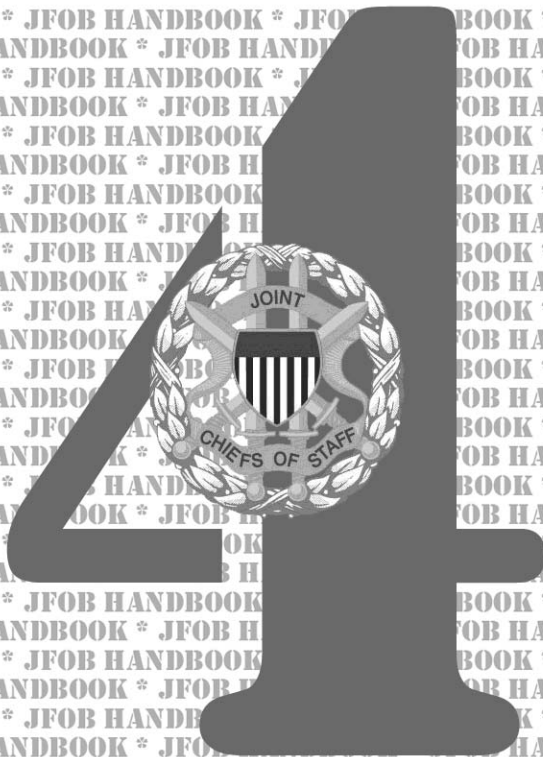


**GTA 90-01-011**  
**EXPIRES 30 SEPTEMBER 2010**

# **JOINT FORWARD OPERATIONS BASE (JFOB) SURVIVABILITY AND PROTECTIVE CONSTRUCTION HANDBOOK**



**FOURTH EDITION - MARCH 2009**

---

**A PUBLICATION OF THE  
JOINT STAFF J3 DEPUTY DIRECTORATE FOR  
ANTITERRORISM/HOMELAND DEFENSE  
ANTITERRORISM/FORCE PROTECTION DIVISION**

Distribution Restriction Statement on inside Front Cover

**FOR OFFICIAL USE ONLY**

# JOINT FORWARD OPERATIONS BASE (JFOB) SURVIVABILITY AND PROTECTIVE CONSTRUCTION HANDBOOK

(Formerly the *JFOB Force Protection Handbook*)

---

This is the **Fourth Edition** of the *JFOB Handbook*, originally issued in November 2005. This edition adds and revises content and organization of the third edition. It also incorporates material previously contained in the *Joint Contingency Operations Base (JCOB) Handbook* and material from the Joint Combat Outpost (JCOP) Quick Reaction Test.

Printed copies of this handbook are available from the nearest Army Training Support Center (ATSC). They can be ordered online at <https://idmsonline.atsc.army.mil>.

Digital copies of this handbook are available from the Joint Staff Anti-terrorism Enterprise Portal (ATEP, at <https://atep.dtic.mil>) or the Reimer Digital Library (RDL, at <http://www.train.army.mil> or <http://www.adtdl.army.mil>).

For additional information or assistance contact the  
JFOB Development Team:  
[jfob@erdc.usace.army.mil](mailto:jfob@erdc.usace.army.mil)

**DISTRIBUTION RESTRICTION:** Distribution is authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made on 16 January 2009. Other requests for this document will be referred to the Survivability Branch (GS-V), Geotechnical and Structures Laboratory, USACE Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, MS 39180-6199.

**DESTRUCTION NOTICE:** Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

## FOR OFFICIAL USE ONLY

The Operational Environment	1
Community Engagement	2
Command and Control	3
Risk Management	4
Planning	5
Site Selection and Layout	6
Critical Infrastructure Assurance	7
Security	8
Access Control	9
Protection	10
Standoff	11
Barriers and Obstacles	12
Entry Control Structures	13
Sidewall Protection	14
Compartmentalization	15
Overhead Cover	16
Lighting	17
Sensor Systems	18
Existing Structures	19
Protective Structures	20
Joint Combat Outposts	21
Abbreviations and Acronyms	A
Force Protection Conditions	B
Materiel Support	C
Soil-Filled Container Applications	D
Tent Camp Layouts	E
References	F

**FOR OFFICIAL USE ONLY**

## Preface to the Fourth Edition

**Scope.** This publication addresses survivability and protective construction at Joint Forward Operations Bases (JFOBs) outside the continental United States. The focus is on defense against mass casualty attacks, specifically rockets, artillery, and mortars (RAMs); vehicle-borne improvised explosive devices (VBIEDs); and personnel-borne improvised explosive devices (PBIEDs). It describes how adversary and friendly courses of action (COAs) are evaluated and implemented to support the JFOB commander's decision making process. It also addresses "best practices" for defeating RAMs, VBIEDs, and PBIEDs. This publication is intended for use primarily by engineer, security, and force protection specialists to assist with operational level planning.

**Purpose.** This publication was prepared under the direction of the Office of the Secretary of Defense. As a result of a Quick Reaction Test (QRT) program, a series of best practices for JFOB defense emerged from current doctrine, Joint tactics, techniques and procedures (JTTPs), and current practices. It provides recommendations for the exercise of protective construction by Combatant Commanders and other JFOB commanders for JFOB defense. It provides military guidance for use by the Services in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of commanders from organizing the force and executing the mission in a manner inconsistent with established plans and operations.

**Application.** This publication is a compilation of the latest Joint and Service doctrine. It also contains the best validated blast mitigation materials and designs from various Department of Defense (DoD) laboratories. The guidance in this publication is not necessarily authoritative. However, many of the practices that result from QRTs may be incorporated into future doctrine or TTPs. The contents of Service publications will take precedence for the activities of Joint Forces unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable.

**Administrative Notes.** This publication replaces the *Joint Forward Operations Base (JFOB) Force Protection Handbook, Third Edition* (GTA 90-01-011), which may be used until its expiration date. It also replaces the *Joint Contingency Operations Base (JCOB) Force Protection Handbook* (GTA 90-01-010), which is obsolete.

Distribution of this handbook is authorized to U.S. Government agencies and their contractors only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made on 16 January 2009. The ERDC Survivability Branch Technical Director determined this handbook can be released to the Allied forces of Australia, Canada, and the United Kingdom. Refer other requests for this document to the Survivability Branch (GS-V), Geotechnical and Structures Laboratory, USACE Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, MS 39180-6199.

**Availability.** This handbook is available in printed form as a Graphic Training Aid (GTA 90-01-011) through the U.S. Army Training Support Center (<https://idmsonline.atsc.army.mil/>). It is also available electronically from either the Joint Staff Antiterrorism Enterprise Portal (ATEP, at <https://atep.dtic.mil>) or the Reimer Digital Library (RDL, at <http://www.train.army.mil/> or <http://www.adtdl.army.mil/>). Other requests for the JFOB Handbook should be directed to the JFOB Development Team ([jfob@erdc.usace.army.mil](mailto:jfob@erdc.usace.army.mil)).

Peter M. Aylward  
Brigadier General, US Army  
Deputy Director for Antiterrorism / Homeland Defense  
The Joint Staff



**FOR OFFICIAL USE ONLY**

## **Acknowledgements**

The Joint Staff wishes to acknowledge the following organizations for providing exceptional support in developing, printing, and distributing the JFOB Survivability and Protective Construction Handbook:

Office of the Secretary of Defense  
Joint Test and Evaluation  
Alexandria, VA

Joint Improvised Explosive Device Defeat Office (JIEDDO)  
Washington, DC 20310

US Central Command (USCENTCOM)  
Joint Security Directorate  
MacDill AFB, FL

Multinational Corps-Iraq (MNC-I)  
Camp Victory, Iraq

US Air Force:

Air Force Civil Engineer Support Agency (AFCESA)  
Tyndall AFB, FL

Force Protection Battlelab  
Lackland AFB, TX

US Army:

Headquarters, Department of the Army (G-3/5/7)  
Washington, DC

Army Test and Evaluation Command (ATEC)  
Alexandria, VA

Rapid Equipping Force  
Fort Belvoir, VA

Headquarters 3rd US Army  
Fort McPherson, GA/Camp Doha, Kuwait

Maneuver Support Center (MANSCEN)  
Fort Leonard Wood, MO

1st Cavalry Division  
Fort Hood, TX

412th Engineer Command  
Vicksburg, MS

20th Engineer Brigade  
Fort Bragg, NC

420th Engineer Brigade  
Bryan, TX

US Army Corps of Engineers:

G-3 Operations  
Washington, DC

Engineer Research and Development Center  
Geotechnical and Structures Laboratory  
Vicksburg, MS

Protective Design Center  
Omaha, NE

US Marine Corps  
Headquarters US Marine Corps, Security Division  
Washington, DC

# Table of Contents

Preface .....	ii
Acknowledgments .....	iv

## Chapter 1: The Operational Environment

Introduction .....	1-1
Joint Security Concept .....	1-2
Forward Operating Bases .....	1-3
Base Functions and Nodes .....	1-5
Threats .....	1-6
Intelligence .....	1-9

## Chapter 2: Community Engagement

Introduction .....	2-1
Information .....	2-2
Planning .....	2-3
Training .....	2-6

## Chapter 3: Command and Control

Introduction .....	3-1
Command Relationships in Joint Security Operations .....	3-2
Unity of Command .....	3-3
Tenant Unit Responsibilities .....	3-4
Operations Centers .....	3-4
Force Protection Team .....	3-7
Incident Response .....	3-8
Consequence Management .....	3-12
Communication Systems .....	3-13
Mass Notification and Warning .....	3-20



**Chapter 4: Risk Management**

Introduction ..... 4-1

Process Overview ..... 4-2

Risk Hazards ..... 4-2

Process Application Guidelines ..... 4-4

Tools ..... 4-6

**Chapter 5: Planning**

Introduction ..... 5-1

Planning Factors ..... 5-2

Joint Operation Planning Process ..... 5-3

Resourcing ..... 5-5

Base Defense Plan ..... 5-5

**Chapter 6: Site Selection and Layout**

Introduction ..... 6-1

General Terrain Considerations ..... 6-1

Site Selection Considerations ..... 6-2

Layout Considerations ..... 6-5

**Chapter 7: Critical Infrastructure Assurance**

Introduction ..... 7-1

Identification ..... 7-1

Additional Infrastructure Areas ..... 7-4

Evaluation ..... 7-9

Resources (For Additional Information) ..... 7-10

**Chapter 8: Security**

Introduction ..... 8-1

Perimeter Security ..... 8-1

Rules of Engagement and Use of Force .....	8-2
Security Forces .....	8-4
Response Forces .....	8-10
Force Protection Condition (FPCON) Measures .....	8-11
Random Antiterrorism Measures .....	8-11

## **Chapter 9: Access Control**

Introduction .....	9-1
Personnel Access Control .....	9-2
Contract Worker/Vendor Access Control .....	9-3
Vehicle Access Control .....	9-6
Materiel Delivery Control .....	9-12

## **Chapter 10: Protection**

Introduction .....	10-1
Joint Protection Functions .....	10-1
Force Protection .....	10-2
Principles of Defense .....	10-3
Levels of Protection .....	10-4
Protective Construction .....	10-5
Mitigation Strategies .....	10-5

## **Chapter 11: Standoff**

Introduction .....	11-1
Physics of an Explosion .....	11-1
Blast Effects .....	11-4
Standoff Guidelines .....	11-8

## **Chapter 12: Barriers and Obstacles**

Introduction .....	12-1
Antipersonnel Barriers .....	12-3
Anti-Vehicle Barriers .....	12-6
Soil-Filled Barriers .....	12-14
Gates .....	12-15

## **Chapter 13: Entry Control Structures**

Introduction .....	13-1
Functional Zones .....	13-1
Overwatch .....	13-2
Design Concepts .....	13-4
Perimeter Barriers .....	13-7
Search and Inspection Areas .....	13-9
Exit Points .....	13-11
Speed Management Techniques .....	13-11

## **Chapter 14: Sidewall Protection**

Introduction .....	14-1
Sandbags .....	14-1
Soil-Filled Wire and Fabric Containers .....	14-3
Soil-Filled Metal Containers .....	14-4
Modular Reinforced Concrete Walls .....	14-5
E-Glass and U-Picket Walls .....	14-6
Modular Protective Systems .....	14-8
Sniper Screens .....	14-9

**Chapter 15: Compartmentalization**

Introduction ..... 15-1

Soil-Filled Plastic Bin Wall ..... 15-2

Wooden Partition Wall ..... 15-4

E-Glass Walls ..... 15-5

Soil-Filled Container Walls ..... 15-6

**Chapter 16: Overhead Cover**

Introduction ..... 16-1

Internal Protection ..... 16-3

External Protection ..... 16-5

SEAhut Overhead Cover Retrofit ..... 16-7

**Chapter 17: Lighting**

Introduction ..... 17-1

Concepts ..... 17-1

Configurations ..... 17-2

Specifications ..... 17-3

Energy Considerations ..... 17-4

**Chapter 18: Sensor Systems**

Introduction ..... 18-1

Intrusion Detection and Surveillance Systems ..... 18-1

IDS Selection Considerations ..... 18-2

**Chapter 19: Existing Structures**

Introduction ..... 19-1

Exterior Soil-Filled Container Retrofit ..... 19-2

Modular Concrete Wall Exterior Retrofit .....	19-2
Pressure Sensitive Adhesive Retrofit .....	19-4
High Capacity Wall Catcher System .....	19-5
Geotextile Fabric Catcher System .....	19-6
Polymer Retrofit System for Masonry .....	19-7

## **Chapter 20: Protective Structures**

Introduction .....	20-1
Bunkers .....	20-1
Fighting Positions and Observation Posts .....	20-4
Towers .....	20-6

## **Chapter 21: Joint Combat Outposts**

Introduction .....	21-1
Threats and Risks .....	21-1
Layout and Design .....	21-2
Perimeter Security .....	21-6
Perimeter Barriers .....	21-8
Entry Control Points .....	21-10
Construction Sequence.....	21-13
Performance Issues .....	21-19

## **Appendix A: Abbreviations and Acronyms .....**

A-1

## **Appendix B: Force Protection Conditions .....**

B-1

## **Appendix C: Materiel Support .....**

C-1

## **Appendix D: Soil-Filled Container Applications ...**

D-1

## **Appendix E: Tent Camp Layouts .....**

E-1

## **Appendix F: References .....**

F-1

This page intentionally blank

# The Operational Environment

## Introduction

The United States, its allies, and its partners face a spectrum of challenges, including violent transnational extremist networks, hostile states armed with weapons of mass destruction, rising regional powers, emerging space and cyber threats, natural and pandemic disasters, and a growing competition for resources. The Department of Defense (DoD) must respond to these challenges while anticipating and preparing for those of tomorrow. The President's 2006 National Security Strategy (NSS) describes an approach founded on two pillars: promoting freedom, justice, and human dignity by working to end tyranny, promote effective democracies and extend prosperity; and confronting the challenges of our time by leading a growing community of democracies. It seeks to foster a world of well-governed states that can meet the needs of their citizens and conduct themselves responsibly in the international system. This approach represents the best way to provide enduring security for the American people.

The National Defense Strategy (NDS) serves as DoD's capstone document in this long-term effort. It outlines how DoD will support the objectives outlined in the NSS, including the need to strengthen alliances and build new partnerships to defeat global terrorism and prevent attacks against us, our allies, and our friends; prevent our enemies from threatening us, our allies, and our friends with weapons of mass destruction (WMD); work with others to defuse regional conflicts, including conflict intervention; and transform national security institutions to face the challenges of the 21st century. The NDS acts on these objectives, evaluates the strategic environment, challenges, and risks we must consider in achieving them, and maps the way forward.

For the foreseeable future, this environment will be defined by a global struggle against a violent extremist ideology that seeks to overturn the international state system. Beyond this transnational struggle, we face other threats, including a variety of irregular challenges, the quest by rogue states for nuclear weapons, and the rising military power of other states. These are long-term challenges. Success in dealing with them will require the orchestration of national and international power over years or decades to come. DoD will continue to transform overseas U.S. military presence through global defense posture realignment, leveraging a more agile continental U.S. (CONUS)-based expeditionary total force and further developing a more relevant and flexible forward network of capabili-

ties and arrangements with allies and partners to ensure strategic access.

Joint Security Concept

The current strategic environment is complex, dynamic, and uncertain. Trends indicate that the demands placed on DoD to conduct operations in the 21st century will be greater than ever. United States forces will be called to prevent escalation of conflict and respond to more foreign or domestic crises or emergencies that significantly impact on US national interests. Our current national security strategy of engagement often requires commitment of forces to secure those interests at home and abroad.

A Joint security area (JSA) is a specific surface area designated to facilitate protection of bases. Regional political considerations and sensitivities will influence whether a JSA is established. The JSA may be used in both linear and nonlinear operations. Figure 1-1 depicts a notional organizational structure for Joint security operations in which all bases are located in a land component commander’s area of operations (AO).

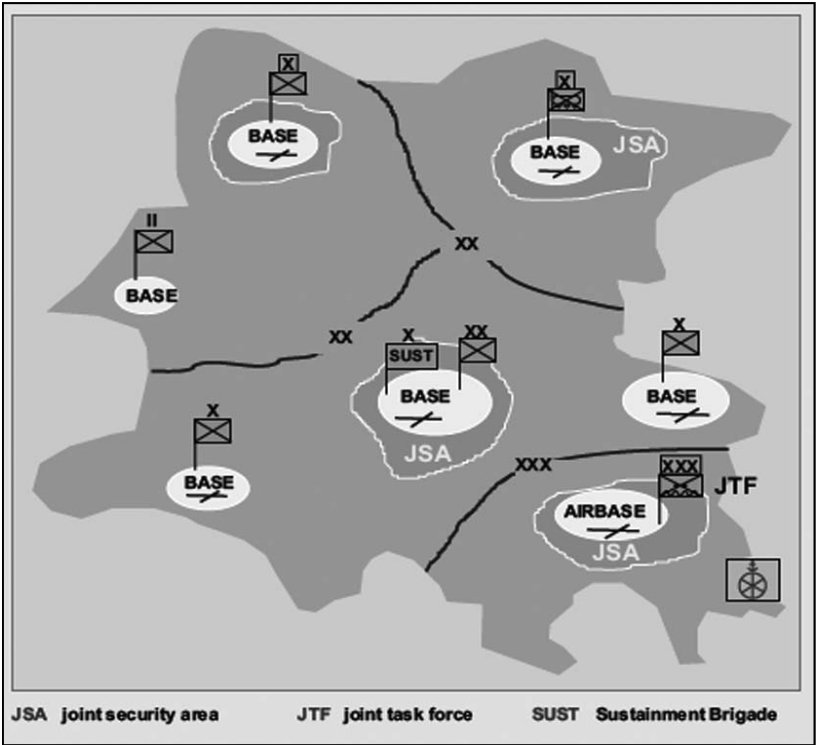


Figure 1-1. Notional Organizational Structure for Joint Security Operations  
(from JP 3-10, *Joint Security Operations in Theater*)



The size of a JSA may vary considerably and is highly dependent on the size of the operational area, mission essential assets, logistic support requirements, threat, or scope of the Joint operation. In linear operations the JSA may be included in, be separate from, or adjoin the rear areas of the Joint Force Land Component Commander (JFLCC) or Joint Force Maritime Component Commander (JFMCC) or Service component commanders.

JSAs may be designated where Joint forces are engaged in combat operations or where stability operations are the primary focus. Providing security of units, activities, bases/base clusters, and LOCs located in noncontiguous areas presents unique challenges based on the location, distance between supporting bases, and the security environment.

JSAs may be established in different countries in the Geographic Combatant Commander's (GCC) area of responsibility (AOR). The airspace above the JSA is normally not included in the JSA.<sup>1</sup> The JSA will typically evolve as the operational area changes in accordance with requirements to support and defend the Joint force. A maritime amphibious objective area may precede a JSA when establishing a lodgment. A lodgment would normally be expanded to an area including existing ports and airfields from which base operations could be conducted, and then eventually evolve to areas including multiple countries and sea boundaries.

## Forward Operating Bases

Current national security, defense, and military strategies utilize flexible expeditionary forces deployed to forward-based activities and forward operating bases (FOBs). The security environment requires that these units, activities, and bases protect themselves against threats designed to interrupt, interfere, or impair the effectiveness of Joint operations. Base and lines of communications (LOCs) security must be properly planned, prepared, executed, and assessed to prevent or mitigate hostile actions against US personnel, resources, facilities, equipment, and information.

Successful onward movement of personnel and accompanying materiel from reception in theater to delivery to the user is vital to the success of Joint force operations. In some operational environments, the greatest risk to Joint force operations may be the threat to the main supply routes (MSRs) from the ports of debarkation forward to the main battle area (in linear operations) or FOBs (in nonlinear, noncontiguous operations).

1. This airspace is normally governed by procedures presented in JP 3-52, *Joint Doctrine for Airspace Control in the Combat Zone*.

Sustained Joint force presence promotes a secure environment in which diplomatic, economic, and informational programs designed to reduce the causes of instability can flourish. Presence can take the form of forward basing, forward deploying, or pre-positioning assets. Joint force presence often keeps unstable situations from escalating into larger conflicts. The sustained presence of strong, capable forces is the most visible sign of US commitment — to allies and adversaries alike. However, if deterrence fails, committed forces must be agile enough to rapidly transition to combat operations. Ideally, deterrent forces should be able to conduct decisive operations immediately. However, if committed forces lack the combat power to conduct decisive operations, they conduct defensive operations while additional forces deploy.

A GCC or a subordinate Joint force commander (JFC) must be prepared to protect bases, base clusters, airfields, seaports, sustainment activities and LOCs within the operational area. JSAs are increasingly vulnerable to adversaries with sophisticated surveillance devices, accurate weapon systems, and transport assets capable of inserting forces behind friendly combat formations. In noncontiguous situations, these forces may operate within the operational areas of friendly forces. Standoff weapon threats in the form of improvised explosive devices (IEDs), mortars, rockets and/or surface-to-air missiles (SAMs) are of particular concern.

Unless determined by higher authority, the JFC will determine the classification of bases according to established policies. A base may be either a Single Service base or a Joint base.

**Single Service Base.** A single-service base contains forces primarily from one Service and where the base's primary mission is under the control of that same Service. Base commanders of these bases are normally designated by the Service component commander.

**Joint Base.** A Joint base has two or more Service units where no Service has a majority of forces or primacy of mission responsibility. The JFC assigns command authority of this base to a Service component and that component will then designate the base commander. When a Joint base is designated, it is critically important that the JFC delegate the authority to conduct Joint security operations within the base boundary to a single commander. However, other Services have forces that contribute to or can accept command of base or base cluster security (for example, elements of the Navy's Naval Expeditionary Combat Command and US Coast Guard port security units).

## Base Functions and Nodes

FOBs can be located in urban or rural areas, on former military bases, in former government complexes, on former religious sites, at critical points on main supply routes, or on rivers. FOBs can be single-service, Joint, allied or coalition to include shared FOBs with host nation military or security forces. FOBs vary in size from small combat outposts to large complexes. Base functions and nodes are shown in Figure 1-2 and described

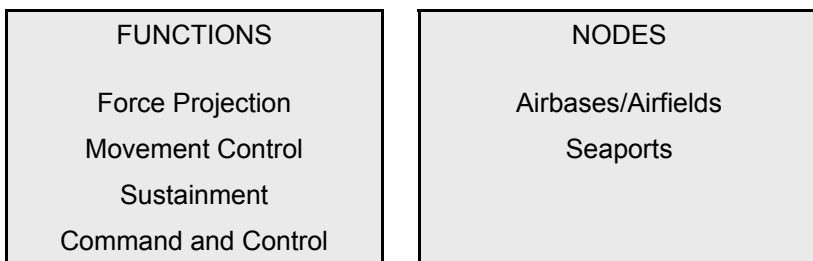


Figure 1-2. Key Joint Security Area Related Functions/Nodes  
(from JP 3-10, *Joint Security Operations in Theater*)

**Force Projection.** Force projection is the ability to project the military instruments of national power from the United States or another theater, in response to requirements for military operations. It allows the JFC to strategically concentrate forces and materiel to set the conditions for mission success. The force projection process involves the mobilization, deployment, employment, sustainment, and redeployment of the Joint force. A secure area is vital for the reception of personnel, materiel, and equipment; assembling them into units at designated staging sites; moving those units to a destination within the operational area; and integrating these units into a mission ready Joint force.

