AIR FORCE TACTICS, TECHNIQUES, AND PROCEDURES 3-32.34V3

1 March 2016

CIVIL ENGINEER EXPEDITIONARY FORCE PROTECTION

DEPARTMENT OF THE AIR FORCE

BY ORDER OF THE
AIR FORCE TTP 3-32.34V3
SECRETARY OF THE AIR FORCE

1 March 2016

Operations

CIVIL ENGINEER EXPEDITIONARY FORCE PROTECTION

OPR: AFCEC/CXX

Certified by: AF/A4C
(Maj Gen Timothy S. Green)

Supersedes: AFH 10-222V3, 1 May 2008

Pages 83

This publication implements civil engineer force protection requirements and force protection training outlined in AFI 10-210, *Prime Base Engineer Emergency Force (BEEF) Program*. It addresses expeditionary force protection tactics, techniques, and procedures (TTP) for use by Air Force (AF) civil engineers to protect mission-critical assets including personnel, facilities and equipment during deployments. It is applicable to Regular Air Force, Air National Guard, and AF Reserve engineers. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance

with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW AF Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). 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 AF.

Chapter 1

INTRODUCTION

1.1. Overview. Force Protection (FP) is critical to the Air Force's ability to perform its worldwide mission and is a top priority for commanders. It is a fundamental principle of military operations as a way of ensuring survivability of forces. Commanders at all levels are responsible for protecting Air Force people and warfighting resources. However, all Airmen are also responsible for FP and need to be prepared, trained, and equipped to protect and defend operations and assets. This publication provides guidance to civil engineers (CE) on implementing FP measures in the expeditionary environment. Many of the references listed throughout this publication are For Official Use Only (FOUO) publications. CE planners maintain copies of these publications and ensure they are available throughout all phases of expeditionary operations.

1.2. Scope. The information in this AFTTP relates to tactics, techniques, and procedures (TTPs) used by civil engineers in supporting precepts outlined in Air Force Doctrine Annex (AFDA) 3-34, *Engineer Operations*. It also supports implementation of Air Force Policy Directive (AFPD) 10-2, *Readiness*, and AFI 10-210, *Prime BEEF Program*.

1.3. Force Protection Defined. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines FP as "Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information." Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease. By comparison, North Atlantic Treaty Organization (NATO) doctrine explains that the operational environment "may have no discernable front-line or rear area and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities." Consequently, NATO includes all operations and activities as potential vulnerabilities under FP. The AF definition of FP covers natural and manmade threats. In Air Force Instruction (AFI) 10-245, *Antiterrorism (AT)*, the definition includes an "integrated approach that requires actions to both defeat the enemy and protect against hazards such as accidents, weather, disease, and natural disasters." The complete definitions are shown in **Attachment 1**.

1.4. Force Protection Doctrine. For much of its existence, the Air Force has been able to rely on the US Army when necessary, for standoff security. In fact, in 1985 the Chiefs of Staff of the Air Force and Army signed *Joint Security Agreement 8* which specified that the Army would provide ground defense outside the perimeter of Air Force bases. However, several subsequent joint exercises, as well as experience in Operations Desert Shield and Desert Storm, showed this arrangement was impractical. The formal agreement remained in effect until 2005, at which time Joint Publication 3-10, *Joint Security Operations in Theater*, codified that the Air Force would defend its own air bases.

1.4.1. Additionally, for most of the Cold War Air Force doctrine was primarily based on the expectation that expeditionary bases would be located in a rear area where the threat would be greatly reduced. In reality, during recent conflicts (especially in Iraq and Afghanistan) many bases were located in urban areas and the perimeter of the base represented the line of contact with the enemy.

1.4.2. Air Force Doctrine Annex (AFDA) 3-10, *Force Protection*, states that FP is achieved through the successful execution of three related but distinct lines of effort: integrated defense, emergency management, and the critical asset risk management program (formerly known as the critical infrastructure program [CIP]). These lines of effort are reviewed in the following paragraphs. The purpose is to integrate these capabilities and achieve the desired FP effects of detect, deter, preempt, negate, and mitigate. AFDA 3-10 also states that the specific and pivotal role of civil engineers is to "design physical security improvements, provide planning, training, and response capabilities to deal with FP-related incidents, and provide explosive ordnance disposal capabilities." It describes three levels of FP threat (**Table 1.1**). Keep in mind that these threats may not occur in any specific sequence or may not even appear to be related.

Table 1.1. Force Protection Threat Levels.

Level I Threats: Include enemy agents, sympathizers, partisans, and terrorists whose primary missions include espionage, sabotage, and subversion.
Level II Threats: Small-scale tactical forces conducting unconventional or hit and run attacks; may include significant standoff weapons such as mortars,

rockets, and rocket propelled grenades.
Level III Threats: Large ground operations; airborne, heliborne, and amphibious operations; air and missile attacks with little warning; operations having the capability of projecting combat power by air, land, and sea anywhere into the operational area.

1.5. Integrated Defense (ID). Effective ID helps ensure effective FP. As mentioned earlier, ID is an AF-wide responsibility and is conducted worldwide, from mature theaters to austere regions. Regardless of location, forces conducting ID employ the basic tactics, techniques, and procedures (TTPs) as those employed at home station during day-to-day operations. As specific threats to base personnel and resources evolve, ID forces adjust TTPs to counter the threat. Adjustments to operating procedures are based on the specific threat to operations; the dynamics of operating in an international environment or the way ID efforts collaborate with joint, combined, civilian, and host nation forces. ID is discussed in broader detail in Chapter 5. For additional information on ID see AFI 31-101, *Integrated Defense*.

1.6. Emergency Management (EM). The protection of AF personnel and resources on AF installations is essential to ensure successful AF operations. The AF EM Program addresses activities across the all-hazards physical threat environment at Continental United States (CONUS) and Outside Continental United States (OCONUS) home station or expeditionary locations to support overall FP. The primary mission of the AF EM Program is to save lives; minimize the loss or degradation of resources; and continue, sustain, and restore operational capability in an all-hazards physical threat environment at AF installations worldwide. The ancillary missions are to support homeland defense and civil support operations and to provide support to civil and host nation authorities according to DOD directives and through the appropriate combatant command (CCMD).

1.6.1. **Air Force Incident Management System (AFIMS).** EM supports protection of personnel and resources through integration of installation preparedness, response, and recovery programs aimed toward reducing the impact of these events on the installation; prepares for risks that cannot be eliminated; and prescribes actions required to deal with consequences of actual events and to recover from those events using AFIMS. See AFI 10-2501, *Air*

Force Emergency Management (EM) Program Planning and Operations for more information on the IEM program.

1.7. Critical Asset Risk Management (CARM) Program. Operations in support of the National Military Strategy are dependent on globally linked physical and cyber infrastructures (US and foreign, public and private sector). CARM interconnects infrastructures, while improving capabilities and mission effectiveness, also decreasing vulnerabilities due to potential human error failures during natural disasters or intentional attack. The mission of the AF CARM Program is to enhance risk management decision-making and ensure that AF critical infrastructure is available to support CCMD and AF mission requirements in an all-threat and all-hazard environment. This risk management approach supports AF prioritization of scarce resources, focusing on the greatest risk based on assessed criticality, vulnerability, threats, and hazards. For additional information on the critical infrastructure program, see Air Force Policy Directive (AFPD) 10-24, *Air Force Critical Infrastructure Program (CIP).*

1.8. Force Protection Effects. FP effects are designed to prevent attacks on DOD assets and interests and minimize the effect of attacks. It is unrealistic to assume every DOD asset can be protected. For this reason, plans and preparations to recover from an attack are focused on enabling the mission to continue and restoring confidence within the unit and throughout the local population. FP efforts conserve the AF's fighting potential by safeguarding its forces and mission capability through achievement of predetermined effects. In all circumstances, commanders tailor resources and capabilities to achieve, at minimum, the following FP effects:

1.8.1. **Deter.** Develop measures to discourage adversarial actions by creating the perception of the existence of a credible threat of unacceptable counteraction. Potential adversaries must perceive the AF has the capability to conduct and sustain offensive and defensive operations. Measures civil engineers can take include placing barriers and roadblocks, strategically locating assets, and ensuring sufficient standoff to reduce the chances of an attack.

1.8.2. **Detect.** Develop measures to identify the presence of an object or an event of possible military interest, whether a threat or hazard. Detection may arise

through civil engineer reconnaissance and observation of the operational area or through deductions made following an analysis of the operational area.

1.8.3. **Preempt.** Once evidence indicating an imminent enemy attack is determined, rapid actions are initiated to respond and establish or gain a position of advantage to eliminate the threat. Essential to effective preemptive operations is an accurate estimation of adversary's capabilities and vulnerabilities. All available intelligence and counterintelligence resources, including civil engineer reconnaissance, are used to determine enemy capabilities, intentions, and probable courses of action. This also includes emergency management planning and training.

1.8.4. **Negate.** Measures taken to render a threat or hazard incapable of interfering with AF operations. This includes the effective employment of coordinated and synchronized offensive and defensive measures and measures to counteract hazards. For example, civil engineers designing and constructing security improvements, protective shelters, fighting positions, obstacles, and revetments as well as EOD capabilities.

1.8.5. **Mitigate.** If actions to negate are unsuccessful employ the full range of active and passive measures such as civil engineers supporting hardening and sidewall protection to lessen the impact of terrorist events against DOD assets.

1.9. Force Protection Condition (FPCON) System. The FPCON system standardizes identification and recommended preventive actions and responses to terrorist threats against US personnel and facilities Table 1.2. FPCON measures are actions taken to deter and/or prevent terrorists from conducting an attack. FPCON measures assimilate facilities, equipment, trained personnel, and procedures into a comprehensive effort designed to provide optimal protection to personnel and assets and are tailored to a specific site. FPCONs are not to 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. AFI 10-245 contains FPCON measures that civil engineers may have to implement during increased FPCON levels.

Table 1.2. 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, 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 are capable of being maintained indefinitely.
Bravo–Increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and military-civil relationships with local authorities.
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. Prolonged implementation of 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 has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for an extended duration.

1.10. 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. Combatant commanders (CCDR) also set terrorist threat levels for specific personnel, family members, units, and installations within their areas of responsibility (AOR) using definitions established by the DIA. Terrorist threat levels are not to be confused with FPCONs that affect the local security posture. Threat level assessments are provided to senior leaders to help determine local FPCONs. Terrorist threat levels are also not to 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.

Table 1.3. Determining 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.
Additional sources of information on terrorist threat levels include AFI 10-245.

1.11. Training. Training is essential to establishing effective FP. The key to effective FP is awareness that is sustained and reinforced from initial entry to termination of DOD service. More specifically, AT training is integrated into training for all AF personnel as required and when deemed appropriate by commanders with AT responsibility. To enable commanders to make the most effective decisions possible, personnel at all organizational levels receive AT training. All personnel are aware of basic personal protective measures and specific threats for the areas they operate in, and receive specialized training for their duty position. AFI 10-245 specifies minimum AT training requirements and the current AT training for AF personnel consists of the four levels shown in **Figure 1.1**.

Figure 1.1. Antiterrorism Training Concept.

Level I training is available on the DOD Antiterrorism website located at https://jkodirect.jten.mil. As part of the Annual Total Force Awareness Training, the Force
Protection (ZZ133079) course is available on the Advanced Distributed Learning System site at https://golearn.csd.disa.mil/kc/rso/login/adls_login.asp. Refer to AFI 10-245 to obtain training sources for levels II through IV. **Table 1.3** defines the four AT levels of training.

Table 1.4. Antiterrorism Training Levels.

