for approach zones, access zones, and response zones, queue space; parking space, and space for vehicle search pits. Use AFH 10-2401 and UFC 4-022-01 as guidance for ECF layout.

A.3.2.7. Clear dense vegetation that can be used by adversaries to hide and conduct surveillance, attempt to gain access to the site, or target a particular facility or critical equipment.

A3.2.8. Avoid having straight-line roads or roads that are perpendicular to critical facilities or assets.

A3.2.9. Construct berms and ditches to enhance perimeter security.

A3.2.10. Avoid siting structures and critical equipment in areas where terrain offers vantage points from which terrorists might target facilities and other critical assets.

A3.2.11. Site key facilities and critical assets towards the center of the site to attain maximum standoff distance from the perimeter.

A3.2.12. Provide redundant utility systems and bury all utility lines.

A3.2.13. If the threat warrants, disperse facilities and key assets to reduce the possibility of collateral damage to multiple assets from a single attack.

A3.2.14. If key assets can be better protected if clustered and force protection resources are available to increase their level of protection, consider this option.

A3.2.15. Orient facilities in a manner that reduces a direct line of sight from outside the perimeter and in a manner that limits the amount of damage from a blast (end-on towards the area of the potential blast versus the sides facing the area of the potential blast).

A3.2.16. Compartmentalize primary gathering facilities to limit damage and injuries from fragmenting weapons in the event of an attack.

A3.2.17. Site areas where revetments and other protective structures (blast/fragmentation walls) must be constructed (i.e., critical assets and key primary gathering facilities, etc.).

A3.2.18. Site facilities that will receive bulk deliveries and other structures that may be more vulnerable to an attack (i.e., industrial areas, hazardous waste/hazardous storage areas, refuse collection areas, etc.) in areas away from the main inhabited portion of the site. These areas must still be secured.

A3.2.19. Assist security personnel in constructing layers of defense to support the IBD effort.

A3.2.20. Ensure parking areas are constructed to provide the minimum stand-off distance from facilities as determined by DOD standards or the geographic combatant commander.

A3.2.21. Site areas for placing trash containers away from facilities and other key assets (at least 10 m/33 ft).

A3.2.22. Site personnel bunkers strategically throughout the site (particularly in highly populated areas) to provide shelter in the event of an attack.

A3.2.23. Site mass notification system components in all areas so that voice notification can be heard throughout the entire site and outside the perimeter.

A3.2.24. Outline the plan to apply hardening, camouflage, and concealment to all key facilities and critical assets once the assets are sited.

A3.2.25. Outline the plan to block lines of sight and lessen the severity of damage to key facilities/assets in the event of an attack (i.e., obscuration screens, predetonation screens, window film application, etc.).