**Movement Control.** Movement control is the planning, routing, scheduling, controlling and coordinating of responsibilities for personnel and cargo movement over LOCs throughout the operational area. Freedom of movement is critical to the support of the Joint force and Joint movement control must be closely coordinated with Joint security operations. The JFC or subordinate JFC normally centralizes transportation movement by designating a Joint movement center (JMC). The JMC controls intratheater force movement, coordinates strategic movements with US Transportation Command (USTRANSCOM) and oversees the execution of transportation priorities. Rail terminals, sea and air ports of debarkation (SPOD, APOD) and other key transportation nodes may be located in a JSA.

**Sustainment.** The primary mission of many of the forces in a JSA is to sustain Joint force operations and forces throughout the operational area. These forces may include any number and type of logistic units and include key supply dumps, medical facilities, and logistic capabilities provided by contractors. Where possible, medical facilities should be situated away from all legitimate military targets to avoid endangerment. The Geneva Conventions prescribe the protections applicable to medical facilities and their personnel.

**Command and Control (C2).** Bases containing C2 capabilities such as major headquarters and signal centers are critical installations in a JSA. The loss of this capability may have a significant impact on the entire operation.

**Air Bases, Airfields, Forward Arming and Refueling Points.** Airfields are critical nodes whether they are APODs and/or force projection air bases. They provide lucrative targets for hostile attack. Aircraft approach and departure corridors and the immediate areas contiguous to the base from which threats to aircraft may originate are a critically important and challenging Joint force security consideration.

**Seaports.** These key nodes are often located on a vulnerable seam between the land and naval force commander AOs. Therefore, component or subordinate Joint force commanders must ensure advance coordination for security operations planning that entails command, communications, rules of engagement (ROE), coordination points and responsibility for security along LOCs and employment of forces. The JFC and subordinate JFCs ensure that port security plans and responsibilities are clearly delineated and assigned.

## Threats

A threat is defined as a source of danger—any opposing force, adversary, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability. Adversaries perform hostile acts against personnel, equipment, and operations. There are four major adversary objectives that describe adversary behavior:

1. Inflicting injury or death on people
2. Destroying or damaging facilities, property, equipment, or resources
3. Stealing equipment, materiel, or information
4. Creating adverse publicity

Threat activities are generally described and categorized in three levels<sup>2</sup> (See Figure 1-3). Each level or any combination of levels may exist in an

operational area, independently or simultaneously. The greatest threat to a FOB, or any activity for that matter, is an attack capable of producing mass casualties. Adversaries will employ a variety of weapons and tactics to achieve this aim.

THREAT LEVEL	EXAMPLES
LEVEL I	Agents, saboteurs, sympathizers, terrorist, civil disturbances
LEVEL II	Small tactical units, unconventional warfare forces, guerrillas, may include significant stand-off weapons threats
LEVEL III	Large tactical force operations, including airborne, heliborne, amphibious, infiltration, and major air operations

Figure 1-3 Levels of Threat (from JP 3-10, *Joint Security Operations in Theater*)

**Level I threats** include adversary agents and terrorists whose primary missions include espionage, sabotage, and subversion. Adversary activity and individual terrorist attacks may include random or directed killing of military and civilian personnel, kidnapping, hijacking air, land, and sea vehicles for use in direct attacks; the use of improvised explosive devices (IEDs), random sniping, vehicle-borne IEDs (VBIEDs), surface to air missiles (SAMs), and/or individual grenade and rocket propelled grenade attacks. Civilians sympathetic to an adversary may become significant threats to US and multinational operations. They may be the most difficult to counter because they are normally not part of an established adversary agent network and their actions may be random and unpredictable. Countering criminal activities and civil disturbance requires doctrine and guidelines that differ from those used to counter conventional forces and normally require detailed coordination with host nation (HN) military, security, and police forces. More significantly, based on political, cultural, or other perspectives, activities that disrupt friendly operations may be perceived as legitimate by a large number of the local populace. Countering Level I threats is considered to be part of the day-to-day force protection measures implemented by all commanders. Key to countering these threats is the active support of some portion of the civilian population, normally those sympathetic to US or multinational goals.

2. The levels of threat used here are introduced in Joint Publication 3-10, *Joint Security Operations in Theater*, to provide a general description and categorization of threat activities. They should not be confused with DoD Threat Levels (Low, Moderate, Significant, and High) or terrorist threat levels (Negligible, Low, Medium, High, and Critical) used in DoD threat assessments (Refer to DoD O-2000.12-H, *DoD Antiterrorism Handbook*).

**Level II threats** include small scale (described as less than company-sized equivalents) irregular forces conducting unconventional warfare that can pose serious threats to military forces and civilians. These attacks can cause significant disruptions to military operations as well as the orderly conduct of local government and services. These forces are capable of conducting well coordinated, but small scale, hit and run attacks, IED and VBIED attacks, and ambushes and may include significant standoff weapons threats such as mortars, rockets, rocket propelled grenades, and SAMs. Level II threats may include special operations forces that are highly trained in unconventional warfare. These activities may also include operations typically associated with terrorist attacks outlined in the previous paragraph including air, land, and sea vehicle hijacking. These forces establish and activate espionage networks, collect intelligence, carry out specific sabotage missions, develop target lists, and conduct damage assessments of targets struck. They are capable of conducting raids and ambushes. If the JFC assigns a base boundary to an installation, sufficient organic forces must exist on that installation to deter and defeat Level II forces as defined.

**Level III threats** may be encountered when a threat force has the capability of projecting combat power by air, land, or sea, anywhere into the operational area. Specific examples include airborne, heli-borne, and amphibious operations; large combined arms ground force operations; and infiltration operations involving large numbers of individuals or small groups infiltrated into the operational area, re-grouped at predetermined times and locations, and committed against priority targets. Air and missile threats to bases/base clusters and lines of communication (LOCs) may also pose risks to Joint forces, presenting themselves with little warning time. Level III threats necessitate a decision to commit a tactical combat force (TCF) or other significant available forces to counter the threat. This threat level is beyond the capability of base and base cluster defense and response forces.

Few states will have the resources, or the need, to attack the US directly in the near future. However, many will challenge it for control or dominance of a region. Potential adversaries may increasingly resort to asymmetric means to threaten our national interests. Such methods include unconventional, unexpected, innovative, or disproportional means used to gain an advantage. Adversaries may use inexpensive approaches that circumvent the US strengths, exploit its vulnerabilities, or confront it in ways the US cannot match in kind. Contemporary threats include terrorism; chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE)

threats; information operations; exploitation of commercial or space-based systems; denial of our access to critical resources; and environmental sabotage.

## Intelligence

Intelligence provides the commander with a threat assessment based on an analysis of the full range of adversary capabilities and a prediction of the adversary's likely intention. With predictive, accurate, and relevant intelligence, commanders may gain the critical advantage of getting inside the adversary's decision-making cycle, improving insight into how the adversary will act or react. The commander can therefore formulate plans based on this knowledge and thus decrease the risks inherent in military operations and increase the likelihood of success.

Intelligence identifies adversary capabilities, helps identify the centers of gravity (COGs), projects probable courses of action (COAs), and assists in planning friendly force employment. By determining the symmetries and asymmetries between friendly and adversary forces, intelligence assists the JFC and operational planners in identifying the best means to accomplish the Joint force mission. For example, in support of Joint information operations (IO), intelligence provides the JFC and component commanders with information on the relevant physical, informational, and cognitive properties of the information environment and its impact on military operations; estimates of what the adversary's information capabilities are; when, where, and how the Joint force can exploit its information superiority; and the threat the adversary poses to friendly information and information systems.

To prepare for an attack, adversaries will conduct surveillance over a period of time. Comprehensive surveillance of a targeted facility usually precedes an attack. Surveillance is often an indicator of a pending attack. This surveillance preceded the Riyadh, Nasiriya and many Iraq VBIED attacks. Recognizing the types of surveillance used should help personnel develop plans to thwart potential attacks more effectively.

**Fixed surveillance** may be carried out from a fixed position, a nearby building, business, or other location. In fixed surveillance scenarios, adversaries may establish themselves in a public location over an extended period of time or choose disguises or occupations such as street vendors, tourists, repair or deliverymen, photographers or even demonstrators. This is the easiest pre-attack surveillance to detect.

**Mobile surveillance** means observing and following targets, or non-mobile facilities. For example, an adversary may drive by a power

plant to observe the building or compound. To make mobile surveillance less detectable and more accurate, many adversaries use progressive surveillance.

In **progressive surveillance**, the adversary will follow a target or observe part of a building for a short period of time, withdraw for a period of time (possibly days or even weeks), and then resume surveillance, possibly from a different location. This continues until the adversary develops target suitability and/or noticeable patterns in the targets movement or vulnerability. This type of transient presence makes the surveillance much more difficult to detect or predict.

The more sophisticated surveillance is likely to be accomplished over a long period of time. A tape discovered in Indonesia, possibly compiled over months, demonstrates the patience used to compile a viable plan and the attention to detail. Watching carefully where US personnel get on their transportation and detailing every possible thing that could help the attack (even manhole covers), the narrators pointed out in great detail how the attack might be carried out.

The most important role of intelligence in military operations is to assist commanders and their staffs in understanding and visualizing relevant aspects of the operational environment. This includes determining adversary capabilities and will, identifying adversary critical links, key nodes, high-value targets (HVTs) and COGs, and discerning adversary probable intentions and likely COAs. Visualization of the operational environment requires a thorough understanding of the characteristics of the operational area and the current dispositions and activities of adversary and neutral forces. It requires knowing the adversary's current and future capability to operate throughout the operational environment based on a detailed analysis of the impact of weather, geography, and other relevant considerations. Most important, visualization requires understanding the adversary's objectives, identifying how the adversary might fulfill those objectives, and determining the adversary's readiness to achieve the objectives. Together, all these factors make a critical contribution to the JFC's capability to achieve information superiority. However, intelligence must also enable the JFC to know the potential and probable future state of events well in advance of the adversary. This knowledge allows the JFC to predict the adversary's future COA and scheme of maneuver, and to anticipate adversary actions and plan detailed countermeasures.



# Community Engagement

## Introduction

Community Engagement (CE) is an element of antiterrorism Joint doctrine necessitating interaction beyond the base perimeter. The basic idea of CE is to separate identity, goals and grievances of extremist groups and the local community (See Figure 2-1). Like force protection, CE is not a mission; it is an enabler for other missions by facilitating positive community interaction.

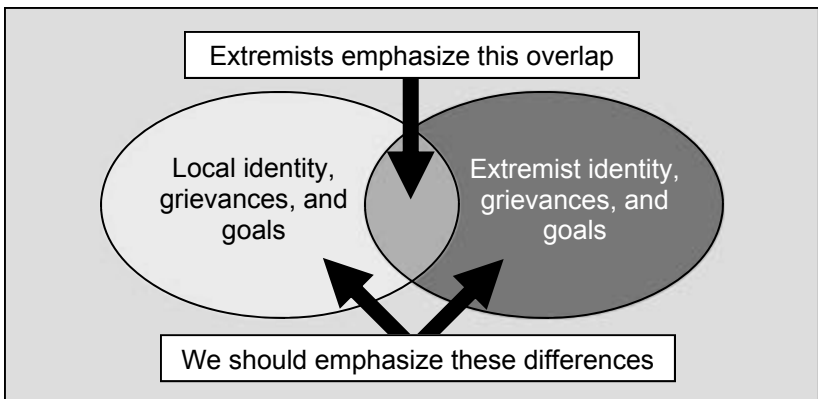


Figure 2-1. Countering Violent Extremists Locally

CE is important because the force becomes part of a local community when it establishes a FOB. Its presence can threaten, embolden, or otherwise alter local inhabitants' influence, routines, prestige, or culture. Interactions with and community impressions of the interaction can either help or hurt the force protection posture of the base. Successful CE can build positive perceptions and help minimize potential negative perceptions of the US presence.

The components of community engagement include information, planning, and training. The traditional roles of CE are explained below.

**CE clarifies the base role in the community.** CE helps the commander to identify community leaders (official and unofficial) and facilitates informal relationships, improved communications, and mutual respect between base and community members by reducing fric-

tion between military and civilian populations. CE provides a two-way communication channel between the community and base leaders. Although the base may not be able to resolve all community concerns, giving a community a venue to voice concerns and build relationships with base leadership supports mutual legitimacy.

**CE facilitates operations.** CE improves the commander's ability to assess the local threat picture through improved situational awareness. CE, and effective two way communication overall, reduces the potential for non threatening issues, such as labor protests, to interfere with base operations or provoke a confrontation with US forces.

**CE supports Countering Violent Extremism (CVE).** CE supports efforts to counter violent extremism and create a sustainable environment that denies support to violent extremists. CE can improve base interactions with the community, empower cooperative voices, educate local populations to counter extremist propaganda, highlight extremist or terrorist weaknesses, and present alternative viewpoints.

## Information

CE contributes to and draws from intelligence by integrating and applying the detailed threat analysis with a broader understanding of the cultural, tribal, ethnic or religious topography of an area. It is important to draw on a number of diverse sources and types of information to avoid an incomplete assessment of the environment.

Review existing references covering recent events, history, government, social structures, society, culture, language, power and authority structures and competing regional interests. Websites that outline material to consider in community engagement research are shown in Figure 2-2.

Talk with a broad selection of Coalition forces, local leaders, translators, local community members, and base employees to learn about local power structures, issues, rivalries, grievances and differences. Observe and research official and unofficial actions by other US forces, international organizations, non governmental organizations, and the local government operating in the same area to synchronize goals and activities whenever possible.

Manage information gathered by personnel off base (for example, which roads are good, which clans are fighting, market locations) so the information can be used by others. If a Biometrics Force Protection Screening Cell is on site, utilize it to map out clan relationships, interview persons of

interest, and assess the sensibilities of local nationals working on your base. The screening process is an excellent opportunity to speak with local nationals out of view of other local nationals.

Observe how US operations are portrayed locally, by insurgents, government, civilians and others by reviewing local newspapers, radio, web-sites, videos and local leader speeches. Work with civil affairs, psychological operations (PSYOP), and public affairs specialists to ensure local perceptions of base actions and information reflect mission objectives.

**Human Terrain System:**  
<https://www.intelink.gov/inteldocs/browse.php?fFolderId=8568>

**Cultural Orientation Resource Center:**  
<http://www.cal.org/co/publications/profiles.html>

**Open Source Intelligence on Cultural resources:**  
<http://www.onstrat.com/osint/#countrystudies>

**Cultural Taxonomy:**  
<https://www.intelink.gov/wiki/MCIACulturalTaxonomy>

**Cultural Intelligence:**  
<https://www.intelink.gov/wiki/CulturalIntelligence>

**Countering Violent Extremism Lessons Learned:**  
<https://www.intelink.gov/wiki/LessonsLearned>

Figure 2-2. Community Engagement Related Web Sites

## Planning

Proper planning will facilitate actions that can build and sustain a positive image of US forces in the area. The image of US forces is important because it can facilitate or hinder future operations. Do not rely on public relations to smooth over difficulties after an event.

**CE Planning Principles.** Know who you are talking to and demonstrate through your actions that you are familiar with their background, culture, and customs. Host and accept invitations to public community meetings, when appropriate, to discuss current events, local needs, and base operations. Support local leader initiatives, such as publications, education programs, as appropriate. Integrate them with broader regional activities when possible.

Promote informed operational planning through knowledge of indigenous populations, norms, customs, culture, religion, etc. Carefully weigh the

effects of kinetic and non-kinetic means used in the area. If kinetic means are used, plan efforts to minimize impact and offset negative implications.

Remain balanced in treatment of community members, especially community leaders. Understand that everyone has their own interests in interacting with the US and military forces. Beware of disenfranchising local influence holders because loss of influence may lead to animosity or hostility against US personnel and the base.

Be accessible and responsive to community members. Answer questions and concerns of locals, or direct them to someone who can address their concern (local non-government organizations, government office, or community leader). Utilize Force Protection Screening Cells or other venues, as appropriate, to speak with local nationals out of the site of other community members.

**The main gate/entry control point.** The main entry control point (ECP) is often the first impression community members have of the US and the base. In addition to force protection concerns and operational requirements, base leaders should consider the base's impact on community perceptions and interaction.

Local nationals visit a base for a variety of reasons, including jobs, liaison, complaints, and both US and local government support. A local visitor's interaction at the main gate creates an impression of base operations overall and communicates US perceptions about the local community. Force protection remains paramount and interaction with locals must remain professional and respectful. Local nationals supporting ECP operations should be trained and held accountable to uphold the US standards for dealing with visitors. Local guards should be monitored to ensure they are not putting local rivalries or personal interests above base intent.

Part of a community landscape, ECP effects on community activities (e.g. traffic or markets) should be taken into consideration before choosing a location. If the location is already determined, ECP operations, including staffing and peak entry/egress times, can also be modified to reduce impact on the community. Also, with routine presence of local workers and visitors on base, the ECP often becomes the venue for demonstrations and attacks. ECP positioning can help to shield community residences and mitigate effects of protests or attacks on the local population and base.

**Use interpreters properly.** A key asset in community interaction is having reliable interpreter support on and off base. Interpreters may come

from the US or may be hired from within the host nation (HN). Considerations for selecting HN interpreters are shown in Figure 2-3.<sup>1</sup>

- Interpreters should be native speakers of the local language and be fluent in English. One suggested way to test English skills is to say something in English and have them paraphrase it.
- Interpreters should be of comparable ethno-religious makeup as the local population.
- Consider the effects of their age, gender or ethnicity on their ability to be effective and respected communicators. For example, in some conservative societies, it is often necessary to have women interpret for women and men interpret for men.

Figure 2-3. Interpreter Selection Considerations

When working through an interpreter, use clear English, avoiding profanity, acronyms, obscure words, jokes/humor, or slang. This helps to facilitate accurate translation. Avoid simultaneous translations (interpreter and speaker speaking at the same time). Pause for the interpreter to finish speaking before starting a new thought and limit the length of phrases between interpretations. Concise segments will facilitate accurate translation, keep dialog flowing, avoid uncomfortable staring, and keep audience attention. When using an interpreter, look at the audience being addressed, not the interpreter. It may help to have the interpreter stand slightly behind the person speaking.

**Know the interpreter's background.** Be aware of biases the interpreter may have concerning tribal, ethnic, religious or other affiliations. If possible, periodically audit the translations with objective US Government interpreters to gauge accuracy.

Working as an interpreter is often considered the highest level of work available to local nationals. In Central Asia, because of the hierarchical structure of society, an interpreter assigned to an officer often deems himself to have equivalent rank. As interpreters gain the confidence of the personnel they support, some may believe they carry the same rank and should be allowed the same privileges as the officer to whom they are assigned. Some may also attempt to use their assumed prestige and influence to exploit local nationals of lesser rank. Therefore, consider rotating interpreters throughout the command so that no one interpreter becomes entrenched in the command hierarchy.

1. For further information, see Appendix C (Linguist Support) of FM 3-24/MCWP 3-33.5, *Counterinsurgency*.

## Training

US representatives interacting with the community should be oriented to the region, people, culture, history and current conflict before beginning CE outreach. Key tenants of this orientation process include:

**Learn basic language skills**, both verbal and non verbal (hand signals). Know basic greeting words and gestures, appropriate levels of physical contact (shaking hands) and different terms for people of different societal rank.

**Study cultural norms and taboos** (public drinking, dietary restrictions, loud speaking or how to enter someone's home). Be familiar with basic religious beliefs, holidays, customs, important symbols and offenses.

**Develop an understanding of the community's value system**, including the indicators of honor, shame, guilt and trust. Other considerations include leadership styles, protocols, conception of time and legitimate authority. For example, in some societies it is considered rude to immediately get to the point of a discussion, and preliminary discussion should focus on matters such as family, the weather, or holidays.

**Understand gender roles**. In some societies men and women do not mix in ways familiar to most Americans. Interacting with members of the opposite sex without regard to societal constraints may be perceived as an affront to honor or insulting to the parties involved.

**Rehearse and roleplay scenarios** to solidify understanding of community engagement tenants. Rehearsals may be used to prepare for potential meetings with local leaders, or proper use of an interpreter.

# Command and Control

### Introduction

No single activity in military operations is more important than command and control (C2). Alone, C2 will not destroy a single adversary target or affect a single emergency resupply. Yet, none of these essential Joint force activities, or any others, would be possible without effective C2. A superior communications system helps commanders to maintain the unity of effort to apply their forces' capabilities at the critical times and places to win.

In one way or another, C2 is essentially about information: getting it, judging its value, processing it into useful form, acting on it, and sharing it with others. There are two basic uses for information. The first is to help create situational awareness (SA) as the basis for a decision. The second is to direct and coordinate actions in the execution of the decision. The communications system must present information in a form that is both quickly understood and useful.

Quite often, C2 is thought of as a distinct and specialized function — like logistics, intelligence, electronic warfare, or administration — with its own peculiar methods, considerations, and vocabulary, and occurring independently of other functions. In fact, C2 encompasses all military functions and operations, synchronizing them into a meaningful whole. C2 is the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.

The first element of a C2 system is people. People acquire information, make decisions, take action, communicate, and collaborate with one another to accomplish a common goal. Human beings — from the senior commander framing a strategic concept to a junior Service member calling in a situation report — are integral components of the C2 system and not merely users of it. The second element of the C2 system taken collectively are the facilities, equipment, communications, and procedures essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. Although families of hardware are often referred to as “systems,” the C2 system is more than simply equipment. High-quality equipment and advanced technology do not guarantee effective C2. Effective C2 starts with well-trained and qualified people and an effective guiding philosophy and procedures.

## Command Relationships in Joint Security Operations

The Joint Force Commander (JFC) will normally designate Joint security areas (JSAs) to ensure the security of base/base clusters and lines of communication (LOCs). The JFC establishes command relationships within the operational area, but may delegate certain authority to subordinate commanders in order to ensure effective control and to facilitate decentralized execution of security operations.

The JFC may retain control of Joint security operations and may coordinate them through the Joint force operations directorate (J-3), or he may designate the Joint Force Land Component Commander (JFLCC) or Joint Force Maritime Component Commander (JFMCC) as an area commander with Joint security responsibilities. To facilitate Joint security operations, commanders should establish a Joint security element to coordinate Joint security operations. The individual who normally leads a Joint security element is referred to as the Joint Security Coordinator (JSC).

Bases and base clusters will normally be established to support Joint operations and placed under the control of a base commander or base cluster commander. The base commander is responsible for security within the base boundary and has a direct interest in the security of the area surrounding the base. The area commander will establish base boundaries in coordination with the base or base cluster commander. Base defense is accomplished in a coordinated effort by base defense forces providing security within the base boundary and other ground or surface forces executing security tasks outside that boundary. The base boundary is not necessarily the base perimeter. It should be established based upon the factors of mission, enemy, terrain and weather, troops and support available - time available (METT-T),<sup>1</sup> specifically balancing the need of the base defense forces to control key terrain with their ability to accomplish the mission. Base boundaries may be dynamic, requiring ongoing coordination because of changing METT-T factors over time.

The JFC may task the land, air, or maritime component commander to provide tactical combat forces to counter large tactical force threats. The JFC also assesses the availability and effectiveness of host nation (HN) contributions to base security. Based on this assessment, the JFC may be required to adjust the concept of operations, sequencing, and unit missions. Transportation (ports, highway networks, waterways, airfields, and railroads) nodes; communication systems, intelligence capabilities, and existing host-nation support and civil considerations all affect JSA organization and conduct of operations.