Level I AT Awareness Training
Level I training is provided annually to all AF personnel with requisite knowledge necessary to remain vigilant for possible terrorist actions and enable employment of the AT TTP as outlined in AFI 10-245, to include every AF Service member, civilian employee, and local national or other country national in a direct-hire status by the DOD, regardless of grade or position. Introduces terrorism and terrorism operations such as personal protective measures, terrorist surveillance techniques, improvised explosive devices (IED), and kidnapping and hostage survival tactics.
Level II Antiterrorism Officer/Antiterrorism Representative Training
Level II training is a resident course designed to prepare officers and Non-Commissioned Officers who have at least two years AT experience to serve as Antiterrorism Officer (ATO). Unit level Antiterrorism Representatives (ATRs) unable to secure in-residence training will complete the AT Level II Refresher

Training (within 180 days) until they are able to attend the AT Level II in-residence course. For both ATOs and ATRs, Level II refresher training is completed once every three years to maintain qualification.
Level III Pre-Command AT Training
Level III training provides prospective squadron, group, and wing commanders and civilian equivalent positions at the O5/O6 level with requisite knowledge to direct and supervise an AT Program. Group/Wing commanders receive the training through Group/Wing commander pre-command courses. Follow on training may be conducted at the installation-level as a refresher or supplement to briefings offered in commander courses.
Level IV AT Executive Seminar
Level IV seminar provides DOD senior military and civilian executive leadership with requisite knowledge to enable development of AT program policies and facilitate oversight of AT programs at the operational and strategic levels. Wing and group commanders and other command and staff officers in the grades O-6 through O-8 and civilian equivalent/senior executive service civilian employees may attend.

Chapter 2

CIVIL ENGINEER ROLE IN FORCE PROTECTION AND ANTITERRORISM

2.1. Overview. Combating unconventional and asymmetrical threats within DOD encompasses antiterrorism (AT), terrorism consequence management (TCM), and intelligence support (IS). The intent is to oppose terrorism throughout the entire threat spectrum, including terrorist use of chemical, biological, radiological, or nuclear (CBRN) materials and explosive hazard (EH) devices. AT is defensive measures taken to reduce vulnerability of individuals and property to terrorist acts; CT is offensive measures taken to prevent, deter, and respond to terrorism; TCM is preparation for and response to the consequences of a terrorist incident/event; and IS is collection and dissemination of terrorism-related information. AF civil engineers are relied upon to implement AT and CT measures, such as fence and berm construction shown in **Figure 2.1**, particularly in expeditionary environments where the threat level is high due to ongoing military operations.

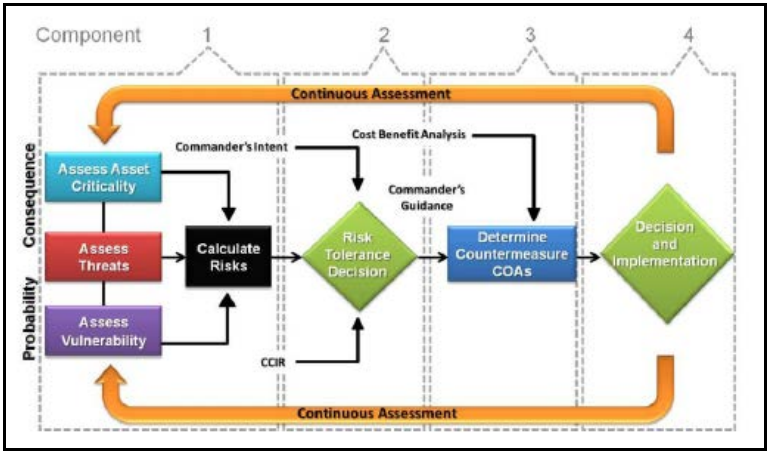
Figure 2.1. Berm Construction in Afghanistan.

2.2. Antiterrorism (AT). As stated earlier, AT is not to be used as a synonymous term with FP. Rather; AT is a sub-element of combating terrorism, which is a subset of the broader FP concept. The AT program is 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 personnel and critical facilities, (2) perimeter security, and (3) mitigation of blast and fragmentation effects through facility hardening and other means. Civil engineers contribute to overall AT efforts in several ways, including ensuring effective standoff, placing barriers, and assisting security forces to establish a defense in-depth capability (layered defense). These types of efforts provide additional deterrence and increase time for security forces to respond in the event of an attack.
Reference JP 3-07.2 and AFI 10-245 for additional details on AT standards and procedures.

2.3. Risk Management. Risk management is the process of identifying, assessing, and controlling risks arising from operational factors and making decisions that balance possible adverse outcomes with mission benefits (**Figure 2.2**). The decision-making process is called a risk assessment. Risk assessments provide commanders with a method to assist in making resource allocation decisions designed to protect personnel and assets from possible 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 may be too reactive and result in wasted efforts and resources. The key role of civil engineers in these three components is discussed later in this chapter. 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 AT plans also participate in risk assessments. The information collected during the risk assessment is critical to developing effective FP plans. For more information on risk management, refer to AFI 10-245 and AFI 31-101.

Figure 2.2. Antiterrorism Risk Management Process.



2.3.1 **Threat Assessment.** The threat assessment is the process used to conduct an analysis and develop an evaluation of a potential threat consistent with the Integrated Defense Risk Management Process (IDRMP) outlined in AFI 31-101. It identifies the full range of known or estimated threat capabilities, including the use or threat of CBRN and EH. It is usually conducted by intelligence personnel; however Air Force Office of Special Investigations (AFOSI) is the AF agency responsible for preparing specific threat assessments. 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 capability, intentions, TTPs, history, probable course of action, and targeting as well as the security environment within which friendly forces operate. The DOD Antiterrorism Officer (ATO) Guide (FOUO) contains guidance on conducting threat assessments. AFI 10-245 also contains limited threat assessment guidance. **Note:** Civil engineer squadrons, through the Emergency Management Working Group, develop and publish an All-Hazards Threat Assessment as part of the All-Hazards Risk Management Process.

2.3.1.1. **Identifying the Threat.** Along with security forces, civil engineers generally have primary responsibility for preparing a design basis threat (DBT),

which describes threats in specific terms. The DBT is established for each installation to identify and evaluate 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. It is a critical component for engineering projects and renovations. The threat identification also includes tactics likely to be used, such as stationary or moving vehicle bombs, airborne or waterborne contamination, bomb delivery via mail or supply shipments, forced or covert entry, standoff or ballistic weapons, visual surveillance, acoustic eavesdropping, and insider compromise. Identifying the specific threat helps in determining asset vulnerability. This information can then be used by civil engineers to develop and implement protective measures to counter the specified threat.

2.3.1.2. **Planning for the Threat.** The threat level assigned to the country or region where a unit may be deploying helps to plan protective measures throughout all phases of deployments, including pre-deployment, initial beddown, sustainment, and redeployment. Upon notification of deployment, unit commanders immediately contact their servicing AFOSI detachment and request a counterintelligence threat assessment. Again, civil engineers are familiar with FP governing directives and can support operations by serving on the installation planning team responsible for preparing the DBT. For DBT planning purposes, Unified Facility Criteria (UFCs) 4-010-01, *DOD Minimum Antiterrorism Standards For Buildings*; 4-020-01, *DOD Security Engineering Facility Planning Manual*; and 4-010-02, *DOD Minimum Antiterrorism Standoff Distances for Buildings (FOUO),* 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 permanent structures.

2.3.2. **Criticality Assessment.** The criticality assessment identifies the relative criticality of assets based upon mission criticality, impact on national defense, replaceability and monetary value. An asset is anything of value, including people, information, equipment, facilities and infrastructure. Assets can also extend to more general or intangible items, such as operations, systems, strategic advantage, morale, and reputation. The primary objectives in the effective asset criticality assessment are to identify key assets, determine whether critical functions can be duplicated, and the resources required for duplication and determine priority of response. 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. Civil engineers are part of the assessment team and provide significant input into this process, especially since the assessments also examine reconstitution of infrastructure and base support. Areas encompassing multiple critical assets are referred to as critical areas. AFI 10-245 and AFI 31-101 provide additional detailed information on conducting criticality assessments.

2.3.3. **Vulnerability Assessment.** Terrorists conduct surveillance of US assets to look for weaknesses in FP measures and security procedures that provide opportunities to attack targets at their greatest vulnerability. 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 are implemented to counter them. A vulnerability assessment (VA) is an evaluation of the site to determine if key assets are provided the appropriate level of protection. When a specific threat has been identified higher levels of protection are provided; when a specific threat has not been identified, minimum standards are applied. During the VA, the terrorist threat, including likely tactics, is analyzed to determine what assets are vulnerable to attack by what means. Civil engineers are usually the lead for conducting an annual VA. Local VA team composition depends on the threat, but generally includes a structural or infrastructure engineer, emergency management specialist, and EOD specialist. AFI 10-245 contains guidance on conducting VAs. The Defense Threat Reduction Agency website, located at **http://www.dtra.mil/**, also contains helpful information for conducting VAs.

2.4. 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 FP program and alter the external appearance of FP patterns. Randomly selecting and implementing FPCON measures without a set pattern, either in terms of the measures selected, time, place, or other variables, frustrates surveillance attempts by terrorists. It becomes harder for them to predict certain actions or discern patterns or routines

that may reveal vulnerabilities. RAM also provides training and increases FP awareness for site personnel by varying routine operations. It helps identify which measures the installation's infrastructure is more capable of sustaining and those that unduly stress resources. Other FP 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. Civil engineer operations can increase RAM visibility and effectiveness in confusing enemy surveillance attempts and planning. A list of baseline FPCON measures can be found in AFI 10-245. These measures are exercised regularly and associated plans are adjusted to correct any inadequacies.

Chapter 3

FORCE PROTECTION PLANNING

3.1. Overview. FP planning is conducted throughout all phases of contingencies. Key aspects of FP planning involving civil engineers include site selection and site layout. Expeditionary sites and bases are positioned where they offer commanders the best means for projecting and sustaining air power. But also positioned where the terrain is favorable to engineering, construction, and environmental considerations. When possible, engineers conduct a pre-site survey to learn as much as possible about the deployed location or region (**Figure 3.1**). The survey can be used to develop relationships, perform inventories, and take measurements. A pre-site survey assists in determining the equipment, tools, and materials required to implement protective measures at the deployed location. 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 are familiar with UFCs that address FP and AT standards. This chapter covers civil engineer 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 Pre-Site Survey in Iraq.

3.2. Force Protection Plan. The FP plan consists of specific anti-threat and antiterrorism measures developed to protect personnel, facilities, and critical

assets to include, but not limited to, threat assessments, threat levels, vulnerability assessments, criticality assessments, risk assessments, and FPCON measures. Important factors in planning force protection in deployed environments include the availability of existing facilities, the types of structures in which people live and work, existing natural and manmade features, types and quantities of indigenous construction materials, available real estate, and layout of utilities and other base infrastructure.

3.2.1. The commander typically establishes an Antiterrorism Working Group to develop the base FP plan. Civil engineers on the working group usually focus on the physical security and integrated defense (ID) aspects of the plan. The plan includes elements that contribute to ID 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.

3.2.2. Absolute protection against enemy or terrorist activities is not possible. Therefore, protective plans and procedures are based on the threat identified by intelligence personnel. Considering the threat, protective measures strike a reasonable balance between protection required, mission requirements, available manpower, and available resources.

3.2.3. The FP Plan itself is not an end state. The plan is a living document constantly reviewed and revised as threats, resource requirements, and innovations cause changes in FP tactics. Civil engineers are prepared to offer observations and innovations that counter and mitigate terrorist threats and increase force protection.

3.3. Resource Constraints. Resources needed to implement FP plans include, but not limited to, time, manpower, materials, equipment, and funding. Resources may be committed to FP at any time during threat, vulnerability, or criticality assessments. When applicable, resource commitment may be delayed until all assessments are complete, including risk assessment.

3.3.1. Commanders typically use risk management to allocate resources towards assets most vulnerable to the identified threat and would have the most damaging effect on mission. Although FP is inherently a top priority for all commanders, limited resources under certain circumstances and during some

stages of deployment may cause risks to become unacceptable from a civil engineer perspective.

3.3.2. Civil engineers are persistent in efforts to obtain required resources to implement FP measures required to counter identified threats. Most efforts to obtain FP resources are performed before deploying and reassessed immediately upon arrival at the deployment location.

3.4. Site Selection. Civil engineers participate in the pre-site survey and learn as much as possible about the region. Selecting a site suitable to beddown the expected population, weapon systems, support equipment, and other assets are considered along with the need for standoff.

3.4.1. Expeditionary and temporary structures are typically composed of metal, fabric, or wood frames and rigid walls which generally make them impractical to harden or retrofit. This makes establishing proper standoff distance the primary approach to FP in the expeditionary environment. Unfortunately, this also drives the need for selecting large beddown sites.

3.4.2. Sufficient space for dispersal of certain functions and equipment is planned so that commanders have flexibility to increase beddown population and standoff distances, if required in response to threats.

3.4.3. Upon arrival to the deployed site, develop a list of equipment, tools, and materials needed to immediately implement protective measures.

3.5. Site Layout. Site layout is an extremely important process in FP planning. If site layout is not well thought out, it may be very manpower exhaustive and costly to rearrange assets once they are in place. Site layout is 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.). Key civil engineer planning aspects include standoff distances, orientation of facilities, layout of roads, layering of defense tactics, sidewall protection, facility hardening techniques, dispersal of critical resources, compartmentalization of assets, and locations of physical barriers, entry control points (ECP), observation posts, defensive fighting positions and personnel bunkers. Chapter 4 covers these areas in more detail. Attachment 2 also contains

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. While conducting site selection and site layout functions, use available geographical information system (GIS) tools to enhance survivability efforts and ensure minimum AT standards are met. Every deployment is unique and therefore presents unique challenges. The following paragraphs highlight some important site layout planning factors.

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 flexibility to attain higher levels of protection to counter threats. Maximum standoff distances are defined in UFC 4-010-01. Standoff distances differ for bases and camps with controlled perimeters and those without controlled perimeters. If a controlled perimeter does not exist, standoff distances usually are greater. When recommended standoff distances cannot be achieved, structures are 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 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 may reduce effects from explosive hazards. **Chapter 4** covers this subject in more detail.

3.5.3. **Provide Effective Road Layout.** Although roads are often designed to minimize travel time from one place to another, caution is taken when planning roads. Roads that provide straight line access to key facilities and other critical assets allow a vehicle to gain the speed necessary to breach protective barriers or crash through facilities. Roads are generally designed to limit the maximum speed a vehicle can attain before the driver loses control or draws attention from security personnel. Designing sharp curves or using barriers to create a serpentine layout that force drivers to negotiate a series of sharp turns can limit vehicle approach speed. Vehicle operators attempting to leave the road in order

to gain speed towards a potential target increase the chance of early detection and response. Roads approaching key facilities are made parallel to the facilities versus a perpendicular approach. Barriers, trees, and other obstacles can reduce a driver's ability to leave roads or to have a direct path to the facility from the road.

3.6. Unified Facilities Criteria. This section focuses on UFCs which prescribe FP standards for new, existing, temporary, and expeditionary structures. These publications can be located at the Whole Building Design Guide website at **http://dod.wbdg.org** and may also be downloaded from the US Army Corps of Engineers (USACE) Protective Design Center (PDC) website at **https://pdc.usace.army.mil**.

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. These standards are intended to minimize the possibility of mass casualties in facilities where no known terrorist activity currently exists. Graphic Training Aid (GTA) 90-01-011, *Joint Forward Operations Base (JFOB) Protection Handbook*, provides standards for expeditionary structures where a terrorist threat 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 AOR. Air Forces Central, Air Forces Southern, United States Air Forces in Europe, and Pacific Air Forces have supplemental instructions regarding FP construction standards. Contact the theater-level A4C planner for more information. Refer to UFC 4-020-01 when developing cost estimates for expeditionary construction and where more stringent local standards apply for detailed descriptions of the levels of protection.

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 are 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.) are 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 for expeditionary assets in high-threat environments, 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, can be provided in the immediate proximity of all areas where personnel live and work (**Figure 3.2**).

Figure 3.2. Protective Shelters at a FOB in Afghanistan.

Selecting levels of protection for all key and critical assets involves a tradeoff for acceptable levels of risk. UFC 4-010-01 defines the different standards for new and existing buildings and expeditionary or temporary structures, and contains *qualitative* descriptions of potential damage to buildings and structures at different levels of protection. Detailed *quantitative* descriptions of the levels of protection can be found in UFC 4-020-02FA, *Security Engineering: Concept Design (FOUO).*

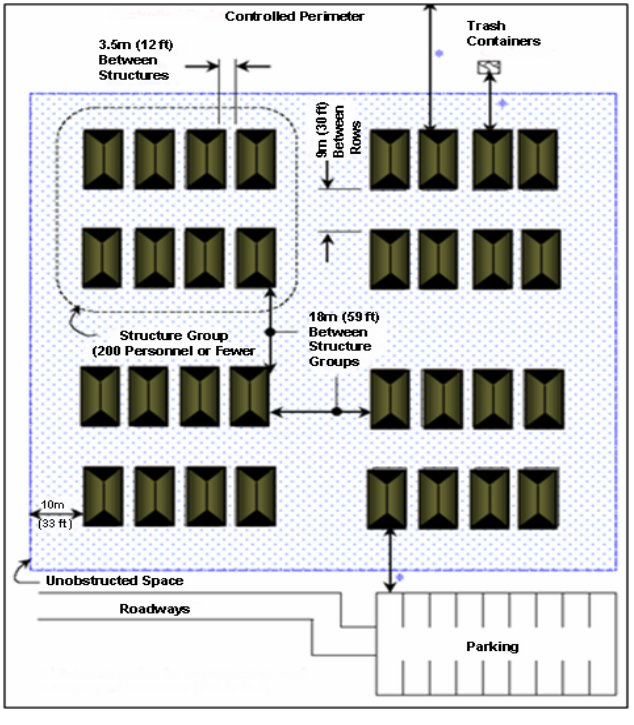
3.6.3. **Standoff Distances.** The primary objective of design and site layout strategy is to keep potential threats as far away from personnel and critical assets

as possible. Due to the type of construction, standoff distances differ for new or existing buildings and expeditionary or temporary structures.

3.6.3.1. **New and Existing Buildings.** Standoff distances for new and existing buildings are defined in Table B-1 and illustrated in Figures B-1 through B-4 of UFC 4-010-01. The standards were developed for a wide range of conventionally constructed buildings. Distances listed under the "Minimum Standoff Distance" column of Table B-1 are provided except where not possible. The UFC further states that lesser standoff distances may be allowed where required level of protection can be shown through analysis or can be achieved through building hardening or other mitigating construction or retrofit. The applicable explosive weights indicated in the table may be obtained from UFC 4-010-02.

3.6.3.2. **Expeditionary and Temporary Structures.** Standoff distances for expeditionary and temporary structures are defined in Table D-1 of UFC 4-010-01 and illustrated in **Figure 3.3** below. These standoff distances were developed for Small and Medium Shelters and Southeast Asia (SEA) Huts. The applicable explosive weights indicated in the UFC table are obtained from UFC 4-010-02. An asterisk "*" in **Figure 3.3** indicates the standoff distance varies by construction and category of construction. An analysis of the structure by an engineer experienced in blast-resistant design is required. Hardening can be applied as necessary to mitigate effects of explosives indicated. If the CCDR determines a higher level of protection than is specified in UFC 4-010-01 is required, based on a known threat and an analysis of vulnerability and criticality assessments, refer to UFC 4-020-01 for methods of achieving higher levels of protection.

Figure 3.3. Standoff Distances and Separation for Expeditionary and Temporary Structures.



Chapter 4

PHYSICAL SECURITY

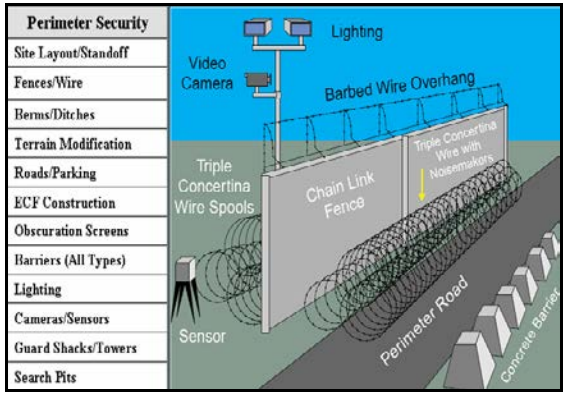
4.1. Overview. A key element of FP is physical security. Physical security programs are designed for prevention and provide the means to counter threats when preventive measures are ignored or bypassed. DOD 5200.08-R, *Physical Security Program*, defines physical security as active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage and criminal activity. This chapter provides guidance and considerations for implementing physical 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 AT 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 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 security measures that provide this early detection capability. Two broad areas of physical security include perimeter security and internal security. This chapter focuses primarily on these two aspects of physical security.

4.3. Perimeter Security. One of the most important FP tasks during the initial stages of deployment and beddown is establishing perimeter security. Working with security forces, civil engineers help establish a continuous physical barrier

which clearly defines the physical limits of the site, to prevent unauthorized access. **Figure 4.1** illustrates key aspects of perimeter security. This involves constructing fences, placing concertina wire, installing perimeter lighting, constructing berms and ditches, placing barriers, and assisting with the installation of security cameras. Also key is ensuring backup power source is available in the event systems requiring power are disrupted by intentional or unintentional damage. In addition, clear zones beyond the perimeter are kept free of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to penetrate perimeter security. Also, secure utility ducts, drainage culverts, concrete trenches, and storm drains originating from outside the perimeter by using screens and grates. Locks can be installed on manhole covers. Intrusion detection sensors may be used along with surveillance equipment to provide greater security. The next few paragraphs discuss how physical security may 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. Refer to UFC 4-022-02, *Selection and Application of Vehicle Barriers*, for design, selection and application of active and passive vehicles barriers.

4.3.1.1. **Barrier Plan.** Developing and implementing a barrier plan is a critical FP function for civil engineers. The barrier plan 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 is usually developed during the various assessments: threat, vulnerability, criticality, and risk assessments. The barrier plan summarizes 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 is appointed, trained, and exercised regularly.

4.3.1.2. **Types of Barriers.** There are many barrier designs that can be used for a variety of purposes (e.g., pedestrians, vehicles, weapons, etc.) and various types of structures and natural features that may be used as barriers (e.g., 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 can 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 may be found in the expeditionary environment (e.g., Bitburg barrier, Jersey barrier, Alaska barrier,

T-barrier, bastions, etc.). Some active barriers commonly found in the expeditionary environment include portable tire shredders 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. Examples include barricades, retractable bollards, beams, gates, and tire shredders. 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 include backup power, emergency cutoff switches, and adequate lighting. **Figure 4.2** through **Figure 4.7** shows examples of active barriers that can be used in the expeditionary environment.

Figure 4.2. Portable Barrier.