1. The US Army considers METT-TC, where C stands for civil considerations.



The base commander is responsible for security operations and will exercise tactical control (TACON) over all forces performing base defense missions within the base boundary. This includes both isolated bases and bases with a contiguous Joint force area commander. The base/base cluster commander will coordinate such operations with the Joint security element, HN security forces, or other agencies as appropriate.

The JFC, normally through a designated JSC, ensures that appropriate command relationships among subordinate area, base and base cluster commanders are established and understood by all affected commands. Command relationships determine the interrelated responsibilities between commanders as well as the authority of commanders in the chain of command. The typical command relationships established in support of Joint security operations should be TACON between the base or base cluster commander and the dedicated security force, when the attached force is from a different component command.

## **Unity of Command**

The FOB commander is responsible for base force protection and security operations. In this capacity, the FOB commander should use all available assets to create the required level of security. Accordingly, the FOB commander may, for purposes of base force protection and security, exercise temporary operational control (OPCON) or TACON over tenant and transient units from other Services or functional components that are assigned or attached to the base. Commanders at all levels assigned, attached, OPCON or TACON to the FOB commander have the responsibility to ensure that all base force protection, security, and defense procedures are executed accordingly. Unity of command is essential to this concept of FOB force protection.

Unity of command will help to overcome the challenges created when different units from different commands with different missions are assigned to support the FOB's force protection mission. A senior commander (usually either the JFC or the FOB commander) will provide the authority to bring the various units together to accomplish the mission. FOB command relationships should be established early, ideally prior to the units' occupying the FOB. In addition, the FOB commander should define areas of responsibility not only for units occupying the FOB but also for the surrounding area that has direct influence on the security of the FOB.

Critical to the success of the FOB force protection mission is the need for coordination and cooperation among the units tasked with supporting the FOB. These units must build operational relationships based on trust and

confidence and mutual support. To encourage this sense of cooperation and to further the building of unit interrelationships, the FOB operations officer, force protection officer, and the force protection working group should take the lead in orchestrating the coordination and cooperation effort.

### **Tenant Unit Responsibilities**

Tenant unit commanders are commanders of units that reside and operate on, but do not fall under the direct command of the FOB commander. Tenant unit commanders must actively participate in the preparation of base security and defense plans. They will normally be required to provide security of their own forces and high-value assets, provide individuals to perform perimeter/gate security, and will often be assigned battle positions according to base security plans. These forces, when provided, will be under the TACON of the base commander for the purpose of base defense. Most importantly, they are required to ensure that all personnel are properly trained to support and participate in base security in the event of attack. Tenant Joint special operations task forces, because of low personnel densities, must coordinate the above requirements with the base commander.

Key concerns of tenant involvement in OIF have been training, rehearsals, coordination, and competing requirements between the security mission and other operational tasks. Commanders remain concerned about friendly-fire incidents and accidental discharges at entry control points. Spectators gathering in areas of recent attacks may impede incident responders and create additional targets. Tenant unit commander force protection responsibilities are shown in Figure 3-1.

Often, tenant units, the program managers for contractors deploying with the force, or even security forces will be operating with incompatible communications equipment. The JSC and subordinate commanders responsible for planning and executing Joint security operations must ensure that specific base, base cluster and line of communication security communications measures are planned for and tested to ensure compatibility. If communications compatibility is identified as an issue, then the appropriate commander must take proper “work-around” actions.

### **Operations Centers**

The JSC (or staff element) may establish operations centers to assist in meeting Joint security requirements. Component and staff representation will vary according to mission, forces, and security requirements.

### Tenant Unit Commander's Responsibilities

- Participating in the preparation of base defense plans
- Providing, staffing, and operating base defense facilities in accordance with base defense plans
- Conducting individual and unit training to ensure readiness for assigned defense tasks
- Providing their share of facilities, equipment, and personnel for the BDOC and, when appropriate, for the BCOC
- Advising the base commander on defense matters peculiar to their units
- Providing for their own internal security
- Sustaining and administering their own forces
- Providing their requirements for common-user communications systems to the base commander's communications element
- Providing organic communications to support their own commands' requirements

Figure 3-1. Tenant Unit Commander's Force Protection Responsibilities

**Joint Security Coordination Center (JSCC).** A JFC may elect to establish a JSCC using the designated JSC staff elements and representatives from the components operating within the operational area. Component and staff representation will vary according to mission, forces, and security zone requirements, and should support the planning, coordination, and execution of all Joint security related operations. The JSC will ensure that component representation and representation from the JSC staff is sufficient to support assigned mission responsibilities. The JSCC serves as the JSC's full time centralized planning, coordinating, monitoring, advising, and directing agency for operational area Joint security operations. It coordinates with other elements on the JSC staff, with higher, lower, and adjacent command staffs, and with HN and allied command staffs. The JSCC is manned with full time staff for key personnel and additional "as needed" personnel with subject matter expertise as available.

**Base Defense Operations Center (BDOC).** A BDOC is a command and control facility established by the base commander as the focal point for force protection, security, and defense within the base boundary. Through the BDOC, the base commander plans, directs, integrates, coordinates, and controls all base security efforts, and coordinates and integrates area security operations with the base cluster operations center (if established) or other designated higher-level staff as designated by the JSC. The nature of the BDOC depends on the combination of forces involved and may include other US Services, multinational HN and/or other US agencies per-

sonnel, depending on the combination of forces located at each particular base. Multi-Service, other agency, HN and/or multinational representation should be part of the BDOC when elements of their armed forces, police, or paramilitary forces are directly involved in the overall base defense effort or they are a major tenant organization to the base. The center normally consists of three primary sections — command, intelligence, and operations — with additional sections as deemed necessary. These additional sections could include a logistics section to plan the provision of services and support to the base, and an area damage control (ADC) section that provides inspection, planning, and control of the base's emergency response/ADC resources. The BDOC is manned full time with key personnel and augmented with subject matter expertise as required.

**Base Cluster Operations Center (BCOC).** A BCOC is a command and control facility established by the base cluster commander to serve as the focal point for the security of the bases within the base cluster. It plans, directs, integrates, coordinates, and controls all base cluster security efforts. The BCOC personnel keep the base cluster commander informed of the situation and resources available to cope with security related requirements. They coordinate all BDOC efforts, and integrate Joint security operations with other designated higher-level staff as designated by the JFC. The nature of the BCOC depends on the combination of forces involved and may include other US Services, multinational HN and/or other US agencies personnel. The BCOC is similar in many respects to the land force unit's tactical operations center and, in some cases, may be one and the same. Representatives from intelligence, maneuver, and fire support staff the BCOC. The base cluster commander provides other functional staff representatives to augment his base commanders as necessary. Multi-Service, other agency, HN and/or multinational representation should be part of the BCOC when elements of their armed forces, police, or paramilitary forces are directly involved in the overall base defense effort or they are a major tenant organization to the base.

**Area Operations Centers (AOC) and Tactical Operations Centers (TOC).** Army and Marine Corps area and subarea commanders may have AOCs and TOCs to assist in accomplishing their area security and defense mission. These command and control facilities serve as the area and subarea commander's planning, coordinating, monitoring, advising and directing agencies for Joint security operations. AOCs may be designated as a JSCC and either AOCs or TOCs can serve as BCOCs and/or BDOCs.

Base and base cluster commanders must set priorities for tasks involved in base security. Work may occur on several concurrent tasks. Figure 3-2 presents some key base security work priorities.

## Base Security Work Priorities

- Preparation of a base security plan
- Establishment of appropriate perimeter standoff based on threat and host nation situation
- Establishment of vehicle and personnel entry points and search areas
- Establishment of access control processes, badges, and local national labor and visitor control procedures
- Construction of personnel survivability shelters in vicinity of work centers, living areas, and recreation facilities
- Establishment of attack warning systems (including alarms, codes, actions and means of population education)
- Integration of host nation or coalition forces as required
- Establishment of mass casualty procedures and capabilities
- Development of Joint coordinated fire plan
- Conduct rehearsals
- Establishment/coordination of active patrols and tactical counterintelligence operations within the base boundary to deny the enemy freedom of action
- When defending airbases: establishment of shoulder-launched surface-to-air missiles suppression patrols and response capabilities to deny the enemy terrain from which to engage aircraft landing/taking off. This will be done within the base boundary or in coordination with the area commander.

Figure 3-2. Base Security Work Priorities  
(From JP 3-10, *Joint Security Operations in Theater*)

## Force Protection Team

A team approach should be implemented in order to have an effective FOB force protection program. For the team to interact efficiently, all participants should understand the concepts, roles, and capabilities of the other members.

**FOB Operations Officer.** The FOB operations officer serves as the principal staff officer responsible for planning, coordinating, and executing all aspects of FOB force protection operations. The FOB operations officer appoints and should rely heavily on the FOB force protection officer to accomplish these tasks.

**FOB Force Protection Officer.** The FOB force protection officer functions as the principal advisor to the commander and operations officer on

all force protection matters. Primary responsibilities should include:

- Coordinating the sharing of intelligence and information among the units that support the FOB force protection mission
- Providing a sense of command and control and overall coordination of force protection operations
- Establishing force protection work priorities
- Coordinating the efforts of the FOB force protection working group in designing, developing and implementing force protection, antiterrorism and physical security policies and procedures

**FOB Force Protection Working Group.** Early during the occupation of a FOB, a FOB force protection working group should be established. The working group is ideally suited for developing the FOB force protection plan, sharing intelligence/ information, and assisting the BDOC in coordinating force protection operations. Members of this group should include representatives from:

- Tenant Units
- Intelligence/Counterintelligence
- Medical
- Fire/Emergency Response
- Engineers
- Security/Law Enforcement
- Chemical, Biological, Radiological, Nuclear, and High Yield Explosives (CBRNE) Defense
- Logistics
- Explosive Ordnance Disposal (EOD)
- Communications and Information Systems
- Public Affairs
- Resource Management (Comptroller)
- Legal
- Emergency Response Forces (External Security Forces, Tactical Combat Force, etc.)
- Host Nation (HN) (as appropriate)

### **Incident Response**

Incident Response (IR) is a short-lived, confused, creative, fast-paced flow of events after an attack, a life-threatening or damage-causing event. It is paramount that immediate action is taken to save lives, prevent suffering, and protect friendly forces, facilities, equipment and supplies from further harm. This response requires that critical actions take place immediately after an incident to minimize the impact on friendly force operations and

expedite the recovery of the FOB to full operational capability. A typical installation response team should be task organized to respond to all incidents regardless of threat, tactic, or event. This requires establishment of an on-scene commander who coordinates all activities at an incident site through an incident command system (a systemic procedure whereby FOB staffs are organized to provide response to an incident). The FOB should have the capability to perform these standard actions:

- Establish command and control at the incident site and secure the area
- Perform a tactical appraisal of the situation
- Prepare a damage and casualty assessment
- Take immediate actions to save lives, prevent suffering, reduce, or mitigate great property damage
- Determine a priority of response effort and subsequent order for follow-on response forces, equipment, and supplies
- Establish staging locations where forces and equipment can be located to support an incident
- Establish mass casualty/care/evacuation centers

**Incident Response Phases.** Five phases of incident response are under the control of the BDOC. Each phase of the operation is coordinated with the BDOC where actions are coordinated with the operations staff.

**Preparation.** The pre-strike phase that focuses on identifying mission essential vulnerable areas (MEVA), developing incident response and consequence management plans, and identifying and providing resource capabilities necessary to respond to attacks on these areas.

**Response.** The first one-half hour after strike when incident responders are notified, arrive, and take control of the scene.

**Occupation.** When the on-scene commander assesses the situation, requests and obtains required support.

**Support.** When support personnel arrive and conduct emergency operations.

**Recovery.** Actions that are carried out to recover from the incident. This phase will transition to consequence management. It may require a few hours but could take several weeks.

**Incident Response Planning.** FOB commanders with tenant command representation form a Force Protection Working Group (FPWG). The planning organization is normally based on those individuals who compose the operations center staff during crisis management, as well as additional staff representation from special offices, such as the budget or civilian personnel offices.

To be successful, members must be pre-designated, train together, and be prepared to perform individual and collective crisis management missions under the control of the installation commander or the designated representative. Tenant commanders may also serve or have staff representation in this organization. The most common participants in the crisis management organization are as follows:

**Medical Team.** This team is capable of conducting triage, patient decontamination and back-up responder decontamination as necessary.

**Fire Fighters.** The senior fire-fighter normally becomes the on-scene commander upon arriving at the incident. This team establishes staging areas and can call back-up forces for hazardous material (HAZMAT) conditions or assistance in controlling a fire.

**Law Enforcement.** This team is responsible for securing the crime scene, providing responder security and controlling ingress and egress at the incident site.

**Search and Rescue Teams.** These teams usually work in pairs and are responsible for casualty extraction. If available, a structural engineer on the team can conduct safety and damage assessment.

**Explosive Ordnance Disposal (EOD).** The EOD Team is responsible to detect, identify and render safe any suspected munitions and to look for secondary devices.

**Incident Response Equipment.** During the planning process, identify equipment that will be utilized during the IR process. This equipment includes:

- Weapons
- Communication systems
- Ambulances
- Fire trucks
- Rescue vehicles
- Extraction equipment (“Jaws of Life,” ropes, block & tackle)
- Construction equipment (hydraulic excavator, bulldozers)
- Barriers
- Aviation assets
- EOD assets

**Quick Reaction Force (QRF).** QRFs are identified, trained, and equipped to support the security of FOBs. Typically, the QRF is designed to defeat Level II threats (See Chapter 1). The specific organization and planning requirements are driven by mission, enemy, terrain and weather, and personnel available. These issues must be continuously assessed. The



QRF may be attached or assigned but is normally under OPCON to the BDOC commander.

The QRF should be resourced to provide 24 hour support to the base camp. The QRF must be fenced off from any other competing requirements. The significant training and coordination requirements argue against changing QRF units out too frequently.

**QRF Training.** The QRF develops and implements drills to defeat Level II threats in their area of responsibility. The two events most likely encountered by a QRF include indirect fire and enemy attack. The QRF also responds to suspicious vehicles or personnel and protects mission essential and vulnerable areas. The QRF should be well rehearsed in a number of tasks. A sampling of these tasks is listed below:

- Friendly and enemy recognition
- Actions on contact
- Find and secure impact sites
- Call for fire and employment of fixed and rotary wing support
- Communication techniques to include hand and arm signals, challenge and password, running passwords, the use of pyrotechnics and other recognition signals
- React to unexploded ordnance
- Enemy prisoner of war (EPW) procedures
- Evacuation and cordon activities
- React to hostage situation

It is important that the QRF has a full understanding of the base defense plan and demonstrates this understanding through periodic rehearsals. The QRF should possess the base defense plan, to include barriers and sector sketches; the base fire support plan; and local medical evacuation (MEDEVAC) procedures. The QRF must understand the base camp standing operating procedures (SOP).

**QRF Employment.** The BDOC commander normally has authority to employ the QRF. Prior to employment, the QRF commander must be briefed on the specifics of the mission, any changes to the rules of engagement (ROE), and any other special requirements. If the QRF is committed, the BDOC will notify medical facilities in the Division's sector to be put on alert to receive patients. If the QRF is committed, the BDOC will direct the Air Liaison Officer (ALO) to alert the air support operations center (ASOC) for possible air support. The BDOC will alert the fire support coordinator (FSCOORD) to establish a no-fire area around the QRF once it is deployed. The QRF commander reports location of his forces to

the BDOC. The QRF commander must approve any requests for indirect fires.

## **Consequence Management**

Consequence Management (CM) is the act of getting operations to a functional state after an incident has occurred. The operations section will define the consequences of the incident and develop courses of action. A solid foundation for planning a coordinated, rapid response centers on the following essential activities:

- Evaluation of emergency plans and procedures, resources, exercises, command and control infrastructure and information systems
- Development of guidance and policy, information systems and decision tools, technologies for agent detection and identification, dispersion and consequence modeling and remediation technologies
- Training through lectures, discussions, sand table exercises, role playing as controllers, evaluators and mock media

## **Command Considerations for Consequence Management**

- Response route considerations:
  - Approach from uphill/upwind if possible
  - Avoid choke points
  - Designate rally points
- Identify safe staging locations for incoming units
- Ensure the use of personal protective equipment (PPE) and personnel accountability
- Continually assess security
- Evaluate the need for specialized units (EOD, military working dogs, etc.)
- Treat every incident as a crime scene:
  - Everything at the site is potential evidence to include unexploded devices, portions of devices, victim's clothing and containers
  - Record all movements in and out of the incident site
  - Create a buffer zone

## **On-Scene Assessment**

- Debris field
- Mass/first responder casualties:

- Unconscious with minimal or no trauma
- Victims exhibit salivation-lacrimation-urination-defecation-gastric emesis-miosis (SLUDGEM) and/or seizures
- Victims exhibit blistering/reddening of skin and/or difficulty breathing
- Severe structural damage without obvious cause
- Dead animals/vegetation
- Unusual odors, colors of smoke

## On-Scene Considerations

- Determine life safety threats to self/responders/victims and public
- Triage victims-ambulatory/non-ambulatory
- Identify damaged/affected surroundings (both structural and utility damage)
- Weather considerations (downwind exposure and weather forecast monitoring)
- Psychological effects (long-term stress on Service members and “fear factor”)

## Communication Systems

The subject of communications is so broad that complete coverage in this handbook is not feasible. However, this section includes basic concepts to inform and remind users about the interconnectivity and use of communications systems in supporting force protection activities. FOB force protection communications systems focus on the networks that allow voice and data communications among command posts, staffs, and critical components of force protection activities. Communications systems enable commanders and staffs to effectively manage ongoing operations. Without a reliable, redundant means of communicating threat status, intelligence, and operations, the FOB commander and staff will not have a viable, common operating picture of the situation, nor will they be able to direct actions in a timely and proactive manner.

The communications system is the Joint Forces Commander’s (JFC) principal tool to collect, transport, process, protect, and disseminate information. Given the criticality of information, the security of the communications system is paramount to ensuring the JFC can trust the information it provides.

**Planning.** Pre-execution planning is essential to the successful installation, operation, and maintenance of FOB force protection communications

systems. The force protection officer and the communications officer should be involved in the communication construction planning well in advance of execution. Their planning will drive numerous other aspects of the force protection plan as well as potentially identifying the Joint agency selected to perform communication construction.

When planning for redundant and reliable FOB communications, the communications officer and the antiterrorism/force protection officer need to know how many systems are needed, why they are needed, and the cost if they have to be acquired. They must also identify those systems which meet the needs for security, system capabilities (range, power requirements and battery life), redundant/backup systems, operator training requirements, frequency requirements, desired capabilities at the deployed location, appropriate directives from theater and higher headquarters as well as HN support and requirements for interoperability with their security forces, civil engineering or Department of Public Works (DPW).

The communications officer must develop signal operating instructions and communication plans and disseminate them to tenant and supporting units. FOB communications plans must be integrated into the Joint Communications Electronic Operating Instructions (JCEOI) to ensure deconfliction of frequencies and call signs. Additionally there must be coordination with HN, coalition forces, and transient units to ensure interoperability and communications systems effectiveness.

Commanders and force protection personnel can use the Communication Systems Planning Questionnaire (See Figure 3-3) to assist with communication planning. The following considerations should be addressed in all communications systems plans at a minimum:

**Requirements.** The actual communications systems requirement must be understood and assessed for feasibility. Requirements must be based on need - not want. Fiscal limitations may delay the acquisition of state of the art systems used by commercial and most stateside garrison organizations. The FOB force protection officer must work with the communications officer to clearly identify the requirements. They must identify equipment and network capabilities that meet the requirement and the capabilities of the units, users, and services to employ those assets.

**Security.** As previously stated, security of the systems must be paramount. Controlled access must be limited to those with a need to know, and all efforts must be taken to limit information from getting into the hands of unauthorized individuals. Removable data storage

devices should be appropriately marked and safeguarded. Access to SIPRNET and NIPRNET data systems must be controlled and users trained as to their responsibilities. Likewise, access to communications systems such as radios and telephones must be for authorized use. Without this limitation, the system will be over utilized and potentially not available for its primary purpose – communicating critical information at the critical moment.

**Power.** Planners must consider power requirements when planning their various networks. Systems that require 110/220 volt power may not be available at all times in the austere locations of a FOB. Back up generators must be available, emplaced and cut over procedures rehearsed. For systems that can rely on battery power, a stock of the appropriate batteries capable of providing 2 – 5 days worth of power must be available and must be maintained so as to be operational.

**Maintenance.** The periodic and scheduled maintenance requirement for communications systems must be reviewed prior to determining the best systems to meet the requirements. If a specific system requires contractor support, that availability must be programmed and available in the area of operations. Additionally, daily preventive maintenance must be maintained. Commanders and leaders at all levels of the force protection team must insure this is done consistently and reliably.

**Hardening.** Systems are vulnerable to attack from indirect fire and acts of terrorism. Additionally, they can be easily disrupted by construction, vehicle traffic and other non-combat related actions. Communications systems components such as cables, wires, antennas, and generators are particularly susceptible. Communications systems planners can minimize this vulnerability by planning for hardening and/or providing alternate wire/cable routes for key communications systems assets.

**Flexibility.** As in any plan, communications systems architecture must be flexible. Rigid reliance on a single means, capability or concept will be counter effective. The systems identified may have multiple uses but must be both capable and available to meet their primary mission.

**Interoperability.** FOB communications systems planners must include this capability as a key point in their planning. The capability for interoperability allows multi-functionality for a single system which both decreases the overall equipment requirement and increases

## Communication Systems Planning Questionnaire

### General

- Has the force protection officer coordinated communications requirements with the FOB Communications Systems Officer?
- Is a contingency plan in place to reroute communications should the main telephone exchange be lost?
- Has the contingency plan been integrated into and does it support the incident response measures of the installation?
- Are there provisions of the contingency plan that conflict with other provisions in the force protection plan/annex?
- Is there a redundant communications feed to the installation? What alternate system is available?
- Do all switches, PBXs, and key systems connected to the main switch have power generation and uninterruptible power supply (UPS) systems?
- Are the UPS systems maintained regularly and exercised?
- Does the power generation equipment undergo periodic load tests?
- Does the telephone switch have physical security measures in place to control access to the facility?
- Are all access points to the telephone switch cable vault and manhole covers properly secured?
- Is the installation cable distribution system designed in a looped configuration?
- Do the force protection contingency plans identify base communications capabilities and limitations?
- Is the communications center afforded adequate physical security against armed intrusion?
- Are communication systems capable of being used to transmit instructions to all key posts simultaneously in a rapid and timely manner?

### Security Forces

- What is the primary means of communication for the security force?
- Does the FOB security force have its own communications system with direct communications between security headquarters and security elements?
- Is there an auxiliary power supply for these communications systems?
- Is there sufficient equipment to maintain continuous communications with each element of the security force?
- Are there alternate means of communication available to the security force? If yes, is it comparable to the main source of communications?
- Do guards/roving personnel/perimeter monitors have communications

Figure 3-3. Communication Systems Planning Questionnaire

capability back to security forces?

- Does the security force use a duress code for emergency situations?
- Is the duress code changed at least monthly?

## **Radio Communications**

- Are proper radio procedures practiced?
- Is all communication equipment properly maintained?
- Are there at least two dedicated radio frequencies for security force use?
- Are portable radios equipped with multiple frequency capability?
- Are portable radios equipped with an automatic tilt or switch-activated duress frequency?
- Are encrypted radio systems available and in use to prevent eavesdropping or hinder signal collection by potential enemy forces?

## **Information Assurance**

- Has the force protection officer coordinated with the FOB communications officer on information assurance requirements?
- Are information assurance (IA) measures in place to prevent viruses, key loggers, spyware, and other malicious software packages from disrupting, denying, or delaying communications activities?
- Are system recovery methods and data backup systems in place in case of loss of power, data corruption, or other event in order to recover systems and data?
- Is backed-up data readily available? If not, how long does it take to make it available? To what degree does this time span to recover data hinder force protection activities?
- Have the requirements been met before authorizing foreign nationals use of the NIPRNET on U.S. information systems?
- Are information incident and intrusion reporting systems in place?
- Has the information system been accredited for use?
- Have a vulnerability assessment and risk analysis been completed for information systems that process, access, transmit, or store data?
- Do continuity of operations plans include actions to take in the event of major disruption (fire, natural disaster, bomb threat, civil disorder, etc.)?

Figure 3-3. Communication Systems Planning Questionnaire (Continued)

capabilities for users. Understanding the frequency spectrums utilized and computer/network operating system capabilities and limitations can allow enhanced interoperability within the FOB communications systems architecture. Full interoperability may not be achievable; however, full interoperability will remain a goal within the Joint community until the services identify and procure communications systems that provide the myriad of capabilities required by each specific service.

**Equipment.** Commercial off-the-shelf (COTS) land and sea-mobile radios and base stations, service-provided tactical radios and telephone systems, and computer network systems are broad names for the communications equipment usually available for FOB communications. Each Service tends to have its favorites, although there is a continuing effort to make communications systems interoperable among the services. The exact systems used are not as important as their ability to meet the minimum characteristics and capabilities and, most importantly, their ability to meet the mission.

Radio systems are normally utilized for both point to point and larger, networked means for communicating information via voice quickly and efficiently to larger quantities of organizations or individuals. The systems available either meet all encryption/security requirements or can be utilized due to their low output power which limits intercept by unauthorized personnel. Units must make the best possible use of systems that provide secure voice capabilities or comply with Data Encryption Standards (DES). As existing non-DES systems reach the end of their life cycles, units must incorporate DES into replacement systems. Units should provide land-mobile radios, base stations, and repeaters with an uninterruptible power source. Radio systems are more easily disrupted by natural and man made interference but usually provide the best means of force protection communications. Frequencies, bandwidth and range considerations must all be identified for any radio system utilized. All frequencies used must be approved and directed by the FOB communications office.

Telephone systems (COTS or service provided) provide an extremely durable and secure means of voice communication but require more robust support, maintenance and training to install, operate and maintain. Telephone systems are also normally user-to-user devices that do not allow for larger broadcasts to multiple components within the FOB. Additionally telephone systems are extremely vulnerable to maintenance malfunctions and disruption due to periodic destruction of critical cable paths by vehicular traffic and DPW operations. Care must be taken to prevent disclosure of sensitive force protection information over telephone systems that are used by HN or other non-coalition forces.



Computer networks allow for both non-secure (NIPRNET) and secure (SIPRNET) data communications. This communications can be either by email, messaging or via web. Like telephone systems, computer networks require more robust support, maintenance and training to install, operate and maintain. Network managers must be identified and properly trained and users must understand the system capabilities and limitations. The use of an operations center or operations-related collaboration web page, essentially a web bulletin board, to post and maintain large amounts of data (such as intelligence updates, task organization, upcoming missions, etc) is effective, but to ensure success, users must obtain verbal confirmation of the information.

**System Protection.** Common sense practices help protect communications systems. The key to this is user accountability. Users must be accountable for protecting communications devices entrusted to their care. The user must store devices properly to prevent damage, theft, and pilfering and ensure use is limited to those with appropriate clearances and a need-to-know. This includes proper marking and safeguarding of removable data storage devices.

The Services have three main programs which describe good practices and accountability - Operational Security (OPSEC), Communications Security (COMSEC) and Information Assurance (IA). All are essential for communications systems protection and mission accomplishment.

Basic to the OPSEC process is determining what information, if available to one or more adversaries would harm an organization's ability to effectively carry out a mission. The accumulation of one or more elements of sensitive information by adversaries could reveal classified information. The goal of OPSEC is to deny an adversary these pieces of information.

COMSEC measures and controls are taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emission security, traffic flow security, and physical security.

Information Assurance (IA) is a unified approach to protect unclassified, sensitive, or classified information stored, processed, accessed, or transmitted by information systems such as computer data networks. It is established to consolidate and focus efforts in securing that information, including its associated systems and resources, to increase the level of trust of this information and the originating source. It includes actions by communications systems planners, network managers, and system users. Service specific, theater and FOB communications offices will provide

overall policy and procedures. Commanders must initiate a program to train operators at all levels and insure that guidance is followed.

### **Mass Notification and Warning**

Mass notification is the capability to provide real-time information to all FOB personnel during emergency situations. To reduce the risk of mass casualties, there must be a timely means to notify personnel of threats and about what should be done in responding to those threats.

Implementation of an effective mass notification system requires the coordinated efforts of engineering, communications, and security personnel. Fire-protection engineering personnel are needed for the successful implementation because they bring a special expertise in life safety evaluations, building evacuation systems, and the design of public notification systems. Coordination with communications personnel is needed because every mass notification system will require the use of base communication systems.

Each FOB should prepare an implementation plan that establishes a comprehensive approach to mass notification that is acceptable to security, communications, and engineering personnel. Elements of an implementation plan include a needs assessment, requirements definition, alternatives evaluation, system selection, and implementation schedule.

**Notification Appliance Network.** A notification appliance network consists of audio speakers located to provide intelligible instructions in and around the building. An **Autonomous Control Unit** is used to monitor and control the notification appliance network and provide consoles for local operation (See Figure 3-4). Using a console, personnel can initiate the delivery of pre-recorded voice messages, provide live voice messages and instructions, and (optionally) initiate visual strobe and text message notification. The autonomous control unit will temporarily deactivate audible fire alarm appliances while delivering voice messages to ensure the messages are intelligible.

If a base-wide control system for mass notification is available, the autonomous control unit also communicates with the central control unit of the base-wide system to provide status information and receive commands and messages.

**Giant Voice System.** This system is also known as “Big Voice.” The Giant Voice system is typically installed as a base-wide system to provide a siren signal and pre-recorded and live voice messages. It is most useful

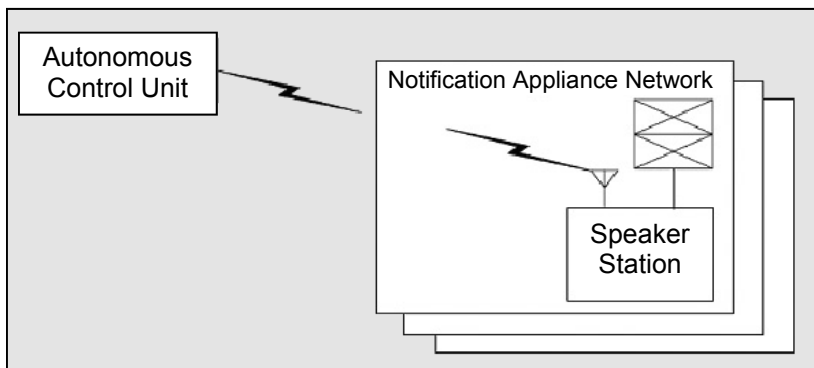


Figure 3-4. Notification Appliance Network/Autonomous Control Unit concept

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 the voice messages are generally un-intelligible. If a base-wide control system for mass notification is available, an interface to the Giant Voice system may improve the functionality of both systems.

**Exterior Based Alert Warning System.** A typical outdoor alert warning system (AWS) used by DoD and federal agencies consists of an outdoor electronic loudspeaker speaker array capable of delivering a uniform (+/- two dBc) sound pressure level (SPL) variable from 114 dBc to 126 dBc at 100 feet throughout 360 degrees of coverage. Different models ranging in size from a one-cell speaker to a ten-cell speaker configuration allow users to customize personnel alerting solutions to the requirements of the command. Systems should include standard warning tones (wail, alert, hi/lo, attack, air horn, and whoop), a pre-recorded message capability, and a real-time public address voice capability.

Regardless of speaker configuration, the system should be capable of operation at full output on battery power for 30 minutes without any alternating current (AC) power connection. Systems that can accept solar panels and wind generators in order to charge the battery back-up system are basically self-sufficient and provide excellent coverage in areas where reliable power is scarce.

A site survey is required in order to determine the cost for equipping a site with an alert warning system. The number and size of electronic loudspeakers required to adequately cover the facility will determine the cost of the system. Point of contact for safety or operational certification is Product Manager, Physical Security Equipment (PM-PSE); Telephone: (703) 704-2416, DSN 654-2416.



This page intentionally blank

# Risk Management

### Introduction

The fundamental goal of risk management is to enhance operational capabilities and mission accomplishment, with minimal acceptable loss. Risk management is a process that assists decision makers in reducing or offsetting risk (by systematically identifying, assessing, and controlling risk arising from operational factors) and making decisions that weigh risks against mission benefits. Risk is an expression of a possible loss or negative mission impact stated in terms of probability and severity. The risk management process provides leaders and individuals a method to assist in identifying the optimum course of action (COA). Risk management must be fully integrated into planning, preparation, and execution. Commanders are responsible for the application of risk management in all military operations. Risk management facilitates the mitigation of the risks of threats to the force. Threat is defined as a source of danger—any opposing force, condition, source, or circumstance with the potential to negatively impact mission accomplishment and/or degrade mission capability.

Each Service uses similar but slightly different processes. This chapter summarizes a single process to enable the Services to manage risk from a common perspective. The overview in this chapter is not an all-encompassing treatment of risk management. Readers should consult with FM 3-100.12 / MCRP 5-12.1C / NTTP 5-03.5 / AFTTP(I) 3-2.34, *Risk Management—Multiservice Tactics, Techniques, and Procedures for Risk Management* for a comprehensive treatment of the subject.

The commander has the dilemma of weighing mission requirements and force protection measures. One of his primary tools for weighing mission and protection is reconciled by assessing and balancing risk. This process forms a direct relationship between force protection and risk management. The force protection process considers three elements: planning, operations, and sustainment. Risk management enables the force protection process by using risk assessment and controls in each element. The relationship between force protection and risk management is summarized as shown in Figure 4-1.

**In *planning*, leaders conduct risk assessment and develop controls.**

**In *operations*, leaders update risk assessment and implement controls.**

**In *sustainment*, leaders continue to update assessments and adjust controls.**

Figure 4-1. Force Protection and Risk Management Relationships

## Process Overview

The risk management process involves the following (See Figure 4-2):

- Identifying threats
- Assessing threats to determine risks
- Developing controls and making risk decisions
- Implementing controls
- Supervising and reviewing

Threat Identification and Threat Assessment elements comprise the risk assessment portion of risk management. In threat identification, individuals identify the threats that may be encountered in executing a mission. In threat assessment, they determine the direct impact of each threat on the operation. Risk assessment provides enhanced awareness and understanding of the situation. This awareness builds confidence and allows timely, efficient, and effective protective measures.

Develop Controls, Make Decisions, Implement Controls, Supervise, and Review elements of the risk management process are the essential follow-through actions of managing risk effectively. Leaders weigh risk against benefits and take appropriate actions to eliminate unnecessary risk. During planning, preparation, and execution, the commander should communicate his acceptable risks to subordinates and continuously assess risks to the overall mission. Finally, leaders and individuals evaluate the effectiveness of controls and capture lessons learned.

## Risk Hazards

Hazards to FOB personnel result from previously identified threats. A hazard is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. Small-arms fire produce localized effects – bullet wounds to various parts of the body. Rocket-propelled grenades cause damage over a larger area than small-arms fire. Human injury and structural damage can

occur. Explosively-formed penetrators are primarily used to defeat armor on vehicles to injure or kill the occupants.

Weapons with effects over larger areas include rockets, artillery shells, mortars, PBIED, and VBIED. An explosive device generates the follow-

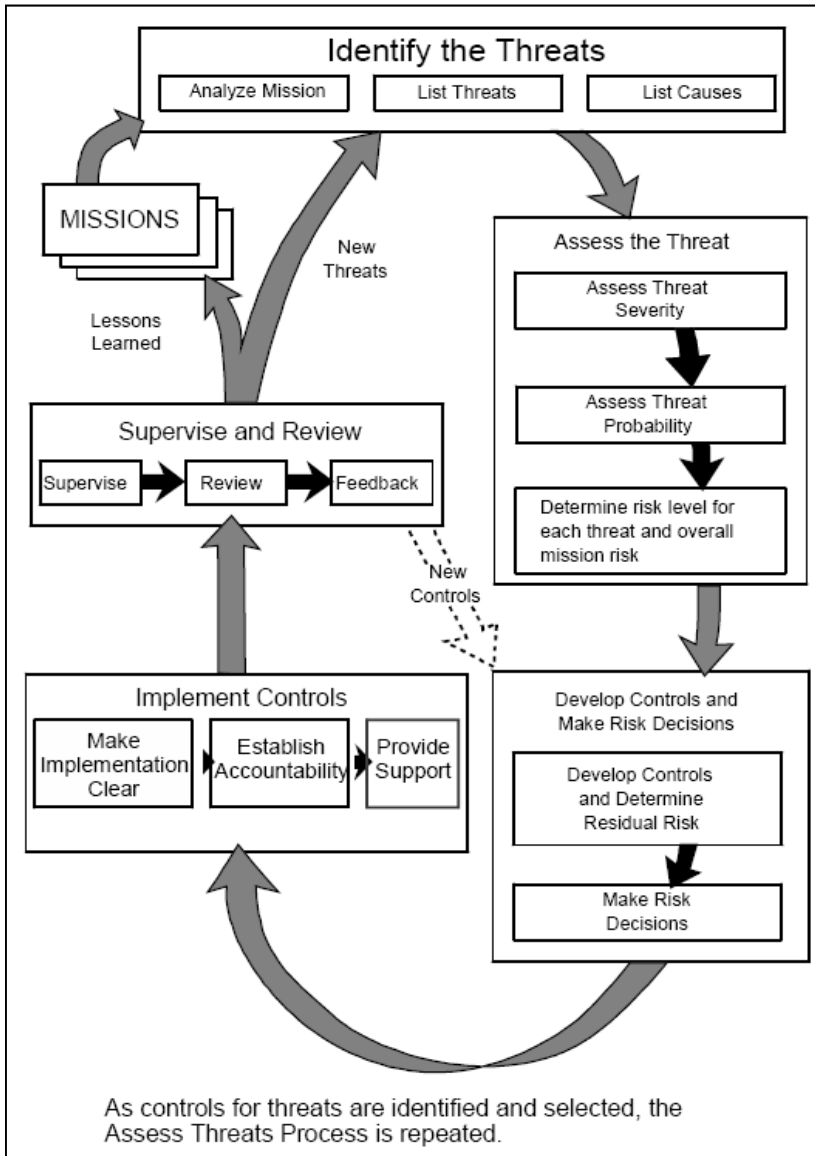


Figure 4-2. Continuous Application of Risk Management  
(from *Multiservice Tactics, Techniques and Procedures for Risk Management*)

ing *primary hazards* to personnel in fixed structures, shelters, and in the open:

**Primary fragments.** Primary fragments consist of projectiles and debris ejected at moderate to high velocities and generally low trajectories.

**Secondary fragments from barriers and structures.** Counter-mobility devices and structures near the large vehicle bomb (LVB) and entry control point (ECP) will be completely involved in the LVB explosion and will produce secondary debris as the force of the blast breaks them up. This debris will be launched at relatively low trajectories, but will have significant velocity. Some may think a concrete barrier wall is sufficient shielding from various blast or fragment effects. By itself, it is not. Fragments on the backside of a concrete wall will travel at high velocity toward anything shielded by the wall, and in turn can become hazardous shrapnel.

**Secondary debris in fixed structures.** Window glass and some structural materials such as masonry walls can fail and become debris that is hazardous to personnel occupying perimeter spaces in buildings.

**Blast effects.** The force of the explosion as it is transmitted through the air (blast) can cause injury to personnel in the open. It can pick up and translate ground debris. Structures can fail and/or collapse, generating numerous injuries and deaths. Primary blast injuries are those resulting from the impact of the overpressure wave with body surfaces. Gas-filled anatomical organs such as the lungs, middle ear, and gastro-intestinal tract are most susceptible to primary blast injuries (See Chapter 11 for more information).

*Secondary hazards* are those blast injuries resulting from flying debris and bomb fragments. These may include penetrating and blunt trauma wounds. They may be caused by bomb fragments or debris created by interaction of the blast wave with surrounding structures such as walls and counter-mobility vehicle barriers. Other injuries include those caused by the body thrown against other objects by the blast wind. Finally, additional injuries include burns, collapse/crush injuries, and toxic inhalation. Table 4-1 provides an indication of the effects of a VBIED attack.

### Process Application Guidelines

**Apply the Process in Sequence.** Each element is a building block for the next one. For example, if threat identification is interrupted to focus control on a particular threat, other more important threats may be overlooked



Table 4-1. Typical Injuries based on Distance from Blast Detonation (from AFH 10-2401, *Vehicle Bomb Mitigation Guide*)

Standoff Distance	Type of Injuries
<b>Very Near to the Detonation, Inside The Fireball</b>	Dominant lethal injury mechanisms are primary fragment penetration and/or blast lung. Eardrum ruptures are common, but not lethal. Depending upon the blast size, burns, whole-body translations, GI tract injuries, and inhalation injuries are likely, but are usually considered superfluous.
<b>Near the Detonation, Outside the fireball</b>	Dominant lethal injury mechanisms are primary fragment penetration and/or blast lung. Eardrum ruptures are common, but not lethal. Burns are unlikely with conventional high explosives. GI tract injuries are less common. If the detonation occurs in the free-field or a vented enclosure, inhalation injuries are unlikely. If the detonation occurs in a frangible structure, blunt trauma from secondary debris and/or crushing due to structural collapse may result in injuries ranging from minor to fatal in severity.
<b>Mid-Range from the Detonation</b>	Eardrum ruptures are common. In an urban environment, blunt trauma from secondary (structural) debris and penetration injuries from secondary (window) debris are likely. These injuries are not likely to be lethal, but may result in operational casualties, major disruptions to operations, and heavy loads on the medical responders.
<b>Far-range from the Detonation</b>	Glass penetration is the most likely source of injuries. These injuries are likely to be only minor to moderately severe, but may be significant operationally, may place heavy loads on the medical responders, and may have a significant psychological impact.

and the risk management process may be distorted. Until threat identification is complete, it is not possible to prioritize risk control efforts properly.

**Maintain Balance in the Process.** All parts of the process are important. If only an hour is available to apply the risk management process, the time must be allocated to ensure the total process can be completed. Spending fifty minutes of the hour on threat identification may not leave enough time to apply the other parts of the process effectively. The result would be suboptimal risk management. Of course, it is simplistic to rigidly insist that each of the parts is allocated ten minutes. The objective is to assess the time and resources available for risk management activities and allocate them to the actions in a manner most likely to produce the best overall result.

**Apply the Process as a Cycle** (Refer to Figure 4-2). Notice that “supervise and review” feeds back into the beginning of the process. When “supervise and review” identifies additional threats or determines that controls are ineffective, the entire risk management process should be repeated.

**Involve People Fully.** The only way to ensure the risk management process is effective is to involve the people actually exposed to the risks. Periodically revalidate risk management procedures to ensure those procedures support the mission.

## Tools

**Risk Management Worksheets.** Each Service has developed risk management processes that use a variety of related worksheets and tools. These worksheets attempt to streamline and document the process in a variety of ways. Describing each worksheet in detail is beyond the scope of this handbook. The main resources for these risk management worksheets are:

- Risk Level Worksheet [DA Form 7278-R]: DA Pamphlet 190-51, Risk Analysis for Army Property
- Composite Risk Management Worksheet [DA Form 7566]: FM 5-19, Composite Risk Management
- ORM Assessment (Five-Step Process): OPNAV Instruction 3500-39B, Operational Risk Management (ORM)
- Risk Assessment Code (RAC): MCO 3500-27B, Operational Risk Management (ORM)
- Six-Step ORM Process: AF Pamphlet 90-902, Operational Risk Management (ORM) Guidelines and Tools

The risk management worksheet provides a starting point to track the process of threats and risks logically. It can be used to document risk management steps taken during planning, preparation, and execution.

**Risk Assessment Matrix.** The Risk Assessment Matrix (See Figure 4-3) combines severity and probability estimates to form a risk assessment for each threat. Use the matrix to evaluate the acceptability of a risk, and the level at which the decision on acceptability will be made. The matrix may

Severity ▼		Probability ►				
		Frequent	Likely	Occasional	Seldom	Unlikely
		A	B	C	D	E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L

**Risk Definitions**

**E - Extremely High Risk:** Loss of ability to accomplish the mission if threats occur during mission. A frequent or likely probability of catastrophic loss (IA or IB) or frequent probability of critical loss (IIA) exists.

**H - High Risk:** Significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if threats occur during the mission. Occasional to seldom probability of catastrophic loss (IC or ID) exists. A likely to occasional probability exists of a critical loss (IIB or IIC) occurring. Frequent probability of marginal losses (IIIA) exists.

**M - Moderate Risk:** Expected degraded mission capabilities in terms of the required mission standard will have a reduced mission capability if threats occur during mission. An unlikely probability of catastrophic loss (IE) exists. The probability of a critical loss is seldom (IID). Marginal losses occur with a likely or occasional probability (IIIB or IIIC). A frequent probability of negligible (IVA) losses exists.

**L - Low Risk:** Expected losses have little or no impact on accomplishing the mission. The probability of critical loss is unlikely (IIE), while that of marginal loss is seldom (IIID) or unlikely (IIIE). The probability of a negligible loss is likely or less (IVB through IVE).

Figure 4-3. Risk Assessment Matrix

also be used to prioritize resources, to resolve risks, or to standardize threat notification or response actions. Severity, probability, and risk assessment should be recorded to serve as a record of the analysis for future use. Severity and probability definitions are shown in Tables 4-2 and 4-3 respectively.

Table 4-2. Risk Severity Categories

Category	Definition
CATASTROPHIC (I)	Loss of ability to accomplish the mission or mission failure. Death or permanent disability. Loss of major or mission-critical system or equipment. Major property (facility) damage. Severe environmental damage. Mission-critical security failure. Unacceptable collateral damage.
CRITICAL (II)	Significantly degraded mission capability, unit readiness, or personal disability. Extensive damage to equipment or systems. Significant damage to property or the environment. Security failure. Significant collateral damage.
MARGINAL (III)	Degraded mission capability or unit readiness. Minor damage to equipment or systems, property, or the environment. Injury or illness of personnel.
NEGLIGIBLE (IV)	Little or no adverse impact on mission capability. First aid or minor medical treatment. Slight equipment or system damage, but fully functional and serviceable. Little or no property or environmental damage.

Table 4-3. Probability Definitions

Element Exposed	Definition
<b>FREQUENT (A) Occurs very often, continuously experienced</b>	
Single item	Occurs very often in service life. Expected to occur several times over duration of a specific mission or operation.
Fleet or inventory of items	Occurs continuously during a specific mission or operation, or over a service life.
Individual	Occurs very often. Expected to occur several times during mission or operation.
All personnel exposed	Occurs continuously during a specific mission or operation.
<b>LIKELY (B) Occurs several times</b>	
Single item	Occurs several times in service life. Expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs at a high rate, but experienced intermittently (regular intervals, generally often).
Individual	Occurs several times. Expected to occur during a specific mission or operation.
All personnel exposed	Occurs at a high rate, but experienced intermittently.
<b>OCCASIONAL (C) Occurs sporadically</b>	
Single item	Occurs some time in service life. May occur about as often as not during a specific mission or operation.
Fleet or inventory of items	Occurs several times in service life.
Individual	Occurs over a period of time. May occur during a specific mission or operation, but not often.
All personnel exposed	Occurs sporadically (irregularly, sparsely, or sometimes).

[Table 4-3 continues on page 4-10]

Table 4-3. Probability Definitions (Continued)

SELDOM (D) Remotely possible; could occur at some time	
Single item	Occurs in service life, but only remotely possible. Not expected to occur during a specific mission or operation.
Fleet or inventory of items	Occurs as isolated incidents. Possible to occur some time in service life, but rarely. Usually does not occur.
Individual	Occurs as isolated incident. Remotely possible, but not expected to occur during a specific mission or operation.
All personnel exposed	Occurs rarely within exposed population as isolated incidents.
UNLIKELY (E) Can assume will not occur, but not impossible	
Single item	Occurrence not impossible, but can assume will almost never occur in service life. Can assume will not occur during a specific mission or operation.
Fleet or inventory of items	Occurs very rarely (almost never or improbable). Incidents may occur over service life.
Individual	Occurrence not impossible, but may assume will not occur during a specific mission or operation.
All personnel exposed	Occurs very rarely, but not impossible.