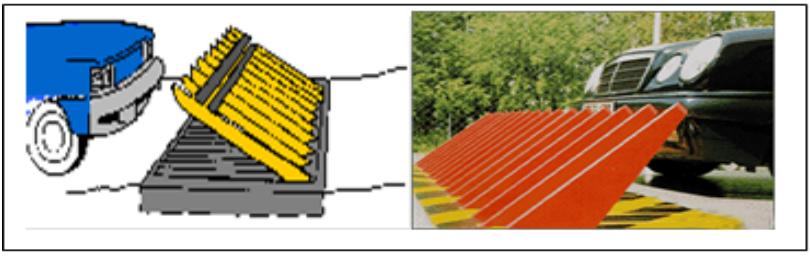


Figure 4.3. Wedge (Drum) Barrier.

Figure 4.4. Retractable Bollards.

Figure 4.5. Lift Plate Barricade System.

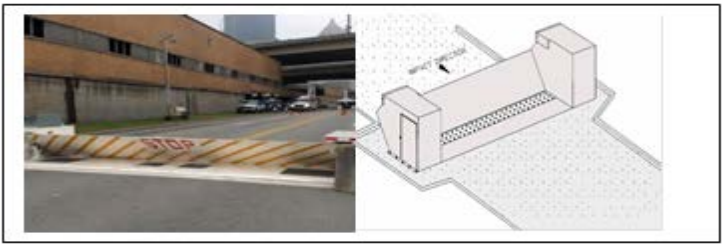


Figure 4.6. Sliding Gate.

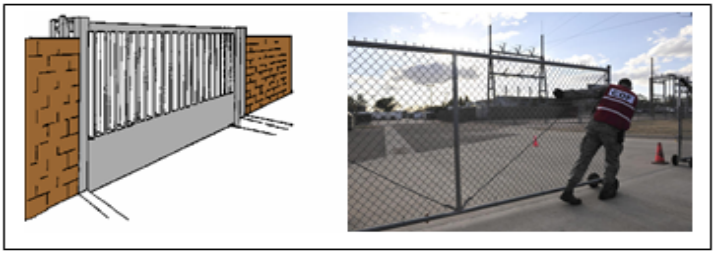
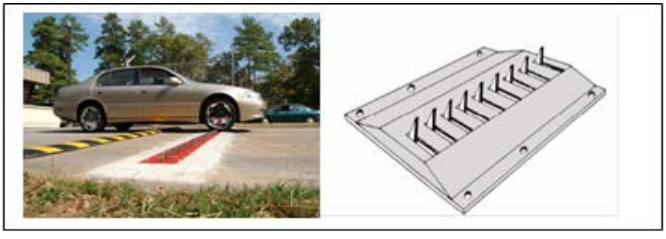


Figure 4.7. Tire Shredder.



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 are 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 4.8** through **Figure 4.13** shows examples of passive barriers that may be used in the expeditionary environment. For additional details on different types of barriers, refer to Air Force Handbook (AFH) 10-222, Volume 14, *Guide to Fighting Positions, Shelters, Obstacles, and Revetments*; and the *JFOB Protection Handbook*. The JFOB handbook may be accessed on the United States Army Central Army Registry (CAR) website. To obtain a copy of the handbook from the CAR website requires a Common Access Card at the following link.

https://rdl.train.army.mil/catalog/go/100.ATSC/0BEF6011-E36F-4F1E-8965-5DB0931D9010-1300684489163.

Figure 4.8. Non-Retractable Bollards.

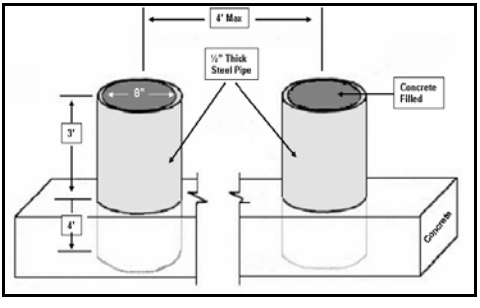


Figure 4.9. Steel Hedgehog Barrier.

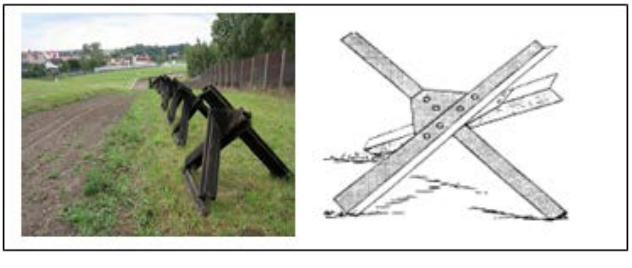


Figure 4.10. Expedient Tire Barrier.

Figure 4.11. Concrete Jersey Barrier.

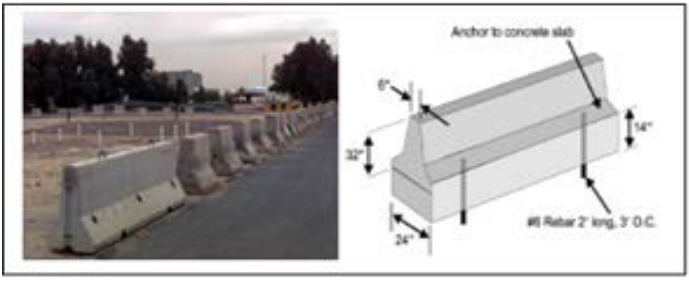


Figure 4.12. Sand Bags.

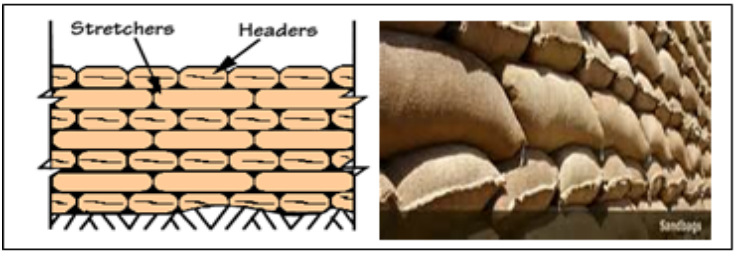


Figure 4.13. Barriers.

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

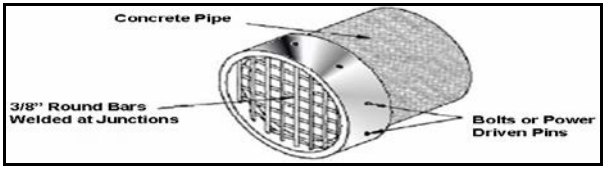
are also used in conjunction with security lighting, IDSs, closed circuit television, and other means of integrating security. Chain link fences are antipersonnel barriers. They are cost-effective, usually readily available, and provide a moderate degree of protection. Chain link fences are more effective if reinforced with cable or topped with outriggers and concertina wire, razor wire, or multiple strands of barbed wire, as shown in **Figure 4.14**. Since most fences can be easily penetrated by a moving vehicle, they are not considered vehicle barriers and can resist impact only if reinforced by barriers capable of absorbing the impact of moving vehicles. For additional details on security fencing, reference Military Handbook (MIL-HDBK)-1013/10, *Design Guidelines for Security Fencing, Gates, Barriers, and Guard Facilities;* and UFC 4-022-03, *Security Fences and Gates*.

Figure 4.14. 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 are minimized. The DOD defines man-passable openings as having a minimum of 96 square inches with the least dimension equal to or greater than 6 inches can be protected by securely fastened, welded bar grilles shown in **Figure 4.15**. AF criteria specify that the minimum opening is 6.4" inches. 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

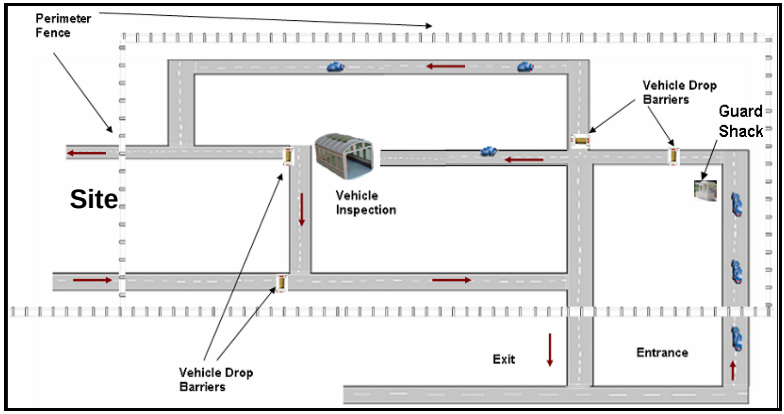
in culverts or other drainage structures, ensure corrective action is taken to compensate for the diminished flow capacity and increased maintenance required. In addition, secure all manhole covers that could be accessed and used to cross the site's perimeter. For detailed information on securing these types of structures, refer to UFC 4-020-03FA, *Security Engineering: Final Design (FOUO)* and AFI 31-101. This document is FOUO and can be downloaded from the USACE's PDC website at **https://pdc.usace.army.mil**.

Figure 4.15. 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. 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 shown in **Figure 4.16**. 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 are based on a threat intelligence assessment.

Figure 4.16. Typical Entry Control Facility.

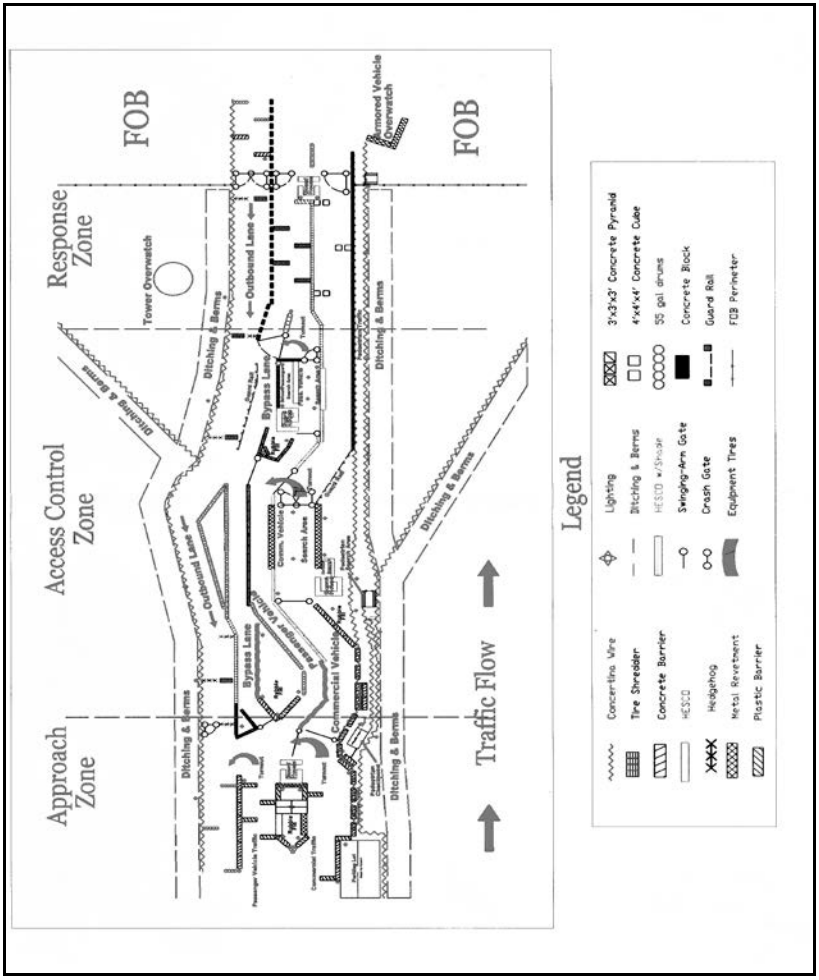


4.3.4.1. **Location.** ECFs are located to provide maximum standoff distance between the ECF and critical facilities and equipment. Minimum standoff distances are outlined in UFCs 4-010-01 and 4-010-02. The CCDR may increase these distances based on the known threat for a particular area. Always refer 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 is subdivided into zones and allow enough queue space to prevent obstructing traffic on main roads by vehicles waiting to enter the site as shown in **Figure 4.17**. 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 sets 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 are channeled through a maze of barriers that force drivers to decrease their rate of speed. Vehicles are

channeled into search pits to allow security personnel to search for and detect explosives. Search pits are separated from local traffic by security fences and vehicle barriers and located outside 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 are 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 4.17. Entry Control Facility Zones.