(The blank matrix below is for use in conducting a local risk assessment)

-----

Severity ▼		Probability ►				
		Frequent	Likely	Occasional	Seldom	Unlikely
		A	B	C	D	E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L

## Chapter 5

# Planning

### Introduction

Joint planning involves activities associated with Joint military operations<sup>1</sup> by combatant commanders and their subordinate Joint Force Commanders<sup>2</sup> (JFCs) in response to contingencies and crises. Joint planning is an adaptive, collaborative process that can be iterative and/or parallel to provide actionable direction to commanders and their staffs across multiple echelons of command. Joint operation planning includes planning for the mobilization, deployment, employment, sustainment, redeployment, and demobilization of Joint forces.

This chapter introduces the Joint Operation Planning Process (JOPP) as an analytical process that produces a plan or order. While Joint planning often focuses on strategic assets and objectives, the process is flexible enough to be used at all levels of operation. A thorough discussion of JOPP can be found in Joint Publication 5-0, *Joint Operation Planning*.

The use of JOPP illustrates the planning process, and the types of information required for development of a force protection plan or annex. Each Service has also developed a process to guide their planning activities (the U.S. Army, for example, uses the Military Decision Making Process outlined in its Field Manual 5-0, *Planning and Orders Production*). This chapter does not advocate one model or process over another since the key elements of plan development—analyze the mission, develop courses of action, select a course of action, and publish orders—are common to all planning models. Instead, the JOPP, a Joint service product and therefore applicable to all Services, is used here as a framework for force protection planning.

---

1. Joint Operation is a term used to describe military actions conducted by Joint forces. The term is also used by Service forces in relationships (for example, support, coordinating authority) which, of themselves, do not establish Joint forces.

2. Joint Force Commander (JFC) is a general term applied to a Combatant Commander, Subunified Commander, or Joint Task Force Commander authorized to exercise combatant command (command authority) or operational control over a Joint force. A JFC may or may not be a FOB commander. However, planning principles would apply to both commands unless indicated otherwise.

## Planning Factors

Early identification of force protection<sup>3</sup> and security requirements is essential to the FOB planning effort. Addressing force protection and security concerns early helps to ensure that site location and layout are compatible with security operations and mission accomplishment. Early development of force protection and security requirements also helps reduce both construction and manpower costs and ensures adequate protection of personnel and assets. It is easier and more cost effective to establish security measures during the planning process than it is to apply force protection and security requirements, after the fact.

The key to effective planning, design and development of FOB force protection requirements is a partnership between force protection/security planners and engineers. This partnership helps to ensure the development of integrated protective measures and security procedures that are consistent with FOB design.

Force protection planning should also be incorporated into the framework of master planning. Master planning provides an integrated strategy for construction and maintenance of required facilities at the best possible cost. The incorporation of force protection and security concerns into the master planning process ensures cost-effective protection of personnel and assets. Master planning requires regular coordination through various force protection working groups.

Proper site selection and effective FOB layout will help to accomplish the objectives of force protection (See Chapter 6). Planners and designers can help accomplish these objectives by considering the following functional elements of the FOB security system when evaluating potential sites and design layout:

**Deter.** Do the location and layout of the FOB present a hardened image to an aggressor, one that will discourage an attack?

**Delay.** Do the location and layout of the FOB make use of the terrain and natural barriers to impede intruders in their efforts to reach their objective?

**Detect.** Do the location and layout of the FOB facilitate the detection of possible threats and attempts at unauthorized entry?

**Assess.** Do the location and layout assist security personnel in assessing the intentions of an unauthorized intrusion or activity?

**Defend.** Do the location and layout assist personnel in defending

---

3. Force Protection is preventive measures taken to mitigate hostile actions against DoD personnel, resources, facilities, and critical information. See Chapter 10 for more information.



against vehicle-borne improvised explosive devices (VBIEDs) and rockets, artillery and mortars (RAMs) by allowing use of natural barriers, standoff, dispersion, compartmentalization, clear fields of fire, etc.?

## Joint Operation Planning Process

The Joint Operation Planning Process (JOPP) supports planning at all levels and for missions across the range of military operations. It applies to both supported and supporting JFCs and to Joint force component commands when the components participate in Joint planning. The process is designed to facilitate interaction between the commander, staff, and subordinate HQ throughout planning. The JOPP helps commanders and their staffs organize their planning activities, share a common understanding of the mission and commander's intent, and develop effective plans and orders.

The JOPP is an orderly, analytical planning process, which consists of a set of logical steps to analyze a mission; develop, analyze, and compare alternative COAs; select the best COA; and produce a plan or order (See Figure 5-1). The steps below are summarized from Joint Publication 5-0, *Joint Operations Planning*, pp. III-19 – III-50.

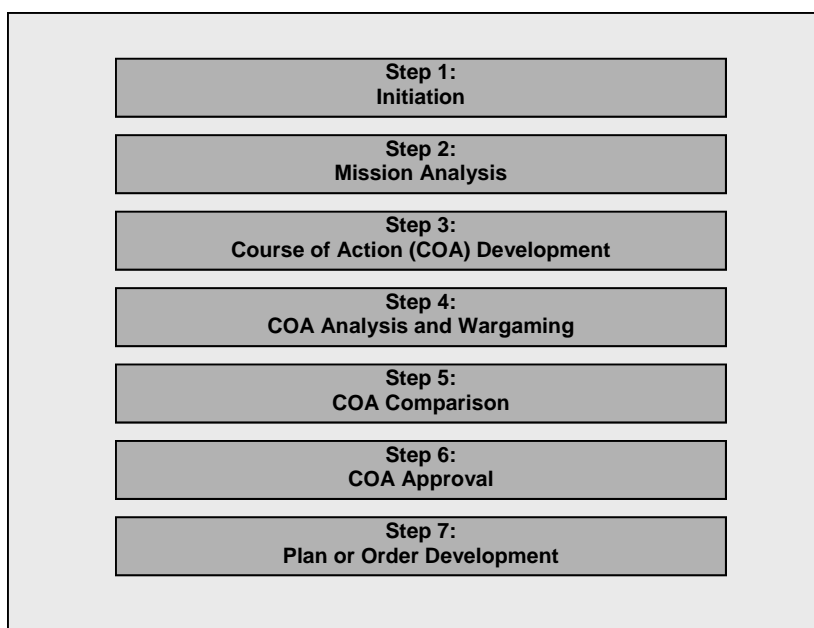


Figure 5-1. The Joint Operation Planning Process (JOPP)  
(from JP 5-0, *Joint Operations Planning*)

**Step 1: Planning Initiation.** The JOPP begins when an appropriate authority recognizes a potential for military capability to be employed in response to a potential or actual crisis. Whether or not planning actually begins here, the CCDR may act within approved rules of engagement (ROE) in an immediate crisis.

**Step 2: Mission Analysis.** Mission analysis drives the JOPP. This purpose of this process step is to review and analyze orders, guidance, intelligence, and other information in order for the commander, planning team, and staff to gain an understanding of the situation and to produce a restated mission statement for the commander's approval.

**Step 3: Course of Action (COA) Development.** Planners use the mission statement, commander's intent, and planning guidance to develop multiple COAs. Then they examine each prospective COA for validity by ensuring adequacy, feasibility, acceptability, and completeness with respect to the current and anticipated situation, the mission, and the commander's intent.

**Step 4: COA Analysis and Wargaming.** COA analysis involves a detailed assessment of each COA as it pertains to the adversary and the operational environment. Each friendly COA is wargamed against selected adversary COAs. This step assists planners in identifying strengths, weaknesses, and associated risks, and in assessing shortfalls for each prospective friendly COA. Wargaming also identifies branches and potential sequels that may require additional planning. Short of execution, COA wargaming provides the most reliable basis for understanding and improving each COA. This step also allows the staff to refine its initial estimates based on additional understanding that is gained from the analysis.

**Step 5: COA Comparison.** COA comparison is an objective process whereby COAs are considered independently of each other and evaluated/compared against a set of criteria that are established by the staff and commander. The goal is to identify the strengths and weaknesses of COAs so that a COA with the highest probability of success can be selected or developed. The commander and staff develop and evaluate a list of important criteria or governing factors, consider each COA's advantages and disadvantages, identify actions to overcome disadvantages, make final tests for feasibility and acceptability, and weigh the relative merits of each.

**Step 6: COA Approval.** All retained friendly COAs are evaluated against established criteria and against each other, ultimately leading to a staff recommendation and the commander's decision.

**Step 7: Plan or Order Development.** The staff uses the commander's COA decision, mission statement, commander's intent, and guidance to develop plans and/or orders that direct subordinate actions. Plans and orders serve as the principal means by which the commander expresses his decision, intent, and guidance.

Transition is the orderly handover of a plan or order to those tasked with execution of the operation. It provides staffs with the situational awareness and rationale for key decisions necessary to ensure that there is a coherent transition from planning to execution. The process, however, does not end here—the process is continuous. Staffs maintain running estimates that allow for plans and orders refinement. The planning staff continues to examine branches and sequels to plans and orders.

## Resourcing

As unit personnel make plans for any operation, competing requirements make demands on resources. Examples of competing requirements are weapons systems, communication systems, force protection needs, logistics support, and other mission-essential equipment. Resources are time, funds, personnel, existing contractor support, existing equipment and material, and other items and assets used to accomplish the mission. A shortage of any of these resources generally results in a need for some form of contracting to meet the mission and fulfill necessary requirements.

Each requirement has a cost associated with it, either of money or other resources, which may or may not be in the budget or operations plan. If proper pre-planning is performed, commanders and senior leaders will have a budget and can purchase necessary supplies or services through contracting to augment available resources and fulfill these requirements. Keep in mind, however, that the needs dictated by a requirement will be unique to each situation and will constantly change.

The Defense Acquisition University developed *Contingency Contracting: A Joint Handbook (VFY 08-01 JAN 08)* as a comprehensive resource for contracting activities and operations. It includes current guidelines, requirements, and funding thresholds. The book is available at [https://acc.dau.mil/docs/jcc/jcc\\_handbook.zip](https://acc.dau.mil/docs/jcc/jcc_handbook.zip). Be advised this is a very large file (580 MB) so plan downloads accordingly.

## Base Defense Plan

The base defense plan is necessary for the development and implementation of a comprehensive, integrated protection program. The plan should compile specific measures taken to establish and maintain an effective

program. The FOB plan should accomplish the following:

- Provide a clear, concise mission statement
- Convey the FOB commander's intent
- Provide tasks and activities, constraints, and coordinating instructions
- Permit subordinate commanders to prepare supporting plans
- Focus on subordinate's activities
- Promote initiative, or at least, not inhibit it
- Include annexes/appendices (if required) in order to expand the information not readily incorporated elsewhere

The plan itself should not be an end state. Instead, the plan should focus efforts to adequately plan and resource all aspects of the FOB defense mission. A sample plan template is shown in Figure 5-2. This template is taken from JP 3-10, *Joint Security Operations in Theater*.

(In Joint Operation Order [OPORD] Format)
SECURITY CLASSIFICATION
Copy No. _____
Issuing Headquarters
Place of Issue
Message Reference Number
Type and Serial Number of Operation Order.
References:
a. Maps or Charts
b. Time Zone. (Insert the time zone used throughout the order)
Task Organization. (List this information here, in paragraph 3, or in an annex if voluminous. The organization for defense should clearly specify the base units providing the forces for each defense element. Attached or transient units and the names of commanders should be included. The defense requirements of US, HN, and other civilian organizations quartered on the base also should be identified. Their capabilities to assist in the defense must be determined and integrated into the base defense plan.)
1. <b>Situation.</b> (Under the following headings, describe the environment in which defense of the base will be conducted, in sufficient detail for subordinate commanders to grasp the way in which their

Figure 5-2. Sample Base Defense Plan  
(From JP 3-10, *Joint Security Operations in Theater*)

tasks support the larger mission.)

a. **Enemy Forces.** (Describe the threat to the base, to include the composition, disposition, location, movements, estimated strengths, and identification and capabilities of hostile forces, including terrorist organizations.)

b. **Friendly Forces.** (List information on friendly forces not covered by this operation order, to include the mission of the next higher headquarters and adjacent bases as well as units not under base command whose actions will affect or assist the defense of the base. These units may include MP or Air Force SF response forces, fire support, naval coastal warfare forces, special operations forces, engineers, NBC decontamination or smoke units, EOD, HN military or police organizations, and public and private civilian organizations of both the United States and HN.)

c. **Attachments or Detachments.** (When not listed in the Task Organization, list elements attached to or detached from base units and the effective times.)

**2. Mission.** (Give a clear, concise statement of the commander's defense mission.)

**3. Concept of the Operation.** (Under the following headings, describe the commander's envisioned concept of the operation.)

a. **Commander's Intent.** (The commander discusses how the development of the defense is envisioned and establishes overall command priorities. This subparagraph should provide subordinates sufficient guidance to act upon if contact is lost or disrupted.)

b. **Concept of Operation.** (Briefly describe how the commander believes the overall operation should progress. Define the areas, buildings, and other facilities considered critical, and establish priorities for their protection.)

(1) **Phasing.** (Set forth, if necessary, the phases of the operation as they are anticipated by the commander.)

(2) **Maneuver.** (Describe the organization of the ground defense forces, the assignment of elements to counter standoff and penetrating attacks to include the base boundary patrol concept of operation and establishment of a defense with primary, alternate, and supplementary defensive positions, as well as reaction force responsibilities. Describe the purpose of counterattacks and set work priorities.)

(3) **Fires.** (State plans for employing supporting fires, such as mortars and other indirect fire assets, smoke, and aviation sup-

Figure 5-2. Sample Base Defense Plan (continued)

port.)

c. Tasks for Subordinate Elements. (If not previously described, this and succeeding subparagraphs should set forth the specific tasks for each subordinate defense element listed in the Task Organization.)

d. Reserve. (The next-to-last subparagraph of paragraph 3 contains instructions to the base's mobile reserve.)

e. Coordinating Instructions. (Always the last subparagraph of paragraph 3. Contains those instructions applicable to two or more elements or to the command as a whole.)

(1) Control Measures. (Define and establish restrictions on access to and movement into critical areas. These restrictions can be categorized as personnel, materiel, and vehicles. Security measures also may be outlined here.)

(a) Base Boundary. (Define and establish the base boundary as coordinated with the area commander. Include a description of plans to cope with enemy standoff attacks.)

(b) Personnel Access. (Establish control pertinent to each area or structure.)

1. Authority. (Give authority for access.)

2. Criteria. (Give access criteria for unit contractor personnel and local police and armed forces.)

3. Identification and Control

a. (Describe the system to be used in each area. If a badge system is used, give a complete description to disseminate requirements for identification and control of personnel who conduct business on the base.)

b. (Describe how the system applies to unit personnel, visitors to restricted or administrative areas, vendors, contractor personnel, and maintenance and support personnel.)

(c) Materiel Control Procedures

1. Incoming

a. (List requirements for admission of materiel and supplies.)

b. (List special controls on delivery of supplies to restricted areas.)

2. Outgoing

Figure 5-2. Sample Base Defense Plan (continued)

- a. (List required documentation.)
  - b. (List special controls on delivery of supplies from restricted areas.)
  - c. (List classified shipments.)
- (d) Vehicle Control
  - 1. (State policy on registration of vehicles.)
  - 2. (State policy on search of vehicles.)
  - 3. (State policy on parking.)
  - 4. (State policy on abandoned vehicles.)
  - 5. (List controls for entering restricted areas.)
- (e) Train Control
  - 1. (State policy on search of railcars.)
  - 2. (State policy on securing railcars.)
  - 3. (State policy on entry and exit of trains.)
- (2) Security Aids. (Indicate the manner in which the following security aids will be implemented on the base.)
  - (a) Protective Barriers
    - 1. Definition.
    - 2. Clear zones.
      - a. Criteria.
      - b. Maintenance.
    - 3. Signs.
      - a. Types.
      - b. Posting.
    - 4. Gates.
      - a. Hours of operation.
      - b. Security requirements.
      - c. Lock security.
      - d. Protective lighting system. (Use and control, inspection, direction, actions during power failures, emergency lighting.)
  - (b) Intrusion Detection System
    - 1. Types and locations.

Figure 5-2. Sample Base Defense Plan (continued)

2. Security classifications.
3. Maintenance.
4. Operation.
5. Probability of Detection
  - a. Limitations.
  - b. Compensating measures.
  - c. Redundant capabilities.

(c) Communications

1. Types.
  - a. Primary.
  - b. Alternate.
2. Operation.
3. Maintenance.
4. Authentication.

(3) Interior Guard Procedures. (Include general instructions that apply to all interior guard personnel, fixed and mobile. Attach detailed instructions such as special orders and standing operating procedures as annexes. Ensure that procedures include randomness.)

(a) Composition and organization. (NOTE: In security and support operations environment, the interior guard may be a contracted civilian security force.)

- (b) Tour of duty.
- (c) Essential posts and routes.
- (d) Weapons and equipment.
- (e) Training.
- (f) Military working dogs.
- (g) Method of challenge.
- (h) Alert force.

1. Composition.
2. Mission.
3. Weapons and equipment.
4. Location.
5. Deployment concept.

Figure 5-2. Sample Base Defense Plan (continued)



(4) Rules of Engagement. (Delineate the circumstances and limitations under which US forces will initiate and/or continue combat engagement with other forces encountered.)

(5) Contingency Plans. (Indicate actions in response to various emergency situations. List as annexes any detailed plans, such as combating terrorism, responding to bomb threats and hostage situations, dealing with disasters, and firefighting.)

(a) Individual actions.

(b) Alert force actions.

(6) Security Alert Status.

(7) Air Surveillance.

(8) Noncombatant Evacuation Operation Plans.

(9) Coordination with HN or Adjacent Base Plans.

(10) Measures for Coordination with Response Force and Tactical Combat Forces.

(11) Procedures for Update of This OPORD. (If the OPORD is not effective upon receipt, indicate when it will become effective.)

**4. Administration and Logistics.** (This paragraph sets forth the manner of logistic support for base defense. State the administrative and logistic arrangements applicable to the operation. If the arrangements are lengthy, include them in an annex or a separate administrative and logistics order. Include enough information in the body of the order to describe the support concept.)

a. Concept of Combat Service Support. (Include a brief summary of the base defense concept from the combat service support point of view.)

b. Materiel and Services. (List supply, maintenance, transportation, construction, and allocation of labor.)

c. Medical Services. (List plans and policies for treatment, hospitalization, and evacuation of both military and civilian personnel.)

d. Damage Control. (List plans for firefighting, clearing debris, and emergency construction.)

e. Personnel. (List procedures for strength reporting, replacements, casualty reporting, and other procedures pertinent to base defense.)

f. Civil Affairs. (Describe control of civil populations, refugees, and related matters.)

Figure 5-2. Sample Base Defense Plan (continued)

**5. Command and Signal**

a. Communications. (Give information about pertinent communications nets, operating frequencies, codes and code words, recognition and identification procedures, and electronic emission constraints. Reference may be made to an annex or to a signal operating instruction.)

b. Command

(1) Joint and multinational relationships. (Command relationships must be spelled out clearly, to include command succession. Shifts in relationships as the defense progresses, as when a response force is committed, must be specified. These relationships may be presented in chart form as an annex.)

(2) Command posts and alternate command posts. (List locations of the BDOC, BCOC, and their alternate sites, along with the times of their activation and deactivation.)

**6. Acknowledgment Instructions**

Annexes:

- A. Task Organization
- B. Intelligence
- C. Operations
- D. Logistics
- E. Personnel
- F. Public Affairs
- G. Civil Affairs
- H. Engineer Support
- J. Command Relationships
- K. Communications
- L. Force Protection
- M. Host-Nation Support
- N. CBRNE

Distribution:

Authentication:

Figure 5-2. Sample Base Defense Plan (continued)

## Chapter 6

# Site Selection and Layout

### Introduction

Site selection and design layout are controlled by competing demands and considerations, such as mission concerns, political constraints, host nation (HN) requirements and Service regulations. Additionally, force protection measures should be consciously integrated into the planning, design, and construction of FOBs. A FOB designed with force protection measures that is properly laid out and constructed will greatly reduce the amount of materials, time, and energy required to protect the FOB and will increase the FOB's defensive posture when threat levels or force protection conditions are raised. Planners and designers should be innovative and alert to additional opportunities and techniques for integrating force protection measures into FOB site location, design and layout.

### General Terrain Considerations

**Observation and Fields of Fire.** Observation is the condition of weather and terrain that permits a force to see the friendly, enemy, and neutral personnel and systems, and key aspects of the environment. Commanders evaluate their observation capabilities for electronic and optical line-of-sight surveillance systems, as well as for unaided visual observation. The highest terrain normally provides the best observation. For this reason, elevated terrain often draws enemy attention. A field of fire is the area that a weapon or group of weapons may cover effectively from a given position. A unit's field of fire is directly related to its ability to observe.

The commander's analysis of observation and fields of fire considers many factors, including the location and effect of dead space. Dead space is an area within the maximum range of a weapon, radar, or observer, which cannot be covered by fire or observation from a particular position because of intervening obstacles, the nature of the ground, or the characteristics of the trajectory, or the limitations of the pointing capabilities of the weapon. Commanders identify potential enemy and friendly engagement areas through observation and fields of fire.

**Avenues of Approach.** An avenue of approach is an air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. An avenue of approach is categorized by the size and type of force that can use it, for example, a dismounted infantry company, an

armored division, or an attack-helicopter company. A good avenue of approach allows ease of movement and good cover, concealment, observation, and fields of fire. It avoids obstacles and contributes to protection of the force by providing adequate maneuver space. Avenues of approach normally incorporate key terrain or deny its use to the enemy.

**Key Terrain.** Key terrain is any locality or area, the seizure or retention of which affords a marked advantage to either combatant. Two factors can make terrain key: how the friendly force commander wants to use it, and whether the enemy force can use it to defeat a friendly COA. Different COAs may have different key terrain associated with them. The same terrain feature may not be key for all COAs. Terrain adjacent to the AO may be key if its control is necessary to accomplish the mission.

**Obstacles.** An obstacle is any obstruction designed or employed to disrupt, fix, turn, or block the movement of an opposing force, and to impose additional losses in personnel, time, and equipment on the opposing force. Obstacles can be natural, manmade, or a combination of both. Obstacles fall into two categories: existing and reinforcing. The types of existing obstacles are natural, manmade, and military. The types of reinforcing obstacles are tactical and protective. A reinforcing obstacle's effectiveness varies with the type of force negotiating it, the fires covering it, the nature of the obstacle, and the weather.

**Cover and Concealment.** Cover is protection from the effects of fires. Concealment is protection from observation and surveillance. Terrain that offers cover and concealment limits fields of fire. Commanders consider cover and concealment to identify potential friendly and enemy locations. Look for possible assembly areas, routes, axes of movement, assault positions, ambushes, and battle positions, considering both friendly and enemy perspectives.

### Site Selection Considerations

Sites for FOBs are selected to facilitate the accomplishment of primary missions. Even so, force protection considerations must not be ignored. The location of a FOB should be chosen to make force protection easier by making an enemy attack more difficult. Planners can facilitate this effort by first conducting a terrain analysis for a proposed FOB. This analysis should consider the military aspects of a location from the standpoints of both the defenders and the enemy. Terrain analysis includes the following considerations.

## FOB Site Selection Considerations

<p><b>Threat.</b> Identify and characterize threats to the FOB. Focus not only on current threats but also on well evaluated intelligence that can be used to predict what future terrorist weapons will be like and what tactics terrorists will use. Once commanders, planners, and designers understand the threat, they can determine the best location for a FOB and can assess the ability of the FOB to survive an attack. A threat assessment is an essential element in the force protection planning process as it defines the parameters on which effective protective measures are based.</p>
<p><b>Political Considerations.</b> Consider the relationship with the local public, including the following:</p> <ul style="list-style-type: none"> <li>• <i>HN Political Climate.</i> Consider how the local situation influences FOB location, design, or land use decisions. Politically unpopular decisions may actually attract acts of aggression.</li> <li>• <i>Adjacent Landowners.</i> Assess potential problems, such as the impact of traffic restrictions on neighbors, their safety, and the way they will be inconvenienced. Identify any neighbors who require special consideration. Identify restrictions that limit public access to the area of the proposed FOB.</li> <li>• <i>Appearance.</i> Consider the local perception of the appearance of a proposed FOB. For example, public perception of a “fortress” may be either desirable or undesirable.</li> </ul>
<p><b>FOB Mission.</b> Examine the FOB’s mission, planned facilities, tenant units/organizations and the FOB’s master planning requirements to identify requirements related to site selection. Mission requirements for the proposed FOB may override other site selection considerations. Regardless, it is important to compare what the mission requires with what is available at the proposed site. Consider availability of the following:</p> <ul style="list-style-type: none"> <li>• <i>Existing Facilities.</i></li> <li>• <i>Types of Structures.</i></li> <li>• <i>Existing natural or manmade features.</i></li> <li>• <i>Types and quantity of indigenous construction materials.</i></li> <li>• <i>Available real estate and other infrastructure.</i></li> </ul>
<p><b>Dispersion and Standoff.</b> Consider dispersion and standoff requirements, for the FOB and individual structures (See Chapter 11).</p>

	<p><b>Defense in Depth.</b> Select a site that will provide defense in depth, one that requires an aggressor to negotiate a series of varied, and often alternating obstacle/barrier layers, interspersed with varying distances of open ground. A singular defensive perimeter only requires an infiltrator to penetrate one obstacle layer before reaching his goal.</p>
	<p><b>Perimeter Requirements.</b> Assess perimeter security requirements (standoff, barriers, entry control points (ECPs), lighting, etc.), and select a site that will best accommodate these requirements.</p>
	<p><b>Parking Lots and Roads.</b> Identify parking lot and road requirements that could impact security. For example, how close will vehicles be allowed to protected assets?</p>
	<p><b>Occupancy Requirements.</b> Determine space requirements and other occupancy related design constraints.</p>
	<p><b>Natural or Man-Made Vantage Points.</b> Locate FOBs away from natural or man-made vantage points. Avoid selecting a site that places the FOB adjacent to either of the following:</p> <ul style="list-style-type: none"> <li>• <i>Higher surrounding terrain or buildings that provide easy viewing of the FOB.</i></li> <li>• <i>Vegetation, drainage channels, ditches, ridges, or culverts that can provide concealment.</i></li> </ul>
	<p><b>Potential Enemy Vantage Points.</b> Situate the FOB to limit, or preferably block, an attack by direct-line-of-sight weapons from potential vantage points. Options include:</p> <ul style="list-style-type: none"> <li>• <i>Use natural or manmade obstructions, such as trees, fences, land forms, or buildings that obscure sight paths.</i></li> <li>• <i>Locate the facility at a high point, if possible, to force aggressors to fire up toward the target.</i></li> <li>• <i>Place protective surfaces so they will be struck at an angle, thus reducing the effectiveness of the attack.</i></li> </ul>
	<p><b>Natural Terrain.</b> Maximize opportunities to use natural terrain features as barriers and deflectors during attack. Depending on circumstances, natural terrain features can be either beneficial or detrimental to force protection planning.</p>
	<p><b>Enemy Hiding Places.</b> Eliminate potential hiding places near a FOB; select a site that provides an unobstructed view around a FOB, one that can maintain clear zones.</p>
	<p><b>Uncontrolled Vehicle Access.</b> Choose a FOB site away from main thoroughfares and uncontrolled vehicle access.</p>

	<b>Access Roads.</b> Minimize the number of access roads and entrances into a FOB. Design entry roads to FOBs and to individual buildings so that they do not provide direct or straight-line vehicular access to high-risk resources.
	<b>Open Space.</b> Maximize the distance between the perimeter fence and surrounding developed areas: provide as much open space (clear zone) as possible to the FOB perimeter.
	<b>Topographic Areas.</b> Avoid low-lying topographic areas that can facilitate the effects of the possible use of biological and/or chemical weapons.

## Layout Considerations

Personnel concerned with FOB layout and design and force protection/security measures must consider a multitude of issues, such as FOB operational and functional issues, HN requirements, safety, and fire protection. In general, these concerns and constraints will be unique to a specific FOB. Designers need to recognize conflicts and establish priorities during the planning stage so they will work toward appropriate and optimal solutions. Some layout considerations are similar to site selection considerations. The layout and design of a FOB should facilitate current operations; have a layered security approach; include ECPs tailored for large vehicles, personnel access, military access, or combinations; have facilities designed to support incident response and quick reaction; and should include redundant utilities, protected critical assets, and accessible protective shelters throughout the FOB (Representative tent camp layouts are shown in Appendix E). FOB layout designers should plan for the areas detailed below.

### FOB Layout General Considerations

	FOB Mission Requirements
	Tenant unit/organization mission and space requirements
	<b>Regulations.</b> Ensure that all pertinent regulations are reviewed and considered.
	<b>Critical Assets.</b> Identify assets to be protected and determine the level of protection needed against an identified threat.
	<b>Procedural or Operational Considerations.</b> Consider FOB user requirements related to operations in heightened threat conditions. Examples include: <ul style="list-style-type: none"> <li><i>Deliveries.</i> Requirements related to how and where deliveries or pickups are to be made to the FOB (for example, how to</li> </ul>

	<p><i>monitor mail, supplies, materials, trash, service, and construction vehicles).</i></p> <ul style="list-style-type: none"> <li>• <i>Restricted Areas. Requirements concerning access to restricted areas within the FOB.</i></li> <li>• <i>Access Controls. Requirements related to whom or what is to be controlled the degree of control, and where and when the controls apply (for example, checks for identification of personnel, weapons, vehicles, and packages).</i></li> <li>• <i>Mission and Functional Procedures. Requirements related to the way the user will operate the FOB, manage relationships between/ among tenant organizations, develop work schedules, identify types of operations to be performed and tenant needs.</i></li> </ul>
	<p><b>Occupancy Requirements.</b> Identify tenant unit/organization space requirements and other occupancy-related design constraints, taking into account the following factors:</p> <ul style="list-style-type: none"> <li>• <i>Available real estate and terrain.</i></li> <li>• <i>Existing natural or man-made features.</i></li> <li>• <i>Available existing facilities and types of structures.</i></li> </ul>
	<p><b>Dispersion and Standoff Requirements.</b> Maximize the distance from occupied structures to the FOB boundary (see Chapter 11).</p>
	<p>HN security requirements, restrictions, and sensitivities.</p>
	<p>Multinational force protection/security requirements and considerations.</p>
	<p>Tenant-unit force protection/security requirements and considerations.</p>
	<p><b>Financial Considerations.</b> Consider funding limitations for force protection/security requirements.</p>
	<p><b>Construction Considerations.</b> Assess the types and quantity of indigenous and other available construction materials, equipment, funding, labor, contractor support, and reverse-engineering considerations.</p>
	<p><b>Safety Considerations.</b> Identify egress requirements and protective measures related to fire safety.</p>
	<p><b>Ammunition Storage.</b> Determine early in the planning stage where to locate ammunition storage points or temporary ammunition holding areas, observation posts, ECPs, overwatch positions, and quick-reaction force, fire, security, and personnel stations.</p>



**Shelters and Bunkers.** Ensure that survivability/defensive positions and protective shelters/bunkers are strategically located to benefit FOB personnel.

## Perimeter Security Considerations

**Layered Defense.** Design a layout that incorporates the concept of a layered defense in depth. Incorporate perimeter security devices (barriers, ECPs, lighting, intrusion detection and surveillance systems (IDS), access control equipment, etc.). Incorporate ECP design considerations located in Chapter 13.

**FOB Design.** Design the FOB perimeter to do the following:

- *Provide an adequate blast standoff distance for a VBIED.*
- *Limit or, preferably, block all sightlines from potential vantage points, including direct line-of-sight, standoff or ballistic weapons.*
- *Maximize the threat ingress/egress time across the exterior site.*
- *Enhance the possibility of visual observation of threat and threat interdiction by security personnel.*

**Perimeter Barriers.** Provide defense against attack from standoff weapons (antitank weapons, mortars, snipers, etc.) by selecting perimeter barriers that block sightlines—obstruction screens or non-critical structures, hedges, trees and shrubs.

**Access Points.** Minimize vehicle and pedestrian access points.

**Approach/Access Roads.** Eliminate lines of approach/access roads perpendicular to the FOB and entry roads that provide direct or straight-line vehicular access to the FOB or to critical assets/high-value targets.

**Vantage Points.** Eliminate potential hiding places near a FOB by providing an unobstructed view (clear zones) around the FOB.

**Standoff Zone.** Restrict parking within the standoff zone.

**Routes of Travel.** Allow for the regulation and control of the direction of traffic on the FOB, including pedestrian paths and vehicular road networks; route unauthorized, unofficial traffic away from critical assets/high-value targets and high-occupancy structures, and account for the needs of security patrols and response forces. For example, multiple approaches to critical assets should be available to minimize the predictability of routes for response forces.

### Critical Asset Considerations

	<b>Asset Location.</b> Locate critical assets in the interior of the FOB, away from the perimeter.
	<b>Visual Surveillance.</b> Deny aggressors a clear line-of-sight to critical assets from off-site; protect the asset against visual surveillance by locating the protected asset out of view of vantage points, such as adjacent high terrain or structures outside the FOB boundary.
	<b>Defensible Space.</b> Create “defensible space” around clustered, functionally compatible critical assets that have similar threat levels to reduce the area to be protected, limit access control points to multiple critical assets, and provide compact security areas. However, critical nodes, such as Joint operations center (JOC), special operations command (SOC), and communication centers should be dispersed within the enclave to prevent one indirect fire round or VBIED from destroying or disabling all areas vital to operations.
	<b>Use of Available Space.</b> Determine where available space is limited and whether asset separation or standoff distance is more important. Asset separation is more effective in mitigating the effects of an indirect fire weapon, but greater standoff distance from the perimeter provides better protection against VBIEDs.
	<b>Access Routes.</b> Locate an asset so that it is not accessible to direct or straight-line vehicular access/vehicle approach routes.
	<b>Vehicle Parking.</b> Locate parking to obtain required standoff distance from critical assets/high value targets to minimize blast effects from potential VBIEDs.
	<b>Exterior Signage.</b> Minimize exterior signage or other indications of critical asset locations.
	<b>Trash Receptacles.</b> Locate trash receptacles as far from critical assets as possible.
	<b>Vegetation.</b> Remove dense vegetation near a critical asset that could screen covert activity.
	<b>Separation Distance.</b> Provide adequate standoff and separation distance between assets to minimize collateral damage (see Chapter 11).
	<b>Structures.</b> Design structures that conceal assets, restrict access to assets, and eliminate hiding places.

## Utilities Considerations

	<b>Utility Access.</b> Provide secure access to power/heat plants, gas mains, water supplies, and electrical service. Where possible, provide underground, concealed, and protected utilities.
	<b>Utility Support.</b> Provide redundant utility systems (particularly electrical services) to support site security, personnel safety, and rescue functions.
	<b>Multiple Power Sources.</b> Provide utility systems with redundant or loop service, particularly in the case of electrical systems, or with quick connects for portable utility backup systems if redundant sources are not available. Where more than one source or service is not currently available, provisions should be made for future connections.
	<b>Public Address System.</b> Install a site-wide public address/mass notification system that extends from the interior to the exterior of structures/facilities.
	<b>Perimeter Penetration.</b> Secure all penetrations of the FOB's perimeter, including utility and maintenance penetrations, concrete trenches, storm drains, duct systems, etc. by use of screens, fences, grates, lattice work, locks on manhole covers, and install intrusion detection sensors, and overt or covert visual surveillance systems if warranted by the sensitivity of assets requiring protection.
	<b>Water Treatment and Storage.</b> Protect water treatment plants and storage facilities by securing access points and maintaining routine water testing to help detect waterborne contaminants.
	<b>Signage.</b> Minimize signs identifying critical utility complexes (power plants and water treatment plants).
	<b>Storage Tanks and Operational Facilities.</b> Locate storage tanks and operations facilities for petroleum, oil and lubricants (POL) down slope from all other facilities, and fuel tanks at a lower elevation and at the required separation distance from critical assets, occupied structures and other utility plants.
	<b>Communication Networks.</b> Decentralize the FOB's communications resources and conceal key network resources, such as network control centers, to withstand the effects of an attack.

### Occupied Structures Considerations

<b>Site.</b>	Locate high occupancy structures in the interior of the FOB, away from the perimeter.
<b>Personnel.</b>	Avoid placing large numbers of personnel in one structure.
<b>Open Space.</b>	Maximize the distance between the perimeter fence and occupied structures, providing as much open space as possible inside the fence along the FOB perimeter
<b>Structural Hardening.</b>	Incorporate structural hardening techniques (tents, temporary and permanent buildings, living areas, primary gathering facilities) in design and construction.
<b>Retrofit/Hardening Techniques.</b>	Consider the use of retrofit/hardening techniques (windows, walls, roofs, dispersion, compartmentalization) on existing facilities.
<b>Standoff Distance.</b>	Provide adequate standoff and separation distance between structures to minimize collateral damage (see Chapter 11).
<b>Windows.</b>	Minimize window area in structures to reduce the risk of casualties from glass fragmentation and to restrict observation from outside.
<b>Safety Window Frames.</b>	Securely anchor window frames and exterior doors to prevent separation as a result of blast overpressure.
<b>Doors.</b>	Construct doors that open outward.
<b>Asset Concealment.</b>	Lay out structures to conceal assets, restrict access to assets, and eliminate hiding places.
<b>Pedestrian Traffic.</b>	Design pedestrian traffic flow within structures to provide unobstructed observation of people approaching controlled areas and occupied spaces
<b>Trash Receptacles.</b>	Locate trash receptacles as far from occupied structures as possible.

### Commercial and Service Access Considerations

<b>Vehicle Delivery.</b>	Locate commercial and service vehicle delivery loading/off-load areas off-site, or designate an entry to the FOB and offload/loading area that is distant from critical assets/high-risk resources and high-occupancy structures.
<b>Signage.</b>	Provide signage that clearly marks separate entrances for deliveries, visitors and employees.
<b>Driveways.</b>	Avoid having driveways within or under facilities.

# Critical Infrastructure Assurance

## Introduction

Critical infrastructure assurance measures are implemented to assure that the FOB will maintain operations during periods of heightened security and during attacks from rockets, artillery, mortars (RAMs), improvised explosive devices (IEDs), etc. The two main objectives of critical infrastructure assurance are:

1. Protect people, physical entities and cyber systems that are survivable to ensure continuity of operations and mission success.
2. Deter or mitigate all hazards on critical infrastructure by people (terrorists, hackers, etc), by nature (hurricanes, tornadoes, etc), or by hazardous materials (HAZMAT) accidents (chemical spills).

Infrastructure protection involves the application of a systematic analytical process fully integrated into all infrastructure functions of the FOB. Infrastructure protection is a security-related, time-efficient and resource-constrained practice intended to be repeatedly used by commanders. This practice can only be effective if applied by commanders and periodically upgraded in accordance with changes in physical entities, cyber systems or the general environment. It consists of the following tasks:

- Identifying critical infrastructure or assets essential for the accomplishment of missions (fire suppression, HAZMAT containment, sewer treatment, water supply, electrical systems, and cyber systems)
- Determining the threat against FOB infrastructures
- Analyzing the vulnerabilities of FOB infrastructures
- Assessing the risk of the degradation or loss of a critical infrastructure
- Applying countermeasures where risk is unacceptable

## Identification

Critical infrastructure can be considered critical or key assets on the FOB. Several of the most important infrastructure areas that must be addressed are covered in the acronym “SWEAT-MSO (Sewer, Water, Electricity, Academics, Trash, Medical, Safety, and Other Considerations; See Figure 7-1). The SWEAT-MSO assessment simply provides a format for assessing these conditions.

**Sewer.** The sewer systems in FOBs can range from burn-out barrels in an initial construction to a municipal sanitary sewer and wastewater treatment

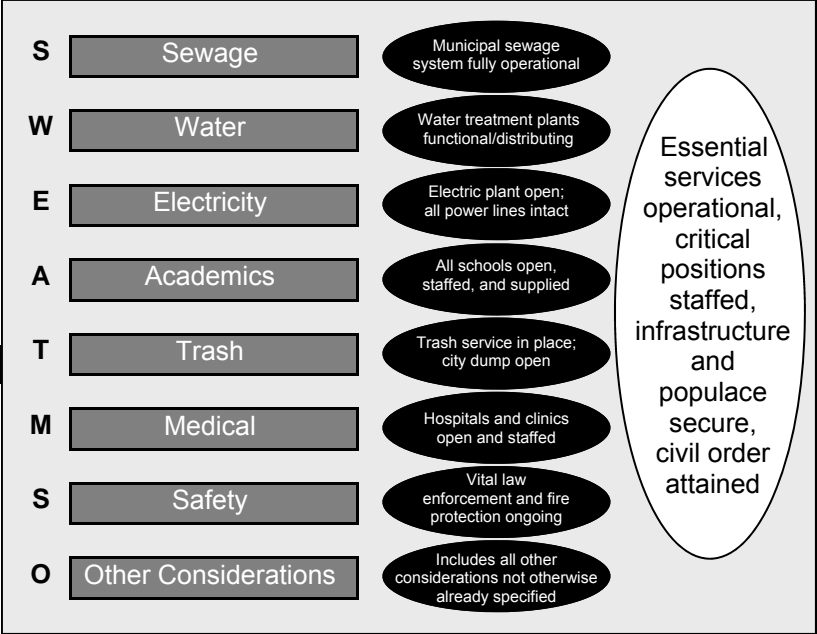


Figure 7-1. Infrastructure and Assessment Survey Model  
(From JP 3-34, *Joint Engineer Operations*)

plant like those found in small towns. Sometimes the sewer may be tied into a local municipality. Expeditionary sewer systems start with burn-out barrels, then evolve to leech fields/lagoons and then to lagoons/treatment plants. Care must be taken to insure sewage does not contribute to pollution or other environmental problems (See Figure 7-2).

**Water.** A reliable water source is critical for the successful operation of a FOB. The initial standard is bottled water, then bottle/ROWPU (Reverse Osmosis Water Purification Unit, See Figure 7-3), and then well and treatment plants as the FOB matures.

In order to sabotage the FOB’s water supply, the enemy would require (1) access to critical equipment, (2) large amounts of an incapacitating agent, and (3) knowledge of the water supply network. Some important points to consider:

- The contamination of a water supply with a biological agent that causes illness or death of victims is possible but not probable
- A successful attack will require knowledge of and access to critical nodes of the water supply network
- A successful attack will likely involve either disruption of the water



Figure 7-2. Trash and sewage pollute the city of Husseiniya. New storm drainage systems, water-quality improvements, and sewage treatment facilities are required to correct the problems (U.S. Army photo).

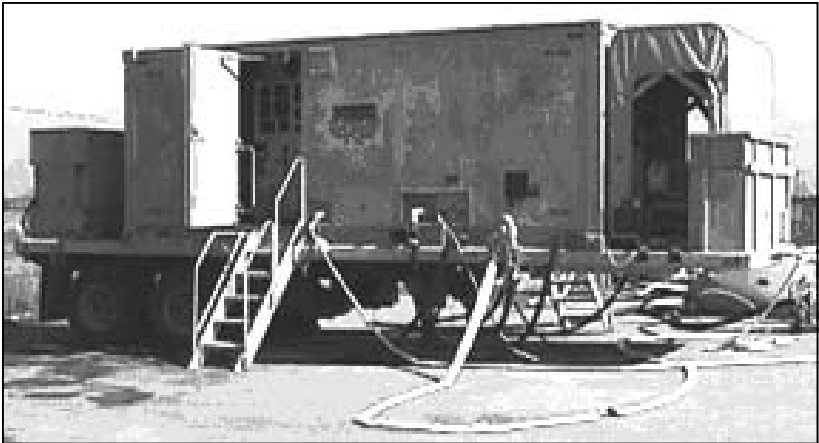


Figure 7-3. Reverse Osmosis Water Purification Unit (ROWPU)

treatment process (for instance, destruction of plumbing or release of disinfectants) or post-treatment contamination near the target

There is a great deal of interdependency between water and other infrastructure systems, the most important being the electric power sector. If

the power source is interrupted or withdrawn, it impacts the entire water system.

**Electricity.** The initial electricity is produced with organic tactical generators of the unit establishing the FOB and/or commercial generators. As the FOB matures, larger generator sets (Prime Power, see Figure 7-4) with redundant capacity may be used. In a mature theater, commercial power plants can be considered. Connecting to the local power grid is a possibility if the situation permits and the local power supply is consistent and of high quality. However in some locations power grids remain unreliable and vulnerable to sabotage. The local power grid should not be the only source of electricity. Backup generator capacity should be maintained on the FOB.

**Academics.** This includes schools, but can also include other cultural, religious, or historic facilities as well (See Figure 7-5). In certain cultures, these facilities may be regarded as equal to (or more important than) water, food, or even health services. Awareness of such facilities within a FOB AOR is therefore significant, even if the facilities will not be occupied by U.S. or Coalition forces.

**Trash.** Initially, trash in FOBs is almost always burned and buried (See Figure 7-6). As the environment becomes more permissive, trash may be disposed of off the FOB by other methods. FOBs may eventually convert to on-site incinerators. The base commander can reduce the volume of garbage for disposal by implementing reduce, reuse, recycle (RRR) programs.

**Medical, Safety, and Other Considerations.** These generally apply to larger FOBs, especially those in or around urban areas. Insure hospitals and clinics are open and staffed. Vital law enforcement and fire protection should be in-place and continuous. Include all other considerations not specified elsewhere. Refer to Joint Publication 3-57, *Civil-Military Operations*, for law enforcement considerations. Medical considerations can be found in Joint Publication 4-02, *Health Service Support*.

## **Additional Infrastructure Areas**

**Communication Systems.** Robust and redundant communication systems are key for Operational Security. Effective communications for Joint base defense present numerous challenges. All component communications systems on the base, both secure and unsecure, must be compatible in order to facilitate effective command and control (C2) of defense and security operations. The Base Defense Operations Center (BDOC), as the focal point for base defense C2, is normally the hub for the base defense





Figure 7-4. Typical Prime Power Generator



Figure 7-5. U.S. presence at a school in Afghanistan (U.S. Army photo)



Figure 7-6. Burning trash at a forward base (U.S. Air Force photo).

communications system. Existing base communications facilities are used to the maximum extent possible for base defense.

Thought should be given to the placement of communication equipment. Communication towers are often targets for mortar attacks.

- If possible, locate the towers away from populated areas so that incoming mortars that target the towers will not detonate in high-population areas
- Illuminate towers at night to warn aviators
- Maintain positive control of secure items, and conduct regular inventories to account for sensitive equipment
- Minimize use of cell phones

**Transportation.** Transportation assets include roadways (paved and unpaved), bridges, pipelines, railroad lines, harbors, and airports. Transportation infrastructure management begins with planning and design and includes asset maintenance, operation, and renewal.

In planning and design, decision makers require data to assist with evaluation of alternatives (repair, rebuild, or bypass). In maintenance, information on asset location and condition is critical to effective asset management and use. There are also security considerations throughout both phases. For vehicle access control measures, refer to Chapter 9. Internal security considerations are addressed in Chapter 8.