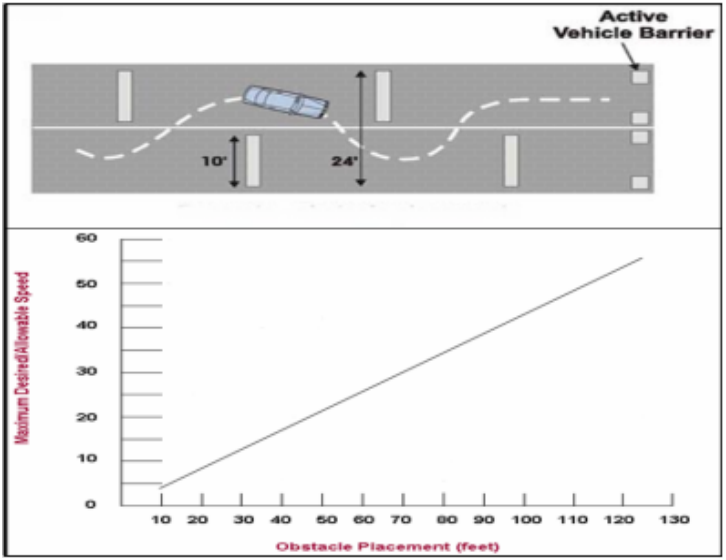


4.3.4.3. **ECF Barriers.** ECF barriers are designed to maintain control. They address the counter-mobility aspect of FP (preventing unauthorized vehicles

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 are strictly controlled. ECF barriers define 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. CE places barriers 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 are anchored to the surface and/or cabled together (**Figure 4.18**) to provide increased resistance to penetration attempts. To slow speeds of approaching vehicles, place barriers in a manner that produces a serpentine path that drivers 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 4.19**. Creating 90-degree turns also forces drivers to reduce speeds. A vehicle leaving these paths draws attention and alerts security personnel of a possible attempt to evade clearance procedures and gain unauthorized access to the site.

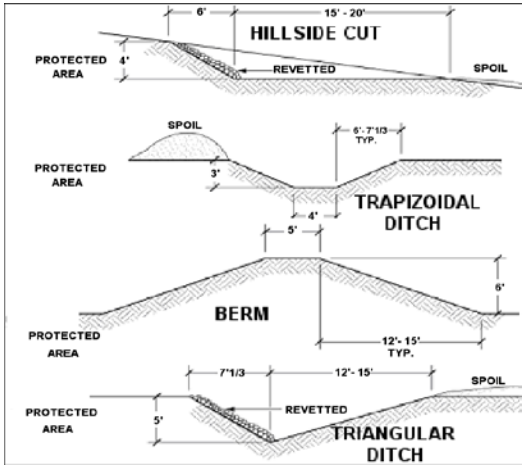
Figure 4.18. Jersey Barriers Cabled Together.

Figure 4.19. 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 as illustrated in **Figure 4.20**. 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 can 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 4.20. Berms and Ditches.



4.3.6. **Lighting and Sensors.** Security lighting allows personnel to observe areas around the perimeter, at ECPs, 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 causes traffic hazards. Different types of terrain and surfaces required to be illuminated can 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 to prevent illuminating a potential target. To be more effective, security lighting may be combined with an intrusion detection system as shown in **Figure 4.21**. 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 4-021-02, *Electronic Security Systems* and AFI 31-101.

Figure 4.21. 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 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 pre-detonation screen, may be used for protection against these types of weapons. Pre-detonation 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 as shown in **Figure 4.22** can also be placed on perimeter fences to block lines of sight into the site. When using obscuration screens, make sure personnel inside the site or facility are still able to see outside and observe any suspicious activities.

Figure 4.22. Obscuration Screen on Perimeter Fence.

4.3.8. **Observation Posts, Guard Towers, and Defensive Fighting Positions.** Civil engineers work closely with security forces personnel in siting and constructing hardened structures to be used for observation, overwatch, and defensive fighting as shown in **Figure 4.23**. 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 are 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. For details on constructing guard towers, observation posts, defensive fighting positions, and bunkers, reference the *JFOB Protection Handbook* referred to earlier and AFH 10-222, Volume 14. Detailed drawings and construction information for these types of structures can also be obtained by contacting the USACE Engineer Research and Development Center at **urocusace@us.army.mil** and requesting the Theater Construction Management System (TCMS) software.

Figure 4.23. Observation Posts, Guard Towers, and Defensive Fighting Positions.

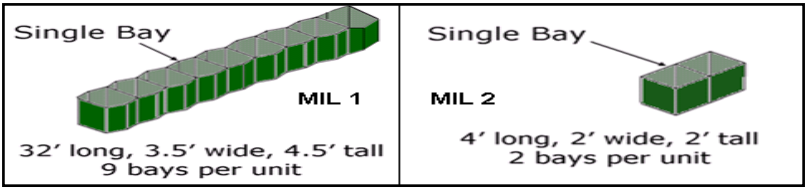
4.3.9. **Barriers.** Earth-filled container barriers (also called bastions) are commonly used in the expeditionary environment to construct various types of structures and sidewall protection. These containers come in various sizes and all have national stock numbers assigned; see **Table 4.1** and **Figure 4.24**.

Table 4.1. Barrier Container Sizes and National Stock Numbers.

UNIT	HEIGHT ft (m)	WIDTH ft (m)	LENGTH ft (m)	NSN
Mil 1 (5442)	4.5ft (1.37m)	3.5ft (1.06m)	32.9ft (10m)	95680-99-835-7866 (Beige) 95680-99-001-9396 (Green)
Mil 2 (2424)	2ft (0.61m)	2ft (0.61m)	4ft (1.22m)	995680-99-68-1764 (Beige) 95680-99-001-9397 (Green)
Mil 3 (3939)	3.25ft (1.0m)	3.25ft (1.0m)	32.9ft (10m)	95680-99-001-9392 (Beige) 95680-99-001-9398 (Green)
Mil 4 (3960)	3.25ft (1.0m)	5ft (1.52m)	32.9ft (10m)	95680-99-001-9393 (Beige) 95680-99-001-9399 (Green)
Mil 5 (2424)	2ft (0.61m)	2ft (0.61m)	10ft (3.05m)	95680-99-001-9394 (Beige) 95680-99-001-9400 (Green)
Mil 6	5.6ft	2ft	10ft	95680-99-001-9395 (Beige)

(6624)	(1.68m)	(0.61m)	(3.05m)	95680-99-001-9401 (Green)
Mil 7 (8784)	7.25ft (2.21m)	7ft (2.13m)	91ft (27.74m)	95680-99-169-0183 (Beige) 95680-99-126-3716 (Green)
Mil 8 (5448)	4.5ft (1.37m)	4ft (1.22m)	32.9ft (10m)	95680-99-335-4902 (Beige) 95680-99-517-3281 (Green)
Mil 9 (3930)	3.25ft (1.0m)	2.5ft (0.76m)	30ft (9.14m)	95680-99-563-5649 (Beige) 95680-99-052-0506 (Green)
Mil 10 (8760)	7.25ft (2.21m)	5ft (1.52m)	100ft (30.50m)	95680-99-391-0852 (Beige) 95680-99-770-0326 (Green)
Mil 11 (4812)	4ft (1.22m)	1ft 0.30m)	4ft (1.22m)	97195-99-867-9131 (Beige) 97195-99-668-0875 (Green)
Mil 12 (8442)	7ft (2.13m)	3.5ft (1.06m)	108ft (33m)	95670-99-974-8891 (Beige) 95670-99-153-1977 (Green)
Mil 19 (10842)	9ft (2.74m)	3.5ft (1.06m)	10.5ft (3.18m)	95670-99-152-1284 (Beige) 95670-99-242-9574 (Green)

Figure 4.24. Illustration of Different Sizes of Barrier Containers.



4.4. Internal Security. The focus on internal security, from a CE perspective, generally involves such tasks as facility hardening, dispersal, compartmentalization, revetment construction, bunker construction, and protection of utilities to name a few (Figure 4.25). 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 are constructed to support ID objectives as covered in Chapter 5. The following are basic concepts and techniques that may be used to provide protection for existing and expeditionary structures. Refer to the *JFOB Protection Handbook* for additional FP construction details and options.

Figure 4.25. 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 (MNS).** MNS provide immediate notification to personnel during emergencies. The system relays information regarding FPCONs, imminent threats, attacks in progress, etc., and directs personnel to take certain response actions (e.g., take cover, evacuate, etc.). Civil engineers, especially Fire Emergency Services and EM, work closely with security and communications personnel to install and maintain a MNS with primary and backup power. Details on MNS 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, shown in **Figure 4.26**.This system is generally not suitable for notifying personnel working or residing in permanent structures since the voice messages may be unintelligible. In these instances, civil engineers work with security and communications personnel to develop alternative ways of providing mass notification.

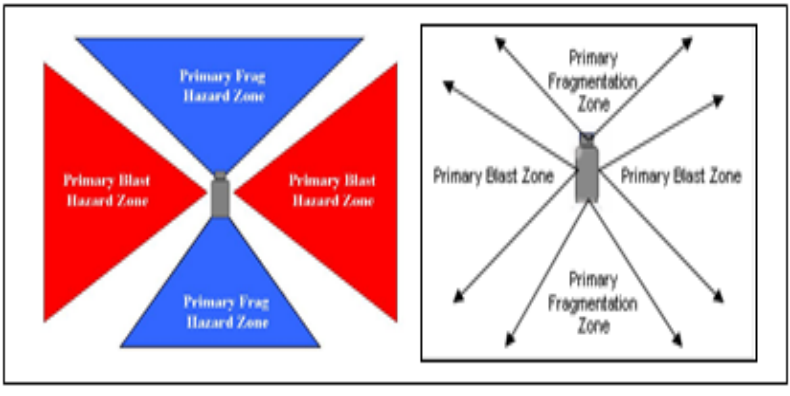
Figure 4.26. Mass Notification System.

4.4.2. **Facilities.** Achieving appropriate levels of protection for facilities most commonly used in the expeditionary environment, such as Small Shelter Systems as shown in **Figure 4.2**7 can be very difficult. This is why standoff is particularly important in expeditionary environments. Personnel may be abnormally 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, civil engineers may need to apply the standards outlined in UFC 4-010-01 for new and existing buildings. 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 may be found in UFC 4-020-01. Also refer to AFH 10-2401, *Vehicle Bomb Mitigation Guide (VBMG) (FOUO)*, for recommendations on increasing protection against vehicle bombs. Both publications may be accessed on 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 may be used in conjunction with standoff distances to mitigate effects of blast/fragmentation on facilities in the expeditionary environment.

Figure 4.27. Expeditionary Structures.

4.4.2.1. **Orientation.** Buildings and structures may be oriented in a manner to help reduce effects of blast on the structure. Tests have shown that structures oriented with the smaller dimension of the structure facing the direction of an anticipated blast (e.g., perimeter fence, ECP, etc.) receive less damage than with the larger dimension 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, as shown in **Figure 4.28**. For more details on vehicle bombs and their effects on all types of structures, including expeditionary structures, refer to AFH 10-2401. That handbook also provides safe standoff distances to defeat and mitigate the effects of vehicle bombs. This information may be used to determine how best to orient facilities during site setup. If possible, doors and windows are 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.

Figure 4.28. Blast and Fragmentation Hazard Zones.

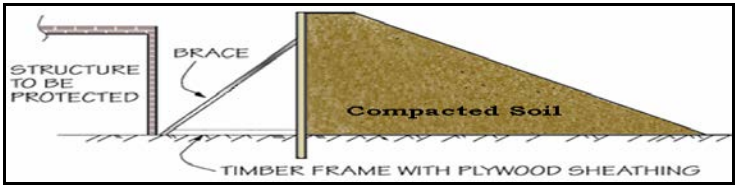


4.4.2.2. **Clustering and Dispersal.** Making the determination to cluster or disperse assets can be based on several factors. Because each tactic has both positive and negative aspects, the planner strikes a careful balance between efficiency and survivability, with emphasis on survivability. Grouping high-risk

activities and concentrating personnel and critical functions in a cluster may 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. Dispersal is a form of passive defense that may be used to lessen the possibility of numerous critical assets being 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 may have an isolating effect that reduces effectiveness of existing security provisions, increases complexity of emergency response, and creates more space to defend. The tradeoff between dispersing assets (past the minimum standoff distance) and grouping them is analyzed. This is a risk management decision made by the site commander using 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 priority assets are located, CE provides physical protection based on the threat. Reference AFH 10-222, Volume 1, *Civil Engineer Bare Base Development*, for additional information on facility dispersal options.

4.4.2.3. **Hardening.** Hardening temporary and expeditionary structures can be difficult or impractical because these structures are designed to be mobile. These structures offer limited protection from threats when compared to permanent facilities. Some degree of protection may be achieved by hardening the structures perimeter. **Figure 4.29** is an example of a compacted soil berm used to protect a structure. Other earth-filled barriers such as concertainer walls and sandbags may also be employed to protect 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 may be effective in stopping primary debris. 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 may be used to harden facilities and other assets.

Figure 4.29. Compacted Soil Revetment.

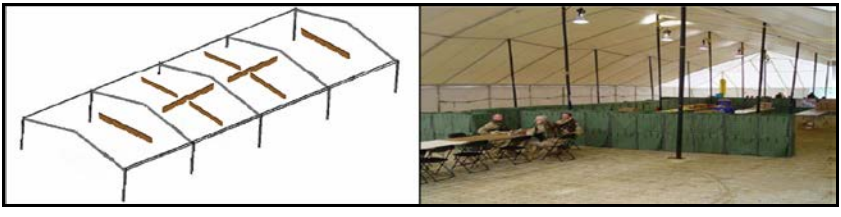


4.4.2.4. **Windows.** Windows are usually the weakest part of a structure. Glass fragments caused by blasts may result in significant injuries. Although expeditionary structures usually do not contain glass windows, host-nation facilities occupied by US forces may in fact contain glass windows. When possible, windows can be covered using plywood or other protective material. If not possible, other methods may be used to reduce hazards from broken glass. Installation of fragment-retention film (**Figure 4.30)** is a plastic (polyester) sheet of film adhered to the glass with special adhesive. This modification helps keep glass fragments together preventing them from causing severe injury and possibly death. Heavy drapes or a "catcher bar" (metal bar installed across the window) may help prevent 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. A trained engineer analyzes several 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) to determine if windows can be properly retrofitted. Protective film in the expeditionary environment is a last resort. As stated earlier, it is preferable to cover windows with plywood or other protective material.

Figure 4.30. Fragmentation Retention Film.

4.4.2.5. **Compartmentalization.** Compartmentalization (**Figure 4.31**) is a technique used to reduce casualties in highly populated facilities, such as dining and recreation facilities. It involves a series of interconnected walls designed to divide large areas into smaller protected areas to limit casualties from impacts of rockets, artillery, and mortars. 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. Tests and analyses have also shown that significant blast hazard do not generally extend beyond the compartment in which the weapon detonates. In addition to compartmentalization, fragmentation barriers are constructed around the facility's exterior to mitigate blast and fragmentation from near misses. The minimum height for interior walls and exterior walls is 5 feet and 8 feet, respectively.

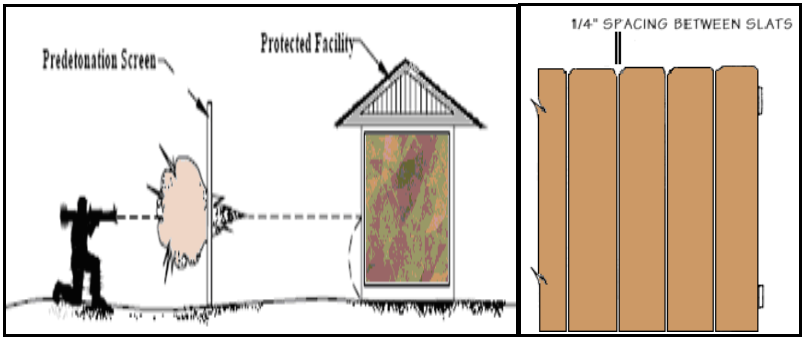
Figure 4.31. Example of Compartmentalization.



4.4.2.6. **Pre-detonation Screens.** Pre-detonation screens are structures built and placed in front of assets to cause anti-tank rounds to detonate before reaching its intended target (**Figure 4.32**). Pre-detonation screens may consist of wood

fences, chain-link fencing, expanded metal mesh, or heavy woven-fiber fabric. Wood fences may be constructed of wood slats or plywood panels a minimum of 3/8-inch (9.4 mm) thick. If made of slats, spacing is no more than 0.25-inch (6.4 mm) apart. Spaces in metal fabric screens are 2 inches (50 mm) by 2 inches (50 mm) maximum and fabric a minimum of 9 gauge (3.8 mm). A direct fire weapon striking a pre-detonation screen either detonates on impact or is dudded. The residual effects of a pre-detonated round on a building are more severe than the effects of a dudded round. After pre-detonation, the weapon's jet and the spent rocket engine from the rocket-propelled grenade continue past the screen. The screen is 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 4-020-03FA for details on construction and standoff distances for pre-detonation screens.

Figure 4.32. Pre-Detonation Screening.



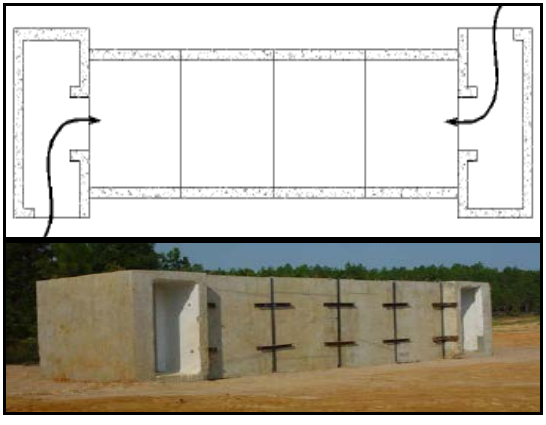
4.4.3. **Revetments.** Revetments are simply walls used to reduce the effects of blast or fragmentation on facilities and equipment resulting from near miss rockets, artillery, and mortars. They are used to protect parked aircraft or other high-value resources. These structures are also referred to as fragmentation or blast walls. Revetments may be constructed of different materials and configured in multiple ways for multiple purposes as shown in **Figure 4.33**. Engineers identify revetment requirements through their servicing logistics function and theater CE staff. Refer to AFH 10-222, Volume 14 for construction

details and an overview of the different types of revetments. The *JFOB Protection Handbook* also contains revetment information.

Figure 4.33. Revetments.

4.4.4. **Personnel Protective Shelters.** In the event of an attack or when attacks are imminent, personnel quickly evacuate expeditionary-type structures. Hardened protective shelters (bunkers) with overhead protection (**Figure 4.34**) are constructed strategically throughout the site, particularly near primary gathering buildings and where large numbers of personnel live and work. Shelters provide protection against direct and indirect weapons fire. Sidewall barriers may be constructed using sandbags, earth-filled container structures, earth-filled wire mesh bastions, or concrete walls. Sidewalls need to be thick enough to resist direct fire weapons or a near miss from an indirect fire weapon. Covers are made capable of supporting the dead weight from sandbags or earth-filled containers. Only bunker designs approved by the USACE's Engineer Research Development Center are constructed. Pre-detonation screens can also be placed above the shelter to cause a weapon to detonate upon impact, thereby reducing the effects upon the bunker. Detailed information on personnel protective shelters can be found in the *JFOB Protection Handbook*; AFH 10-222, Volume 14; the USACE's website; and the TCMS software.

Figure 4.34. Personnel Protective Shelter.



4.4.5. **Utilities.** Vulnerability assessments usually assess the potential for aggressors to damage, destroy, or tamper with site utilities, particularly at those sites where utility lines cross the site perimeter. In addition to screening, sealing, and securing utility lines to prevent unauthorized access engineers 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 (**Figure 4.35**) are one of the most critical assets in the expeditionary environment. Protect power plant resources with revetments, barriers, concertina or barbed wire (entanglements), camouflage, and berming. Depending upon 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 redundancy after an attack. Also, power distribution cables are 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 4.35. Expeditionary Power Plant at Camp Victory, Iraq.

4.4.5.2. **Water Production and Supply.** Water sources, water purification and distribution equipment, and water supplies are kept under constant surveillance and tested frequently for contamination. Water transfer pipes may be tapped under pressure providing aggressors the opportunity to introduce contaminants into the water supply. Civil engineers work closely with Bioenvironmental Engineering, Public Health, and Safety personnel to ensure water supplies are protected from intentional or unintentional contamination. Water sources are guarded, water production equipment reveted, and water lines buried at the first opportunity (**Figure 4.36**). Roving patrols establish surveillance points to alert personnel to the possibility of tampering. An emergency response plan is developed in the event the water supply is contaminated. The plan includes a map indicating the location of all potential water sources, water production equipment, water storage areas, and alternative approaches to supplying safe water (e.g., boiling, special treatment, alternative water supply points, procedures for having bottled water brought in from other sources, etc.). For further specific guidance on CE responsibilities related to FP of water sources and establishing and maintaining a potable water production capability refer to AFMAN 10-246, *Food and Water Protection Program*; Air Force Pamphlet (AFPAM) 10-219, Volume 5, *Bare Base Conceptual Planning*; and AFMAN 48-138_IP, *Sanitary Control and Surveillance of Field Water Supplies*.

Figure 4.36. Burying Utility Lines.

4.4.6. **Camouflage and Concealment.** Camouflage and concealment are tactics used to enhance FP. Use whatever natural or artificial materials are 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, need 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 as shown in **Figure 4.37**. 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 are used after hardening and cover are applied to the assets to be protected. Refer to AFH 10-222, Volume 10, *Civil Engineer Camouflage, Concealment, and Deception Measure*s, for more information.

Figure 4.37. Camouflage Netting Being Applied.

4.4.7. **Contract Support.** Once hostilities subside and initial beddown phase moves towards sustainment, contract support is available to implement and sustain base support operations (**Figure 4.38**). 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 CE and services capabilities during worldwide contingency planning and deployment operations. AFCAP may provide construction support at overseas locations and can support recovery operations after natural disasters, accidents, or terrorist attacks. The Navy's Global Contingency Construction and Global Contingency Services 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, Logistics Contract Augmentation Program or LOGCAP, 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 Major Command Civil Engineer or Air Force Civil Engineer Center for contract support assistance.

Figure 4.38. LOGCAP Power Support at Camp Taji, Iraq.