## Critical Infrastructure “SWEAT” Considerations

**SEWER.** Initial sewer treatment may involve hauling liquid wastes off site in sewage disposal trucks. These trucks could become prime targets for use of vehicle-borne improvised explosive devices (VBIEDs). Security should implement the following measures to protect vulnerabilities of the sewer system:

	Obtain ownership of the sewage disposal truck.
	Always keep the truck on site when not in use.
	Provide security for the driver when the sewage disposal truck leaves the FOB.
	Search the truck thoroughly before allowing it back on the FOB after wastes are dumped.
	Upgrade the sewage system to prepackaged sewage plants that can process the majority of the liquid organic wastes produced on the FOB as the FOB matures.
	Include force protection measures and emergency backup plans when contracting with outside sources, to include municipalities, for disposal service.

**WATER.** Options to consider include the following:

	Dig water wells if a local aquifer can produce the volume and quality of water demanded.
	Tie into local communities if they have adequate potable water production capabilities. In this case, ensure that local water works or utilities maintain a secure perimeter around the source and the treatment facility.
	Maintain security around critical nodes, such as pumping facilities, storage facilities, and the network of water mains and subsidiary pipes.

A water supply threat involves the release of biological organisms or toxins into the reservoir or water tank. In order for these contaminants to cause illness or death, large amounts are needed to overcome dilution by a large volume of water. The contamination of a water tower will require less agent than a reservoir but will only impact a small area. To reduce this risk, security should do the following:

	Enhance physical security of critical nodes.
	Monitor chlorine levels to ensure they are adequate.

Some potable water (either bulk or bottled water) requires transport to the FOB. These trucks are a target for contamination of water by bandits that attack the convoys. To protect the trucks, security should do the following:

Provide escorts for the trucks.

Maintain positive control of these trucks while they are convoying, entering the facility, unloading, and exiting the facility.

Protect ROWPUs and water bladders within the FOB against sabotage.

Establish several sources and locations of water so that an attack does not disrupt the water supply.

**ELECTRICITY.** Many FOBs currently have large capacity generator plants and a mixture of overhead and buried power grids. Common failures are construction related damage, surge during summer when units operate at lower efficiency, unplanned ties to the grid, and indirect fire. Security measures to be taken include the following:

Configure the electrical distribution system so that generators are compartmentalized.

Provide backup power for critical assets that can be brought online immediately if the primary source of electricity goes down.

Protect electric grids by continual monitoring, planned changes, and routine maintenance.

Develop priorities for the critical consumers (medical, command and control, food service, etc.) of electricity.

Develop and exercise a shutdown plan.

Protect generators from small arms firing and RAMs with sidewall protection and overhead cover if possible.

Protect fuel sources, power generation plants, and distribution lines.

Consider hardening for critical power nodes that drive command and control systems, medical, and food storage

**ACADEMICS.** In regards to schools and religious facilities, security should do the following:

Protect and monitor schools.

Guard religious sites and facilities as any other key terrain in order to maintain good relations with the host nation (HN).

	Monitor religious structures (steeple, minarets, etc.) for observers and as launch points for surface-to-air missiles (SAMs).
	Closely monitor chapels, morale, welfare, and recreation (MWR) areas, and any other areas where large crowds gather for suicide bombers.
<b>TRASH.</b> Security measures that should be implemented include:	
	Monitor the burn site to ensure that explosive devices are not placed in the burn pile to be detonated by the heat or by remote detonation.
	Develop tactics, techniques, and procedures (TTP's) to monitor off-post trash sites to prevent the placement of IEDs into the burn piles. The off-post burn sites should be monitored with human intelligence (HUMINT) or unmanned aerial vehicles (UAVs).
	If necessary, set up transfer points for contractors to pickup trash at independent locations or haul it to facilities with incinerators
	Inspect garbage trucks carefully for VBIEDs before they are allowed on base.
	Garbage trucks are currently a vehicle of choice for delivering VBIEDs. Keep garbage trucks on base when not in use to prevent them from being set up for a VBIED attack.

## Evaluation

The following are considerations for evaluating critical infrastructures to determine their current status and required upgrades and modifications.

**Redundant design.** The design of critical infrastructures should be such that components are similar and duplicated so that if one unit becomes unserviceable, the two or three units next to it can continue to perform at an increased output until the damaged unit is repaired or replaced. Use redundancy in design to help maintain operational readiness due to difficulty of getting repair parts in theater.

**Hardness of critical nodes.** Unprotected critical infrastructure nodes can be very vulnerable to sabotage and attack. Evaluate critical nodes for their potential as targets. The evaluation will determine the necessity of additional hardening. Add additional hardening such as overhead and sidewall protection as necessary. Other possible hardening options include relocation of node, earthen berms, chain link fence, electronic detection devices, increased standoff, compartmentalization, and security guards.

**Contingency services as backup.** Plan contingency services that are prepared to take over for primary services when required. Provide backup for

each primary utility. If generators are used to produce electricity, obtain extra generators of the same capacity for the contingency. This contingency would be fairly routine since you must also plan an excess capacity for population surge periods and downtime for maintenance. Identify alternate sources of potable water, and exercise the contingency plan for validation. Potential water sources include deep wells, local municipal water systems, ROWPU, and bottled water. Also, plan alternate methods of sewage treatment/disposal.

**Appropriate sizing.** Evaluate the existing systems for their sustainable output capacity compared to the current and anticipated usage. Utilities should be sized generously. Factors you should consider when planning for a new system or an upgrade to an existing system include the current population and usage, expected growth or decrease in population, compatibility of additions with the existing system, and the possibility of later additions also considered in the design. It is generally better to have several smaller systems than one large system. Power generation can be divided among functional areas within the FOB. Potable water production can be divided among several wells or ROWPUs.

**Tie in to public utilities.** Public utilities including, but not limited to potable water, electricity, and sewer, can be considered for use by the FOB. The condition of the HN infrastructure post combat can initially be assumed to be non-operational. Until confirmation with the local civil authorities, it can be assumed that the local infrastructure cannot support the additional burden of the FOB. As the theater matures and the local utilities become operational and reliable, they can be considered as a means for reducing funds requirements. Local public utilities have too many risks associated with them to be considered as the only source of a service. Water, sewer, and electricity are all subject to sabotage and routine outages.

### **Resources (For Additional Information)**

**Army:** *SWEAT/IR Book Version 2.1 Infrastructure Reconnaissance* (available through AKO at the General Engineering-USAES page, <https://www.us.army.mil/suite/kc/4571701>).

**Navy:** *Critical Infrastructure Protection Remediation Planning Guide* (available at <http://www.doncio.navy.mil>).

**Air Force:** AFD 10-24, *Air Force Critical Infrastructure Program (CIP)*. and AFDD 2-4.4, *Bases, Infrastructure, and Facilities* (available at <http://www.e-publishing.af.mil>).

## Chapter 8

# Security

### Introduction

The security environment requires that deployed military units, forward-based activities, and forward operating bases protect themselves against threats designed to interrupt, interfere, or impair the effectiveness of Joint operations. Base and lines of communications (LOCs) security must be properly planned, prepared, executed, and assessed to prevent or mitigate hostile actions against US personnel, resources, facilities, equipment, and information. Security areas are increasingly vulnerable to enemy forces with sophisticated surveillance devices, accurate weapon systems, and transport assets capable of inserting forces behind friendly combat formations.

Whether establishing a new FOB or occupying an existing one, military leaders should initially focus on establishing or reassessing protective measures at the perimeter of the base. Once these measures are adequate, leaders can then direct attention to measures used to protect personnel or assets located on the interior of the base. Regardless of the type of measure implemented, FOB commanders should use a team approach to develop security procedures and manage the overall FOB protection mission.

### Perimeter Security

The perimeter security system often forms the first line of defense for the FOB. The goal of perimeter security is to safeguard the FOB mission by protecting both personnel and property. This is accomplished through the prevention, detection, and response to enemy-threat tactics, to include dedicated attack, rocket, artillery and mortar attacks (RAM), vehicle-borne improvised explosive devices (VBIED), acts of terrorism, sabotage, theft, pilferage, trespass, espionage or other insurgent activity.

A properly designed perimeter security system should perform in an integrated, layered, defense-in-depth. A controlled perimeter is crucial to providing protection and should achieve the following:

- Provide adequate large vehicle bomb blast standoff distance to occupied buildings
- Limit (or preferably block) all direct-fire, standoff, or ballistic weapon sightlines from potential off-site vantage points

- Establish positive control of all personnel and vehicles entering the site
- Maximize the clear zones on the perimeter exterior to increase threat entry/exit times
- Enhance the possibility of observation and interdiction of potential threats in the area outside the perimeter
- Allow FOB occupants to detect attempts to reconnoiter or attack; warn occupants that an attack is imminent or under way; deny the enemy access to the FOB; and enhance the ability to delay and disrupt an attack.

The perimeter zone is not limited to the actual perimeter of the FOB. It can also include an area outside the perimeter from which the site would be vulnerable to VBIED attacks, direct fire and standoff weapons.

### **Rules of Engagement and Use of Force**

DoD defines rules of engagement (ROE) as “directives issued by competent military authority which delineate the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered.” ROE are commanders’ rules for the use of force. ROE determine when, where and how force shall be used. Such rules can be both general and specific (See Figure 8-1). ROE focus on four issues:

- When force may be used?
- Where force may be used?
- Against whom force should be used in the circumstances described above?
- How force should be used to achieve the desired ends?

As a result, ROE take two forms:

1. Actions a service member may take without consulting a higher authority, unless explicitly forbidden
2. Actions that may only be taken if explicitly ordered by a higher authority

ROE can be top-driven, meaning that a higher echelon commander, for instance the Commander, U.S. Central Command (USCENTCOM) establishes ROE that must be disseminated verbatim to all lower echelons. The preferred method, because it encourages lower echelon initiative, is for ROE to be top-fed, meaning that a higher-echelon commander establishes rules for immediate subordinate echelons. These subordinate echelons in turn disseminate ROE that are consistent with those of higher headquarters but tailored to the particular unit’s mission.



### Rules of Engagement Key Points

- Service members have an inherent right to self-defense
- Only the minimum essential force necessary to neutralize the threat should be used
- Any use of force should be proportional to the threat encountered
- The ROE places very few limits on the use of force, but security force personnel should only use force when absolutely necessary and should avoid collateral damage
- When in doubt, Service personnel should remember RAMP:
  - R - Return Fire with Aimed Fire.** Return force with force. You always have the right to repel hostile acts with necessary force.
  - A - Anticipate Attack.** Use force if, but only if, you see clear indicators of hostile intent.
  - M - Measure the amount of Force used,** if time and circumstances permit. Use only the amount of force necessary to protect lives and accomplish the mission.
  - P - Protect with deadly force only** human life, and property designated by your commander. Stop short of deadly force when protecting other property.

Figure 8-1. Rules of Engagement Key Points

**FOB Rules of Engagement Considerations.** Prior to drafting ROE for FOB force protection, commanders should first review DoD, Joint Staff, and COCOM ROE. In addition to the security force standing orders, personnel involved in the FOB force protection mission should be provided ROE before performing any aspect of the mission. The ROE should cover circumstances, such as how to retaliate after an attack, how to treat captured targets, and how force should be used during the operation.

### FOB Rules of Engagement Considerations

	The first rule of engagement is always the right to use force in self-defense and the commander's right and obligation to self-defense.
	ROE should evolve with force protection mission requirements, should be tailored to mission realities, and should be consistent with unit initiative.
	ROE should be flexible and designed to best support the mission through various operational phases and should reflect changes in the threat.
	Effective ROE should be enforceable, understandable, tactically sound, consistent and legally sufficient.
	Effective ROE should not assign specific tasks or drive specific tactical solutions; they should allow a commander to quickly and clearly convey to subordinate units a desired posture regarding the use of force.
	ROE need to balance two competing goals: <ul style="list-style-type: none"> <li>• The need to use force effectively to accomplish the mission objectives</li> <li>• The need to avoid unnecessary force</li> </ul>

	Excessively tight ROE can constrain a commander from performing his mission effectively.
	Excessively loose ROE can facilitate the escalation of a conflict which, while being tactically effective, can negate the political objectives that the use of force was meant to achieve.
	ROE must strike a balance between force protection and mission objectives.
	ROE should be permissive rather than restrictive.
	ROE planning should receive at least the same careful consideration as courses of action development. This objective is best guaranteed by the commander's dedicating the right amount of time for insightful planning of the ROE and on a continuous basis.
	ROE should be fully understood by operational forces. This goal can only be accomplished through training on the ROE.
	Military units strive to "train like we fight." ROE training should be no different. Understanding and application of the ROE could become a critical element in the success or failure of the mission. Therefore, it is essential that ROE training take on the same significance as any other combat skill.
	ROE never justify illegal actions. In all situations, soldiers and commanders use force that is necessary and proportional.
	Commanders at all levels should continually review the ROE to ensure their effectiveness in light of current and projected conditions in their area of operations.

## Security Forces

In conjunction with the physical security measures employed on the perimeter, the first line of defense against hostile acts on a FOB is the security force. The security force constitutes one of the most important elements of the FOB's protective mission. Security forces consist of personnel specifically organized, trained, and equipped to provide security functions for the entire FOB. Security forces also consist of personnel assigned as interior guards for specific areas or assets, who also require organization, training and equipment specific to their assigned duties. Properly used, these personnel can be one of the most effective tools in a comprehensive, integrated FOB force protection program. Regardless of the type of personnel employed, the security force should be designed to perform the following functions:

- Detect, deter and defeat insurgent attacks and acts of terrorism
- Prevent/deter theft and other losses caused by fire damage, accident, trespass, sabotage, espionage, etc.

- Protect life, property and the rights of individuals
- Enforce rules, regulations and statutes

**Security Force Considerations.** When determining the type, size and composition of the security force for a FOB, the FOB commander must address several factors critical to the security force. In all instances, the security force, regardless of size, should meet the requirement for a reaction force capability.

- Threat for the FOB
- Size and location of the FOB
- Geographic characteristics of the FOB
- FOB Mission
- Number, type, and size of restricted areas
- Use and effectiveness of physical security equipment/ measures/ barriers
- Availability of tenant unit, assigned, attached or other supporting security forces
- Installation population and composition of the FOB
- Criticality of assets being protected

Since no two FOBs have the same security requirements, it is not feasible to establish theater-wide criteria for the required number of posts. In all cases, the number of posts should be based on an analysis of security post requirements. A systems approach should be used to perform the analysis; it should not be based upon convenience. Pertinent to this approach is consideration of the following:

- Security mission being performed
- Available manpower
- Existing security measures
- Planned upgrades, such as closing of nonessential posts and the employment of mechanical and electronic physical security technology (barriers, electronic security systems, etc.)

A systems approach to determining security force requirements should include a consideration of the factors listed above. Also include, as a minimum, the items shown in the Security Force Requirements Questionnaire (See Figure 8-2).

**Security Post Requirements and Considerations.** The specific post requirements and operating procedures for the FOB should be established with the help of FOB operational and security force personnel. Security force personnel are normally deployed throughout the FOB in various operating configurations that include the following:

## Security Force Requirements Questionnaire

- What commander or staff has overall responsibility for the FOB's security force?
- What is the commander's intent for the security force?
- What security force strength and composition are needed to meet the commander's intent and mission? Are the strength and composition commensurate with the degree of security protection required?
- What is on the mission essential task list (METL) for the security force?
- What critical assets or unique systems are located at the FOB?
- Where is the security force located?
- What specialized equipment is needed for the security force?
- What forces are required to reinforce the primary security force?
- Who interfaces with these auxiliary security elements?
- What is the alert notification procedure for these elements?
- What are the rules of engagement (ROE) for the security force?
- Who authorizes direct action by security force personnel?
- Was the security force included in force protection plan development?
- What specialized training does the security force require?
- Are no-notice exercises and rehearsals conducted?
- Is specialized training for securing critical assets or unique systems provided?
- Has coordination been accomplished for patrolling areas outside the FOB?
- Have security force orders/standing operation procedures (SOP) been developed?
- Is there a review process, and does the force protection officer conduct a detailed review at least semi-annually?
- Will security force members require security clearances equivalent to the highest degree of security classification of the documents, material, etc., to which access may be required?
- Does the FOB maintain an organized and equipped Quick Reaction Force (QRF)?
- Does the QRF receive adequate training?
- Are there sufficient personnel available who could be utilized to adequately staff the QRF?
- Has consideration been given to employing manpower-saving measures, such as intrusion-detection systems, closed-circuit television, elimination of non-essential perimeter gates?
- Are there adequate visitor escort procedures established to preclude the use of security force personnel as escorts?
- Are guard assignments, times, and patrol routes varied at frequent intervals to avoid establishing routines?
- Are periodic assessments of weapons and ammunition made to determine adequacy, and are measures taken to change allowances as appropriate?

Figure 8-2. Security Force Requirements Questionnaire

**Entry Control Points (ECP)/Gates.** Since ECPs and gates typically have large manpower requirements (see Chapter 9), these posts should be limited to the minimum number required to permit expeditious flow of traffic in and out of the FOB. Operating hours for each ECP/Gate determine manning requirements. Accordingly, FOBs with a limited number of security personnel should consider limiting the operating hours of ECPs/Gates. Peak-hour augmentation requirements should be included in post-manning calculations. However, using personnel obtained temporarily from mobile posts to man fixed posts reduces emergency response capability.

**Perimeter Observation Posts (OPs).** The justification for perimeter posts is in direct proportion to the necessity for preventing unauthorized entry and the need to maintain continuous observation along the perimeter. Effective perimeter security requires a combination of physical security measures, such as physical barriers, fencing, protective lighting and electronic security systems. All of these measures should be observed and assessed continuously by security personnel (see Chapter 6). The number of perimeter posts should be based on this observation and assessment requirement.

**Restricted Area Posts.** Restricted areas are normally established to limit access to critical assets, such as a command headquarters or a communications complex. An interior guard force should be assigned the responsibility of protecting restricted areas and critical assets. The strength of the interior guard must be commensurate with the importance of the area/assets being protected and the threat.

**Mobile/Roving Patrols.** Two-person patrols are normally adequate. These patrols can be either vehicular or foot patrols and should patrol a specific area of the FOB, responding as necessary. For example, a roving patrol may be dispatched on an alarm to conduct a preliminary assessment followed by a full response from a QRF if a real threat presents itself. Roving patrols can make the defensive plan of a FOB unpredictable, while making it easier to maintain observation over a large area. However, because of their mobile nature, roving patrols cannot provide continuous observation of a specific area. Consequently, someone attempting to infiltrate a FOB can hide whenever he hears a mobile patrol approaching or sees vehicle lights or has determined the patterns to the patrols. Roving patrols can mitigate this weakness with unpredictable routes and patrol times or by stopping occasionally, turning off the vehicle and observing an area in the darkness for 15 to 20 min. At night, patrols can use night vision devices and blackout lights. Roving patrols are most effective when

integrated with fixed OPs on the FOB perimeter. The roving patrols provide immediate investigation of any suspicious activities identified by fixed OPs, provide rapid response to any hostile activities, and can inspect dead zones or other areas which are not visible from the OP. Any roving patrols outside the fence line must be coordinated with the HN prior to the patrols commencing.

**Visitor Escorts.** Full-time posts for visitor escorts manned by security force personnel should not be established (unless the FOB has the resources to do so). Rather, the unit or facility sponsoring the visitor should be responsible for escorting the visitor. The person receiving visitors should escort visitors in and out of the FOB as determined by the commanding officer and applicable orders.

**Security Force Orders/Checklists.** Also called Special Security Instructions (SSIs), Security Force Instructions (SFIs), and Special Security Orders (SSOs), security force orders or checklists describe responsibilities and authorize security force personnel to execute and enforce regulations. Therefore, the commander of each FOB should publish, sign, and maintain security force orders/checklists.

Security force checklists should be specifically written for each post and should describe the guard's duties in detail. The orders should be brief, concise, specific, written in a clear and simple language, and reviewed annually. A copy of post-specific orders should be maintained at each post. The checklists should include post-specific ROE, ROE scenarios, daily intelligence briefs, and range cards. Checklists should help guards to identify threats and to decide when to take actions not specifically spelled out in the ROE. For example, the checklist should explain procedures for initiating a base-wide alert. The orders, at a minimum, should contain the following:

- Special orders for each post which specify the limits of the post, specific duties to be performed, hours of operation, and required uniform, arms, and equipment
- Specific instructions in the application and use of deadly force and detailed guidance in the safe handling of weapons
- Training requirements for security personnel and designated posts
- Security force chain of command

**Security Force Training.** All personnel assigned duties with a security force should have received, as a minimum training in the following areas:

- The use of force, ROE, and the safe handling of firearms
- Weapons training and qualification
- Legal aspects of jurisdiction and apprehension

- Mechanics of apprehension, search, and seizure
- General and special orders and all aspects of the security force order
- Use of security force equipment
- Specific threat (for example, vehicle bomb searches, terrorism awareness, weapons of mass destruction (WMD) awareness)

Additional topics include, but are not limited to the following:

- Current FPCON and THREAT LEVEL and appropriate actions required
- Recent local trends in surveillance
- HN customs, courtesies, and sensitivities
- Basic counter surveillance techniques
- Individual protective measures
- CBRNE personal protective measures
- How to inspect vehicles, packages, work and living spaces for improvised explosive device (IEDs)
- Use of a phrase card containing key phrases (phonetically) in the HN language
- Use of emergency phone numbers and points of contact

Security force personnel, QRF, medical response, and EOD personnel all require regular refresher training for contingency operations. The general population and command structure of the FOB should also participate in regular drills which exercise reactions and operations during various threats. Some examples of exercises include:

- Missile attack
- Mortar attack
- IED detected at ECP/gate
- IED located in chow hall/dining facility
- Surveillance of installation being conducted from outside perimeter (HN coordination should be made in advance to smooth off-base travel of QRF)
- Chemical attack
- Conventional forces assault

**Security Force Equipment.** Types and quantities of equipment made available to the security force are based on available resources and the mission being performed. Situation requirements such as HN agreements, assets protection, and threat conditions also affect the choice of equipment issued to security force personnel.

Weapons and ammunition are normally standard issue items. Security force personnel should be assigned a service pistol, service rifle, or shotgun while in the performance of their duties, as determined by the FOB

commander. Additionally, machine guns, grenade launchers, etc. can be issued for use if security force personnel have received required weapons training. The possession and use of privately owned weapons by military personnel in the performance of assigned duties should be strictly prohibited.

Security force personnel should be provided with sufficient vehicles to conduct required patrols and to dispatch reaction force personnel. Security force vehicles should also be equipped with radios and configured for the safe transportation of additional passengers, including those persons apprehended or detained by security force personnel.

Reliable communications systems will aid in the establishment of the FOB force protection mission and will allow the security force to complete assigned missions. Communications equipment should be available to all posts. The type of system employed must be tailored to meet the specific needs of the FOB and the specific requirements of the security force.

## Response Forces

Response forces are an integral part of the FOB force protection mission. Response forces have three interrelated functions to perform:

1. **Deterrence.** The presence of response forces is a visible, tangible reminder of the response that would meet an intruder who attacks a FOB.
2. **Assessment.** Response forces are an essential element of intrusion detection systems (IDS). Typically, they are responsible for making an on-the-spot assessment of initial alarms or incidents.
3. **Containment.** Response forces are often the initial response force and are responsible for initial incident control and containment, as well as augmentation and more specialized functions in the event of a terrorist incident.

**Quick Reaction Force (QRF).** The QRF is responsible for providing rapid response to unusual or hostile situations. The size of the QRF may vary from a fire team to a squad size element (4 to 13 personnel). QRF personnel are usually equipped with vehicles and have a variety of weapons (for example, M-16A2s, M203s, M-2s, M60s, M240Gs, M249s, Mk 19s) and equipment (for example, night vision device (NVDs), spotlights, radios). Response times for QRFs range from 5 to 15 minutes.

**Augmentation Force.** If manning requirements exceed security force manning levels, augmentation forces must be used to complement the existing security forces. The augmentation force must be identified and fully



trained with security equipment and procedures prior to their actual employment.