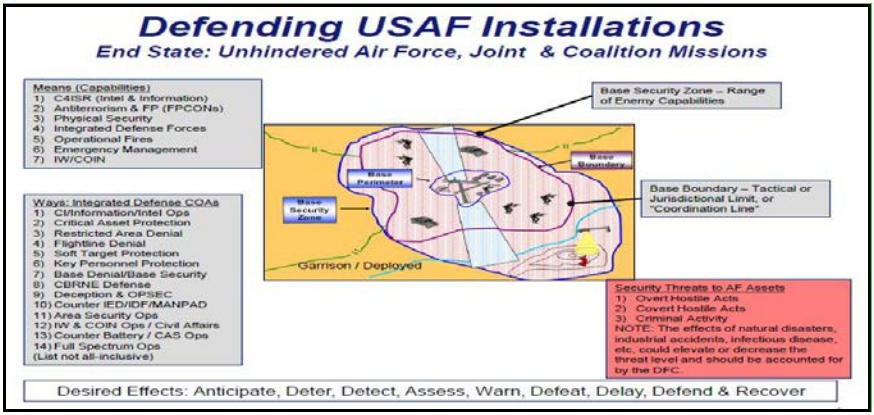
Chapter 5

INTEGRATED DEFENSE

5.1. Overview. Integrated Defense (ID) is the integration of active and passive, offensive and defensive capabilities, to mitigate potential risks and defeat adversary threats to AF operations. ID employs a number of capabilities in a variety of ways to produce desired effects in the base defense battle space. This includes the base boundary, base security zone, and the base perimeter. This strategy leverages assigned resources against adaptive threats to protect resources and personnel. This chapter outlines actions civil engineers take to support effective application of the ID concept.

5.2. Integrated Defense Concept. One of the most vital capabilities a base has to counter threats, especially in an expeditionary environment, is the ability to apply an ID concept (Figure 5.1). Civil engineers are trained to be familiar with the FP terminology that describes the defense battlespace of the base, both inside *and* outside the wire. AFH 31-109, *Integrated Defense in Expeditionary Environments*, describes the base perimeter as basically the fenced area of the base. It shows the physical and legal demarcation of the installation, that only authorized personnel may occupy, and is usually made obvious to the general public so inadvertent penetration is avoided. The base boundary (BB) is the line that delineates the surface area of the base for the purpose of facilitating coordination and deconfliction of operations between adjacent (and usually friendly) units. It includes key terrain that is secured through active control by security forces or coordination with host nation forces. The base security zone (BSZ) is an AF unique term used to describe the area outside the base perimeter from which base personnel, resources, or aircraft approaching/departing the base may be vulnerable to standoff threats (e.g. mortars, rockets, and man portable aerial defense systems).

Figure 5.1. AF Integrated Defense Concept.



5.2.1. **Actions and Effects.** Essential actions and effects of the ID concept are those deemed critical to successful planning, programing, and combat support operations execution. Successful ID effects depend on the prevailing threat, the operating environment, friendly forces available, rules of engagement, and other factors that characterize the battlespace. ID is planned and executed based upon the estimated threat (or combination of threats) and operating environment, and is approved by the Installation Commander.

5.2.2. **Integrated Defense Risk Management Process (IDRMP).** The analytical tool used to achieve ID is the IDRMP, for the Installation Commander to manage risks based upon the association of the criticality of assigned assets and infrastructure, a comprehensive analysis of the threat and the respective vulnerabilities to those assets. ID is employed at all garrisons and expeditionary locations.

5.3. Desired ID Effects. Conducting ID is accomplished by achieving nine desired effects. These effects are: anticipate, deter, detect, assess, warn, defeat, delay, defend, and recover from threats or hostile actions to resources. ID measures ensure that unauthorized access to resources is denied before their seizure, loss, damage or destruction. AFI 31-101, defines the desired ID effects toolkit.

5.3.1. **Anticipation.** Anticipating the enemy is the critical first step Anticipation involves determining options, intentions, and actions an adversary might take, to intelligently prepare the operational environment in order 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.

5.3.2. **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 shown in **Table 5.2** to make adversaries understand that a successful attack is unlikely.

Table 5.1. Threat Deterrence.

Base Boundary and Base Security Zone
Deter threat activity through active community policing (e.g., Eagle Eyes Program), boundary and internal circulation control, controlled area marking, prudent physical security measures.
Installation Perimeters
Deter threats by presenting a strong, professional, perceptively impenetrable physical boundary free of foliage or objects (e.g., trees) that might allow surreptitious access.
Installation Entry Control Points
Deter threats by presenting predictably stringent screening TTP and unpredictable searches of vehicles/persons entering installations.
Physical Security Requirements
Deter threat actions through the use of warning signs, barriers, fencing; make the threat’s goal too costly and risky.

5.3.3. **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, see **Table 5.2**. 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.

Table 5.2. Threat Detection.

Base Boundary and Base Security Zone
Detect threats through the use of lighting, IDS, early warning systems (EWS), closed-circuit television, etc.
Installation Perimeters
Detect threats' attempts to exploit perimeters by establishing well-lit, sufficiently observed physical boundaries. Thorough discussion of detection is in AFH 31-109.
Installation Entry Control Points
Detect threats by proper ID vetting, vehicle searches, and sentries' cognizance for threat surveillance.
Physical Security Requirements
Detect threats in time to respond appropriately through use of lighting, IDS, EWS, vegetation control (clear zones), physical security checks, host nation/exterior community networking, robust Eagle Eyes Program integration, listening posts, observation posts, internal circulation controls, RAMs, etc.

5.3.4. **Assessment.** As stated in **Chapter 2**, an assessment of the critical assets, threat and vulnerability is conducted to calculate the overall risk (risk assessment) to determine how best to employ defensive measures. These assessments are conducted by a group of subject matter experts (SME), such as the local Threat Working Group (TWG). This assessment helps develop strategies leveraging finite resources against adaptive threats to protect assets. Otherwise, time and material could be wasted in an effort to provide total protection for every asset, which is not practical.

5.3.5. **Warn.** Warn friendly forces of adversary activity primarily through the IDS and EWS. Additional systems such as mass notification, radio, public address, commander's access channels, voice, hand and arm signals, cellular telephones, instant messenger, short message system texting, etc., also provide warning.

5.3.6. **Defeat.** Defeat threats through appropriate, timely, progressive application of force; using a layered application of barriers, obstacles, technology, physical security measures and forces (defense-in-depth). Integration of steel cabling or other barriers; reinforce physical boundaries which aides defeating penetrative VBIED threats. Additional defeat techniques are discussed in AFH 31-109.

5.3.7. **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 ID. The obstacles and elements of security are employed in layers, forcing the adversary to breach several layers of defense (active and passive) to reach a certain target as shown in **Table 5.3**. 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 the appropriate level of force up to and including 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**.

Table 5.3. Threat Delay.

Base Boundary and Base Security Zone
Delay adversaries using a layers application of barriers, obstacles, technology, physical security measures, and forces (defense-in-depth).
Installation Perimeters
Delay threats in order to increase likelihood of detection and allow friendly forces to respond as needed. Delaying techniques are further discussed in AFH 31-109.

Installation Entry Control Points
Delay adversaries until additional friendly forces can be massed to defeat them.
Physical Security Requirements
Delay the threat's access to facilities, assets, and areas through the use of fencing, barriers, locks, and hasps.

5.3.8. **Defend.** Defend assets through threat-and effects-based planning and analysis that integrate all friendly forces into a single, comprehensive plan. Integrate all friendly forces into the defense plan and ensure all personnel are trained and qualified on arming, rules of engagement, use of force, and expeditionary skills. Perimeter defense is critical to defending the installation by integrating with other perimeter defense forces.

5.3.9. **Recover.** After an enemy withdraws or has been defeated recovery from adversarial events is applied through effective command and control, and executing the installation emergency management plan 10-2. The installation commander directs consolidation and reorganization actions to include reestablishing security and communication; providing first aid and medical evacuation of wounded; damaged obstacle repair; and redistribution of supplies and materials.

JOHN B. COOPER, Lt Gen, USAF
DCS/Logistics, Engineering & Force Protection

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFDA 3-10, *Force Protection*, 13 August 2014

AFDA 3-34, *Engineer Operations*, 30 Dec 2014

AFI 10-210, *Prime Base Engineer Emergency Force (BEEF) Program*, 21 January 2015

AFI 10-245, *Antiterrorism (AT)*, 25 June 2015

AFI 10-2501, *Air Force Emergency Management (EM) Program Planning and Operations*, 24 January 2007 (Incorporating Change 3, 29 April 2013)

AFMAN 10-246, *Food and Water Protection Program*, 27 May 2014

AFMAN 33-363, *Management of Records*, 1 March 2008

AFMAN 48-138_IP, *Sanitary Control and Surveillance of Field Water Supplies*, 1 May 2010

AFPAM 10-219, Volume 5, *Bare Base Conceptual Planning*, 30 March 2012

AFH 10-222, Volume 1, *Civil Engineer Bare Base Development*, 23 January 2012

AFH 10-222, Volume 5, *Guide to Contingency Electrical Power System Installation*, 1 July 2008

AFH 10-222, Volume 10, *Civil Engineer Camouflage, Concealment, and Deception Measures*, 18 February 2011

AFH 10-222, Volume 14, *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 1 August 2008

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

AFH 31-109, *Integrated Defense in Expeditionary Environments*, 1 May 2013

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

JP 1-02, *DOD Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 November 2015)

JP 3-0, *Joint Operations*, 11 August 2011

JP 3-07.2 (FOUO), *Antiterrorism*, 14 March 2014

JP 3-10, *Joint Security Operations in Theater*, 13 November 2014

Joint Force Operations Base (JFOB) Protection Handbook, Sixth Edition, October 2011

UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings*, 9 February 2012, (Change 1, 1 October 2013)

UFC 4-010-02 (FOUO), *DOD Minimum Antiterrorism Standoff Distances for Buildings*, 9 February 2012

UFC 4-020-01, *DOD Security Engineering Facilities Planning Manual*, 11 September 2008

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

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

UFC 4-021-01, *Design and O&M: Mass Notification Systems*, 9 April 2008, (Change 1, January 2010)

UFC 4-021-02, *Electronic Security Systems*, 1 October 2013

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*, 8 June 2009 (Change 1, 9 August 2010)

UFC 4-022-03, *Security Fences and Gates*, 1 October 2013

DOD 5200.08-R, *Physical Security Program*, 9 April 2007 (Incorporating Change 1, 27 May 2009)

Prescribed Forms **-** None

Adopted Forms – None

Abbreviations and Acronyms

AF—Air Force
AFCAP—Air Force Contract Augmentation Program
AFCEC—Air Force Civil Engineer Center
AFDA—Air Force Doctrine Annex
AFH—Air Force Handbook
AFI—Air Force Instruction
AFIMS—Air Force Incident Management System
AFMAN—Air Force Manual
AFOSI—Air Force Office of Special Investigations
AFPAM—Air Force Pamphlet
AFPD—Air Force Policy Directive
AFRIMS—Air Force Records Information Management System
AOR—Area of Responsibility
AT—Antiterrorism
ATO—Antiterrorism Officer
ATR—Antiterrorism Representative
CARM—Critical Asset Risk Management Program
CBRNE—Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives
CCDR—Combatant Commander
CCMD—Combatant Command
CE—Civil Engineer
CIP—Critical Infrastructure Program
DBT—Design Basis Threat
DIA—Defense Intelligence Agency
DOD—Department of Defense

DODD—Department of Defense Directive
DODI—Department of Defense Instruction
ECF—Entry Control Facility
ECP—Entry Control Point
EM—Emergency Management
ETL—Engineering Technical Letter
EWS—Early Warning System
FOUO—For Official Use Only
FP—Force Protection
FPCON—Force Protection Condition
GIS—Geographic Information Systems
IAW—In Accordance With
ID—Integrated Defense
IDRMP—Integrated Defense Risk Management Process
IDS—Intrusion Detection System
IED—Improvised Explosive Devices
IESNA—Illuminating Engineering Society of North America
JP—Joint Publication
MIL-HDBK—Military Handbook
MNS—Mass Notification System
OPR—Office of Primary Responsibility
OPSEC—Operations Security
PDC—Protective Design Center
Prime BEEF—Prime Base Engineer Emergency Force
RAM—Random Antiterrorism Measures
RDS—Records Disposition Schedule
SEA Hut—Southeast Asia Hut
TCMS—Theater Construction Management System
TR—Technical Report
TTP—Tactics, Techniques, and Procedures

UFC—Unified Facilities Criteria

US—United States

USACE—United States Army Corps of Engineers

USAMC—United States Army Materiel Command

VA—Vulnerability Assessment

VBIED—Vehicle-borne Improvised Explosive Device

Terms

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

Antiterrorism—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces. Also called **AT.** See also **counterterrorism; terrorism.** (JP 3-07.2)

Area of Responsibility—The geographical area associated with a Combatant Command within which a geographic combatant commander has authority to plan and conduct operations. Also called the **AOR**. (JP 1-02)

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.

Combatant Commander—A commander of one of the unified or specified combatant commands established by the President. Also called CCDR.

Combating Terrorism (CbT)—Combating terrorism within the DOD encompasses all actions, including AT, counterterrorism, terrorism consequence management (preparation for and response to the consequences of a terrorist incident or event) and terrorism intelligence support (collection and

dissemination of terrorism-related information), taken to oppose terrorism throughout the entire threat spectrum, including terrorist use of CBRNE. (AFI 10-245)

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, foreign persons, or international terrorist activities. Also called **CI**. See also **counterespionage; security.** (JP 1-02)

Criticality Assessment—An assessment of the effect of temporary or permanent loss of key assets or infrastructures on the installation or a unit‘s ability to perform its mission. The assessment also examines costs of recovery and reconstitution including time, funds, capability and infrastructure support. (AFI 10-245)

Design Basis Threat (DBT)—The threat against which buildings and other structures must be protected and upon which the protective system’s design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT includes the aggressor’s tactics and the associated tools, weapons, and explosives employed in these tactics.

Deterrence—The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (JP 3-0, *Joint Operations*). 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. (AFI 10-245)

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

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, International Organization of Standards, and Container Express containers.

Force Protection (FP)—Preventive measures taken to prevent or mitigate hostile actions against DOD personnel (to include family members), resources, facilities and critical information. Also called **FP.** See also **force; force protection condition; protection.** (JP 1-02). **Note:** Because terminology is always evolving, the Air Force believes a more precise definition is: [*An integrated application of offensive and defensive actions that deter, detect, preempt, mitigate or negate threats against Air Force air and space operations and assets, based upon an acceptable level of risk*.] (AFDA 3-10) {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

Force Protection Conditions (FPCONs)—A Chairman of the Joint Chiefs of Staff-approved standard for identification of and recommended responses to terrorist threats against US personnel and facilities. Also called **FPCON.** See also **antiterrorism; force protection.** (JP 3-07.2). A DOD-approved system standardizing the Department's identification, recommended preventive actions and responses to terrorist threats against U.S. personnel and facilities. This system is the principal means for a commander to apply an operational decision on how to protect against terrorism. It facilitates inter-Service coordination and support for AT activities. (AFI 10-245)

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)—A device placed or 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 normally devised from nonmilitary components. Also called **IED.** (JP 1-02)

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. (UFC 4-010-01)

Integrated Defense—The integration of multidisciplinary active and passive, offensive and defensive capabilities, employed to mitigate potential risks and defeat adversary threats to AF operations. (AFI 31-101)

Intelligence—1.) The product resulting from the collection, processing, integration, evaluation, analysis and interpretation of available information concerning foreign countries or areas. 2). The information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (AFI 10-245 & AFI 31-101)

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.

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. See also **active defense.** (JP 1-02)

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. (JP 3-0)

Pre-detonation 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.

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 to 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. Also called **RM.** See also **risk.** (JP 3-0)

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

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, International Organization for Standardization, and Container Express containers, pre-engineered buildings, trailers, stress-tensioned shelters, Expandable Shelter Containers, and Aircraft Hangars (ACH).

Terrorism—The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political. See also **antiterrorism; combating terrorism; counterterrorism; force protection condition.** (JP 3-07.2). The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate

governments or societies in the pursuit of goals that are generally political, religious, or ideological. (AFI 10-245)

Terrorist—An individual who commits an act or acts of violence or threatens violence in pursuit of political, religious, or ideological objectives. (AFI 10-245)

Terrorism Threat Level (TTL)—An intelligence threat assessment of the level of terrorist threat faced by U.S. personnel and interests. The assessment is based on a continuous intelligence analysis of a minimum of four elements: terrorist group operational capability, intentions, activity and operational environment. There are four threat levels: LOW, MODERATE, SIGNIFICANT and HIGH. Threat levels must not be confused with FPCONs. Threat-level assessments are provided to senior leaders to assist them in determining the appropriate local FPCON. (AFI 10-245)

Terrorist Group—Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives. (AFI 10-245)

Terrorist Threat Level—A DOD intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country; the levels are expressed as **LOW**, **MODERATE**, **SIGNIFICANT**, and **HIGH**. (JP 3-07.2)

Threat Assessment—In antiterrorism, examining the capabilities, intentions, and activities, past and present, of terrorist organizations as well as the security environment within which friendly forces operate to determine the level of threat. Also called TA. (JP 3-07.2)

Vulnerability—1. 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. (JP 1-02) In AT, a situation or circumstance which, if left unchanged, may result in the loss of life or damage to mission-essential resources. It includes the characteristics of an installation, system, asset, application, or its dependencies that could cause it to suffer a degradation or loss (incapacity to perform its designated function) as a result of having been subjected to a certain level of threat or hazard. (AFI 10-245)

Vulnerability Assessment—A DOD, command, or unit-level evaluation (assessment) to determine the vulnerability of an installation, unit, exercise, port, ship, residence, facility, or other site to a terrorist attack. Identifies areas of

improvement to withstand, mitigate, or deter acts of violence or terrorism. **Also called VA.** (JP 3-07.2)

Attachment 2

SITE SELECTION AND LAYOUT CONSIDERATIONS

A2.1. 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 can be developed and used during the site selection process. Keep the following force protection considerations in mind when selecting beddown sites:

A2.1.1. Consider the threat throughout the entire site selection process.

A2.1.2. Consider minimum AT standards established by DOD and whether the site supports or inhibits efforts to attain and maintain AT standards.

A2.1.3. Consider force protection standards established by the CCDR and whether the site supports or inhibits efforts to attain and maintain these standards.

A2.1.4. Select a site that provides the opportunity to maximize standoff distances.

A2.1.5. Select beddown areas that are away from public roads and uncontrolled areas.

A2.1.6. Avoid areas where terrain features provide adversaries with too many vantage points.

A2.1.7. Avoid areas that do not provide sufficient standoff distances.

A2.1.8. Consider future need for additional space to support a population increase.

A2.1.9. Consider future need to increase standoff distances as a result of increased threat levels.

A2.1.10. 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.).

A2.1.11. Consider the need to establish a defense-in-depth posture for integrated base defense.

A2.1.12. Consider adjacent land use and direct lines of sight or access to the site.

A2.1.13. Consider the need to modify terrain outside the established perimeter to provide clear zones and eliminate potential hiding places.

A2.1.14. Consider support needed from the local area (i.e., utilities, sanitation, indigenous materials, equipment, etc.) and how this impacts force protection efforts.

A2.1.15. Consider site elevation to deny advantage for potential aggressors (i.e., lines of sight, targeting opportunities, etc.).

A2.1.16. Consider retrofits of existing facilities to meet minimum local AT standards.

A2.1.17. Evaluate potential use of existing roads to enhance FP efforts.

A2.1.18. Consider the need to establish separate ECPs for delivery vehicles.

A2.1.19. Consider the need for vehicle queue space and search pits.

A2.1.20. Consider the need to disperse key facilities and critical assets.

A2.1.21. Select a site that lends itself to establishing an effective controlled perimeter.

A2.1.22. Consider the need to bury utility lines.

A2.1.23. Consider the need to orient facilities to avoid direct line of sight from the perimeter.

A2.1.24. Consider the need to position high-value facilities and assets near the center of the site.

A2.2. Site Layout. Key elements to consider during site layout include standoff distances, layered security, number and location of 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. Also consider the following elements during site layout.

A2.2.1. Use the threat assessment when determining how best to site facilities in relation to existing roads and the controlled perimeter.

A2.2.2. Consider minimum AT standards established by DOD when siting facilities and critical assets.

A2.2.3. Consider force protection standards established by CCDRs when siting facilities and critical assets.

A2.2.4. Maximize standoff distance between the controlled perimeter and inhabited buildings and other key assets.

A2.2.5. Limit ECPs to an absolute minimum, and establish a separate entry control points for trucks and delivery vehicles at an appreciable standoff distance from inhabited facilities and other key assets.

A2.2.6. Consider terrain, elevation, and available space when siting 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.2.2.7. Clear dense vegetation around the perimeter that may be used by adversaries to camouflage or conceal themselves while conducting surveillance, attempting to gain access to the site, or targeting priority assets.

A2.2.8. Avoid straight-line roads or roads that are perpendicular to critical facilities or assets.

A2.2.9. Construct berms and ditches to enhance perimeter security.

A2.2.10. Avoid siting structures and critical equipment in areas where terrain offers vantage points from which adversaries might target facilities and other critical assets.

A2.2.11. Site key facilities and critical assets towards the center of the site to attain maximum standoff distance from the perimeter.

A2.2.12. Provide redundant utility systems and bury all utility lines.

A2.2.13. If the threat warrants, disperse facilities and key assets to reduce the possibility of collateral damage to multiple assets from a single attack.

A2.2.14. If key assets can be better protected if clustered and FP resources are available to increase their level of protection, consider this option.

A2.2.15. 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 (the end of a facility faces the area of the potential blast versus the sides facing the area of the potential blast).

A2.2.16. Compartmentalize primary gathering facilities to limit damage and injuries from fragmenting weapons in the event of an attack.

A2.2.17. Determine appropriate areas to site revetments and other protective structures (blast/fragmentation walls) (e.g., critical assets and key primary gathering facilities, etc.).

A2.2.18. Site facilities that receive bulk deliveries and other structures more vulnerable to an attack (e.g., industrial areas, hazardous waste/hazardous storage areas, refuse collection areas, etc.) in areas away from the main inhabited portion of the site. These areas still need to be secured.

A2.2.19. Assist security personnel in constructing layers of defense to support the ID effort.

A2.2.20. Ensure parking areas are constructed to provide the minimum standoff distance from facilities as determined by DOD standards or the CCDR.

A2.2.21. Select areas for siting trash containers at least 10m/33ft away from facilities and other key assets.

A2.2.22. Site personnel bunkers strategically throughout the site (particularly in highly populated areas) to provide shelter in the event of an attack.

A2.2.23. Site MNS components in areas so that voice notification may be heard throughout the entire site.

A2.2.24. Outline a plan to apply hardening, camouflage, and concealment to all key facilities and critical assets once sited.

A2.2.25. Outline a plan to construct obscuration screens and pre-detonation screens, and install window film application to lessen the severity of damage to key facilities/assets in the event of an attack.