### **Force Protection Condition (FPCON) Measures**

The DoD FPCON System is a progressive level of protective measures that can be implemented by all DoD components in response to terrorist threats. These guidelines are designed to assist commanders in reducing the effect of terrorist and other security threats to DoD units and activities. A complete discussion of the DoD FPCON system can be found in Appendix H of Joint Publication 3-07.2, *Antiterrorism*.<sup>1</sup>

Although generally not applicable in a combat zone, these measures can be used as a template in the development of prudent force protection measures for a FOB. In the absence of any other force protection guidance, the FPCON measures can serve as the principal means through which the prudent FOB commander can apply an operational decision on how to best guard against the threat.

### **Random Antiterrorism Measures**

Random antiterrorism measures (RAMs) change the security atmosphere of a FOB. When implemented in a truly random fashion, RAMs alter the external appearance or security “signature” of a FOB so that insurgents conducting surveillance cannot identify force protection patterns. RAMs present the insurgents with an ambiguous security profile for the FOB. The impact of RAMs is difficult to measure, but such programs introduce uncertainty for planners and organizers of insurgent attacks. RAMs provide the FOB with the following advantages:

- Variation in security routines makes it harder for terrorists to identify important assets or build detailed descriptions of significant routines or predict movement within a targeted facility or installation
- RAMs increase awareness for FOB personnel and force protection/security personnel
- RAMs reduce adverse operational impacts and unplanned economic costs when enhanced force protection measures must be maintained for extended periods

The basic approach to implementing RAMs is to identify force protection condition (FPCON) measures or other site-specific measures that can be randomly employed to supplement the measures already in place.

---

1. This information is included in Appendix B.

**Purposes of RAMs.** RAMs can be used as a tool to test which measures have higher costs to a FOB in terms of productivity than others. RAMs can help identify those measures that security personnel and the installation infrastructure are more capable of sustaining and those that will be unduly stressful on human and materiel resources.

RAMs provide security forces with training and simulation. By keeping the guard force interested and alert, RAM programs appear to increase security, even if they do so only by making the security forces more attentive to their regular assignments.

RAMs change the security atmosphere surrounding a FOB and convey an external impression of greater vigilance and awareness. RAMs may force insurgents to ponder the question “Do they know we are here, and have we been compromised?” and ask, “What is the impact of these new security practices on our ability to achieve our operational goals?” RAMs are part of a proactive and dynamic force protection program. FOB commanders should consider the following when developing and implementing RAMs.

#### **Random Antiterrorism Measures Considerations**

	RAMs are not without cost. Implementation of RAMs will consume security force and other personnel, time, energy, efforts, and resources. As with changes in the operational tempo of any organization, there is likely to be a slight increase in accidents, minor mishaps, wear and tear on materials and equipment.
	RAMs should be visible (to confuse surveillance attempts) and should involve the command as a whole, not just the security forces.
	To be effective, tenant and transient units must be fully integrated into and support the FOB RAM program. RAMs should not be limited to security force personnel only.
	RAMs should be used throughout all threat levels and should include other measures not normally associated with FPCON measures, such as command-developed measures, or locally-developed site-specific measures.
	To confuse insurgent surveillance attempts, RAMs should be implemented in a strictly irregular fashion, never using a set time frame or location for a given measure.
	Prior to implementation, local threat capabilities should be assessed and then effective RAM countermeasures identified.
	RAMs should help to mitigate FOB vulnerabilities.
	RAMs should be conducted both internally to the FOB and externally in coordination with local HN authorities.
	RAMs should be compatible and coordinated with current FOB surveillance detection and security measures.

# Access Control

## Introduction

Access control<sup>1</sup> measures are designed to identify and screen personnel, vehicles, and materials to ensure that only authorized personnel gain entry to the FOB. Access control measures can also help detect contraband and mitigate the potential for sabotage, theft, trespassing, terrorism, espionage, or other criminal activity.

Each FOB must clearly define access control measures required to safeguard the FOB and ensure mission accomplishment. FOB commanders must develop, establish, and maintain policies and procedures to control FOB access. These policies and procedures should accomplish the following:

- Use a defense-in-depth concept to provide levels of protection from the FOB perimeter to critical assets
- Determine the degree of control required over personnel, material, vehicles, and equipment entering or leaving the FOB
- Prescribe and distribute procedures to be followed during the search of persons (and their possessions) and vehicles prior to their entering or exiting the FOB and while they are on the FOB
- Specify procedures for enforcing the removal of, or denying access to, persons who threaten order, security, or discipline of the FOB
- Identify steps to be used to randomize antiterrorism measures and change schedules to reduce patterns, to visibly enhance the security profile of the FOB, and to help reduce the effectiveness of preoperational surveillance by hostile elements

To be effective, access control procedures should be designed to increase the amount of time needed to gain access to the FOB in order to allow security personnel to sound alarms and take immediate protective actions in the event of attack. Access control procedures can both delay attackers in reaching critical assets and inhibit escape from the FOB. These procedures aid in containing and resolving the incident as well as in the apprehension of the perpetrators.

---

1. In this handbook, *Access Control* refers to the **procedures** used to restrict access to a FOB. *Entry Control* refers to the **physical structures** (gates, roads, fences, barriers, etc.) that either facilitate or prevent access. The two terms are often used interchangeably. See Chapter 13 for more on entry control structures.

## Personnel Access Control

A personnel access control system should establish authority, policy, and control measures pertinent to the FOB or a protected critical asset. Access control should apply uniformly to a variety of personnel, such as visitors, vendors, contracted workers (both maintenance and support), host nationals, police, armed forces, etc. The system must also clearly establish the types of authorized identification used to verify authority and access criteria. For example, if a badge system is used, the policy should contain a complete description of acceptable badges. Access control procedures should also define personnel search procedures and methods.

**Access Control Lists.** Access control lists are essential to security. They should contain names of only those individuals specifically authorized access to a FOB or critical asset. They should be stringently controlled and continuously updated. They should never be displayed to the public. If a computerized access list system is used, the computer files used to generate such a list must be safeguarded against tampering. Personnel whose names appear on an access control list should be positively identified prior to granting access. Admission of persons other than those on the authorized access list should be approved by the FOB commander or designated representative.

**Pass-and-Badge System.** If the number of personnel requiring access to the FOB is large enough such that they can not be personally recognized by security personnel, consider using a pass-and-badge identification system. Security badges should contain a picture of the individual who has authorized access and may contain additional information about the individual. Information that should not be printed on the badge includes home address, specific work location address and telephone number, security clearance information, or information identifying the badge holder as a DoD or U.S. Government employee.

**Exchange-Pass System.** An exchange-pass identification system may be employed to ensure stringent access control for a FOB. This system involves exchanging one or more identification media (such as an ID card or pass) for another separate type of identifier (such as a badge). This system is particularly useful in controlling visitors. The process of exchanging passes is a personal one, permitting security personnel an opportunity to closely examine all persons before they enter and exit the FOB.

**Escort System.** Escorting is an effective method to control visiting personnel or contracted workers within a FOB. The escort must remain with the visitor at all times while he/she is within the FOB. Escorts should be military personnel assigned or attached to the FOB. A major objective in

escorting visitors around a FOB is to ensure that all material brought into the FOB by the visitor is searched for contraband or explosives and that no packages or other materials are left behind when the visitor departs. If local policy establishes rules so that an individual does not require an escort, the individual must meet all entry requirements for unescorted access.

## **Contract Worker/Vendor Access Control**

Contract workers/vendors may be used to operate dining facilities, collect trash, perform custodial services, and maintain utility systems on the FOB. Procedures must be established to screen the background of these personnel and control their access on FOBs. The best way to minimize the possible threat posed by contract worker/vendors is to minimize their use and avoid fraternizing with those who do work on the FOB.

**Background Investigation.** All potential contracted workers/vendors should receive a preliminary historical inquiry prior to their employment. An inquiry and thorough investigation will identify any documented history of anti-U.S. sentiment or criminal activity. Important background information for an individual includes:

- Does the contracted worker/vendor have valid identification papers?
- Does the contracted worker/vendor have any history of terrorist activity?
- Does the contracted worker/vendor have any mental or physical problems that could cause injury to other person(s)?
- Does the contracted worker/vendor have a large family whose needs exceed his financial capabilities?

**Control.** A pass and badge system coupled with an escort system is the most effective way to control contracted workers/vendors. A pass-and-badge system serves to identify and restrict access to certain areas of a FOB. Badges can be color-coded to identify the level of escort/supervision required. At the minimum, a pass-and-badge system should include the following information on all contracted workers/vendors:

- Photo
- Name
- Duty
- Title
- Badge Number
- Expiration Date
- Some unique marking which can be used to help detect counterfeit badges

Color-coded badges work best at FOBs that are divided into zones or sectors. The color of these badges should identify the specific zone or activity to which contracted workers/vendors are restricted, such as the dining facility. Badges should also identify whether or not a contracted worker/vendor has access to more than one zone. When a contracted worker/vendor is outside of his assigned area, he must be escorted.

Contracted workers/vendors should also be controlled by use of an access control list that names those contracted workers/vendors authorized access to the FOB. The access control list is most effective when used in conjunction with the pass-and-badge system described above. If photo IDs are not available, security personnel working FOB access control should have a photograph book of authorized contracted workers/vendors. Sample procedures for controlling contracted worker access to a FOB are shown in Figure 9-1.

**Contracted Worker/Vendor Uniforms.** If resources are available, it is recommended that contracted workers/vendors be issued uniforms, such as distinctive coveralls, that will serve to enhance their control and move-

**Sample Procedures for Controlling Contract Worker  
or Vendor Access to a FOB**

1. The contracted workers/vendors arrive for work at a designated ECP.
2. Security personnel verify a contracted worker's/vendor's identification against his badge, which is kept at the ECP, or a photo book and the access control list.
3. If the contracted worker/vendor has authorization for unescorted access, he is issued his photographic badge and allowed to proceed to the search area.
4. If the contracted worker/vendor requires an escort, the appropriate unit is contacted to provide an escort and verify the contracted worker's/vendor's authorization to enter the base.
5. Once the escort arrives the contracted worker/vendor is allowed to proceed to the search area.
6. If a contracted worker/vendor is not authorized onto the FOB, the individual is detained and HN security forces are contacted.
7. All badges are collected as contracted workers/vendors leave the base.
8. All badges are reconciled daily to ensure that all contracted workers/vendors have left the base and returned their badges.

Figure 9-1. Sample FOB Contractor/Vendor Access Procedures

ment. Uniforms must be controlled in a similar manner and to the same degree as badges.

**Control Officer.** A contracted worker/vendor liaison or control officer should be designated to handle all contracted worker/vendor related affairs. This officer should ensure that all contracted workers/vendors attend an indoctrination course that clearly outlines access control rules and security policies. Likewise, all U.S./coalition personnel should attend a class on the handling of and escort procedures for contracted workers/vendors. Escorts must know how to properly observe contracted workers/vendors and know the appropriate actions to take in the event of a hostile or an emergency situation.

**Parking.** FOBs that contract their support services should stipulate that workers will be transported to the site. If contracted workers/vendors are not transported to the site, off-site parking should be available. Off-site parking areas should be placed far enough away from the FOB and ECP that protective standoff is maintained.

**Packages.** The type of packages/bags that contracted workers/vendors are allowed to bring onto a FOB must be restricted. Security personnel must ensure that contracted workers/vendors leave the FOB with the same item (s) that they brought with them. Contracted workers/vendors performing custodial services should have only the necessary cleaning materials required to perform their duties. All such items and packages must be searched thoroughly to ensure that they do not contain contraband or explosives.

**OPSEC/COMSEC/INFOSEC.** Operations security (OPSEC), communications security (COMSEC), and information security (INFOSEC) are critical. U.S. personnel must guard against fraternization with contracted workers/vendors. It is wise to assume that every contracted worker/vendor is collecting information at all times. When working with or around contracted workers/vendors, personnel must be mindful of information that can easily be seen, such as items posted on bulletin boards or left on unattended desks. All mail, faxes, envelopes, and paper correspondence, including personal envelopes and correspondence, should be shredded or similarly destroyed because they can be used to gather information and possibly threaten deployed service members or their families stateside. Conversations around contracted workers/vendors should also be guarded.

## Vehicle Access Control

Entry control points (ECPs)<sup>2</sup> and facilities are usually the weakest point in a perimeter. These areas have a complex set of issues that make them extremely difficult to operate and significantly increase the exposure of those manning them to VBIEDs. Consequently, they are frequently targeted by insurgents and adversaries.

Vehicle access control procedures must address specific control measures, to include HN requirements that are to be followed at vehicle search areas, gates, and ECPs. Specific considerations for vehicle access control include:

- Vehicle/driver/passenger search requirements (random, 100 percent, incoming and outgoing, etc.)
- Methods of searching (U.S. security personnel, MWD, transmission/back-scatter x-ray, vapor sensors, etc.)
- Responsible parties (U.S. security forces, HN security, HN/responsible unit, etc.)
- Equipment requirements (lights, poles, ladders, ramps, creepers, SCBA, etc.)
- Security requirements (driver segregation, overwatch, etc.)
- Facilities requirements (overhead protection, segregation walls, blast berms, air-conditioning for MWD, etc.)

Specific procedures for vehicle searches should be established for each FOB based on the FOB mission and operational constraints and manpower, equipment, and explosive detection assets available to conduct searches. The following procedures are provided as a general discussion of techniques for vehicle searches.

**Visual Searches.** Visual searches are used to find hastily placed improvised explosive devices (IEDs) and to identify indicators of a deliberately placed IED, such as extraneous wires or altered engine components. The searcher is unlikely to find traces of a deliberately placed IED when he is using search mirrors to conduct a visual search underneath a vehicle. Mirrors provide limited thoroughness because they only allow the searcher to see the outer two feet of a vehicle's underside.

**Mechanical Searches.** Mechanical searches involve looking for deliberately placed IEDs. During a mechanical search, the searcher requires the driver and passenger(s) to open all doors, hoods, and trunk. The searcher then taps areas which should be hollow, such as doors, side panels, and

2. For convenience, ECP refers to all entry control structures, facilities, and points. See Chapter 13 for entry control design considerations.



exhaust systems to ensure they do not have something inside. The searcher also looks at the air filter, engine reservoir fluids, glove compartment, spare tire, gas tank, and electrical system to include the horn, lights, windshield wiper, and ignition wiring. A long pole or other “dipstick” should be used to probe the storage tank of tanker trucks to ensure nothing was submerged in the transported liquid.

**Military Working Dog (MWD) Searches.** MWD searches rely on the dog’s ability to detect the scent of certain explosives. In order to maintain the MWD’s skills, the dog needs to be tested regularly. Testing should incorporate explosive training aids and should be conducted without prior notification to the dog handlers. Because heat and long hours will significantly degrade the effectiveness of MWDs, they need to be kept cool and well rested.

**Package Searches.** Package searches involve examining baggage for weapons and explosives. Searchers should make the owner open all baggage, and MWDs should also check the baggage.

**Individual Searches.** Individual searches are used to check personnel for weapons, explosives, and triggering devices. All drivers and passengers should be searched prior to entering the FOB. The use of handheld metal detectors and physical searches (frisking) are effective means of conducting individual searches.

**General Guidance for Conducting Vehicle Searches.** Specific guidelines for conducting vehicle searches should be established for each FOB. During the search of a vehicle, if searchers find anything suspicious, they should follow local procedures (for example, evacuate the search area and notify explosive ordnance disposal-EOD). Searchers should look not only for the “big bomb” but also for any type of weapon, IED, or cache of explosives. A vehicle can be considered suspicious or believed to contain a suspicious item if the driver refuses to open any compartment (hood, trunk, passenger doors, glove box, or even a package).

Search the vehicle from the terrorist’s perspective. Consider and imagine where the terrorist would hide an explosive device or quantity of explosives. Common sense is an extremely valuable tool. If the vehicle is a tractor-trailer type, treat the tractor like a larger passenger vehicle. The trailer should be thoroughly searched with the explosive detector dog (EDD) and unloaded if necessary to methodically inspect all cargo. Be aware that simply inspecting the perimeter of the cargo is not thorough enough; there may be explosives hidden at the center.

The following considerations can be used as general guidance when establishing guidelines for conducting detailed vehicle searches. Personnel conducting searches should complete one search technique before starting another one.

### General Vehicle Search Considerations

	Driver brings vehicle into search area.
	Driver dismounts vehicle and opens all compartments, doors, the hood and trunk and bags in the vehicle.
	Driver and passengers are moved to a holding area. The holding area is isolated so the driver or passengers cannot see their vehicle. Here vehicle occupants are searched with portable metal detectors. If there is reasonable cause to conduct a physical search, personnel are frisked. Throughout search procedures, driver and passengers are kept under observation by an armed guard.
	MWD team searches vehicle engine compartment, trunk, gas tank, interior compartments, walls, doors, upholstery, cargo areas, and packages.
	Search team taps on doors and vehicle walls to ensure they are empty. The team swings vehicle doors to ensure they are the appropriate weight.
	Search team examines engine compartment. They look for extraneous wires, improper fluids in reservoirs (for example, gas in washer fluid reservoir), air filter replaced with wires or explosives, new components in engine, and other extraneous components (for instance, an alternator not connected to a belt).
	In the case of cargo vehicles, an MWD thoroughly sweeps the truck. Search team randomly chooses cargo items and directs driver to open them. Storage tank and side gas tanks are probed. The Mobile Search Advanced X-Ray Portable Inspection System and the Mobile VACIS - Gamma Ray Imaging System can also be used to search commercial vehicles.
	Search team directs driver to bring vehicle on top of ramp or over search pit.
	Search team examines vehicle undercarriage. They look for extraneous wires and new components check wheel wells, and ensure that the exhaust system is hollow.
	Driver and passengers re-enter vehicle and proceed through ECP.

### Vehicle Exterior Search Considerations

	Search from the bottom of the vehicle, working to the top.
	Search by “Braille” if necessary. Feel in areas that cannot easily be seen. If something is found, do not pull it out.
	Look for body repairs, freshly painted sections, anything indicating tampering with the external surface of the vehicle.
	Use a flashlight and mirror with a creeper (if possible) to carefully inspect under the vehicle.
	Check the suspension, drive train, the wheel wells, the bumpers, under the engine, and above the gas tank.
	Look for any unusual devices taped, tied, screwed, etc. to the undercarriage.
	Look for an unusually clean portion of the undercarriage, or the presence of new weld marks / bolts / screws.
	Be sure all connections are properly made (for example, the gas tank filler tube runs from the fill port to the tank, the exhaust pipe runs from the manifold the entire length of the vehicle to the muffler). Inspect the exhaust pipe for inserted objects.

### Vehicle Engine Compartment Search Considerations

	Take a minute to observe everything within view, and then start at the outermost edge (the front or side the battery is on) of the compartment and work towards the center of the vehicle.
	Look for additional wires running from the vehicle’s battery.
	Look for out-of-place or unusually clean components, devices, and/or wiring and electrical tape.
	Check under larger components, e.g., the air cleaner and fan blade shrouds, for packages or devices.
	Look for containers that may contain fuel, indicating the gas tank may contain an explosive charge.
	Look for additional wires running from the hoodlight or the absence of a bulb in the hoodlight socket.

Vehicle Trunk Compartment Search Considerations

	Take a minute to observe everything within view; then begin at the edge and inspect inward.
	Pay attention to packages/devices (alarm clocks, iron or PVC pipe) that look out of place. Inspect items normally found in a trunk (tool box, supplies, blankets and water containers, etc.).
	Look for bits of electrical tape, wire, stripped wire insulation, string, fine wire, fishing line, and/or time fuse on the floor.
	Check for hidden compartments (spare tire well, jack/tool storage, etc.).
	Check for any additional or improvised wires attached to the brake lights or rear turn signals.
	Don't forget to look in the area behind the rear seat.

Vehicle Passenger Compartment Search Considerations

	Take a minute to observe everything within view; then start at the floor and work up. Pay close attention to packages/devices (alarm clocks, iron or PVC pipe) that look out of place.
	Look for bits of electrical tape, wire, stripped wire insulation, string, fine wire, fishing line, and/or time fuse on the floor, dash, or seats.
	Check under floor mats for wires or switches.
	Use a flashlight to check under all seats for anything out of the ordinary.
	Check behind speaker grills and in ashtrays.
	Check the door panels for signs of tampering.
	Be sure the vehicle driver opens the glove box and inspect inside of it.
	Check under the dash for any loose or unusual wiring. Pay attention to any modifications done to the dash (such as extra switches with no label as to their function, or indicator lights that remain on although the vehicle is not running).
	Check the roof liner for bulges, rips, and/or repairs, indicating possible concealment of an explosive device.

**Explosive Detector Dog (EDD) Searches.** The search techniques provided below were derived from the USAF Handbook 10-2401, *Vehicle Bomb Mitigation Guide*. Although specific EDD search procedures will vary according to local FOB policy, individual MWD handler preference, and the unique abilities of individual canines, the typical approach follows five general steps:



Figure 9-2. Explosive Detector Dog Search

1. The driver exits the vehicle and opens all doors, the hood and trunk lids, any other compartments, and any packages, and is then placed in a holding area where he or she is not allowed to witness the vehicle search (the driver should also be physically searched).
2. The EDD team (the handler and the dog) proceeds directly to the downwind side of the vehicle.
3. The EDD team starts the search at a specific point and searches in a counterclockwise manner, with the handler visually guiding the EDD to search for scents along the fenders, wheel wells, hubcaps, spare tire, and bumpers (See Figure 9-2).
4. The dog is directed to search all opened compartments, vehicle seats, and floorboard.
5. The dog is directed to search any on-board packages and parcels.

**Search Techniques for Special Types of Vehicles.** Certain special types of vehicles require unique search techniques and procedures. Water/fuel tankers, cement mixer trucks, and hot-mix asphalt delivery trucks represent potential bomb platforms that may not be effectively screened with traditional MWD searches or physical inspection methods previously mentioned. The current approaches used to address these special case vehicles are outlined in the following Special Vehicle Search Considerations:

#### Special Vehicle Search Considerations

	Establish transfer stations. Use these to transfer the cargo from the “dirty” vehicle outside the perimeter to bladders, or “clean” vehicles inside the perimeter. Never let the vehicles get near the assets being protected.
	Individually search each vehicle before cargo is loaded at the origin.
	After vehicle cargo is loaded, escort the delivery vehicle to the FOB.
	Physically inspect the entire vehicle again at the FOB with search personnel and military working dogs (MWDs).

## Materiel Delivery Control

Large vehicles concealing IEDs remain one of the most serious threats to FOBs. Most of these vehicles provide bulk material or supplies to bases and are managed under direct contract. Some simple but effective techniques can provide a great deal of protection with minimal impact on the quality of support. Examples successfully used in the Iraq Theater of Operation are detailed below.

- 1. Maintain positive control of trucks at all times.** This technique is currently being employed for logistics convoys and requires vehicles to be under positive control of US forces while under contract. Food and water generally are transported using this technique.

This method is also being employed by the waste management and water contractor. The service trucks remain on the military compound when not in use and drivers are transported to the job site. If trucks exit the compound, they are escorted to trash dumps or waste disposal sites and remain under constant visual surveillance by military personnel. This method works well if combined with pulse logistics where a contract for delivery is delivered at one time to a material staging area inside the base and then the trucks are dismissed until a new contract is needed.

- 2. Maintain constant positive control of trucks** through the use of convoy escorts from loading in the supply point to delivery at the material yard. Trucks load at one time and run in convoy to the delivery point. Trucks are inspected prior to load and are under control of military personnel during the period of service. While not as good as the first technique, the overall result is the same.

- 3. Develop a material transfer point or load transfer (“trans-load”) yard** where trucks are directed to and are required to spread their load. The material yard is placed in a corner of the FOB. This technique prevents unvetted trucks from attempting to enter the FOB through one of the other truck gates or soldier gates. The trans-load yard can be used for the transfer of gravel, sand, and other construction materials. It can also be used for the trans-loading of water, liquid and solid waste, and fuels (see Figure 9-3). As the materials to be trans-loaded become more complicated the process to on and off load has to be adjusted to ensure protection of the trans-load yard workers and that the materials are carefully screened for IED hazards. This technique prevents back up of vehicles at the entry control point.

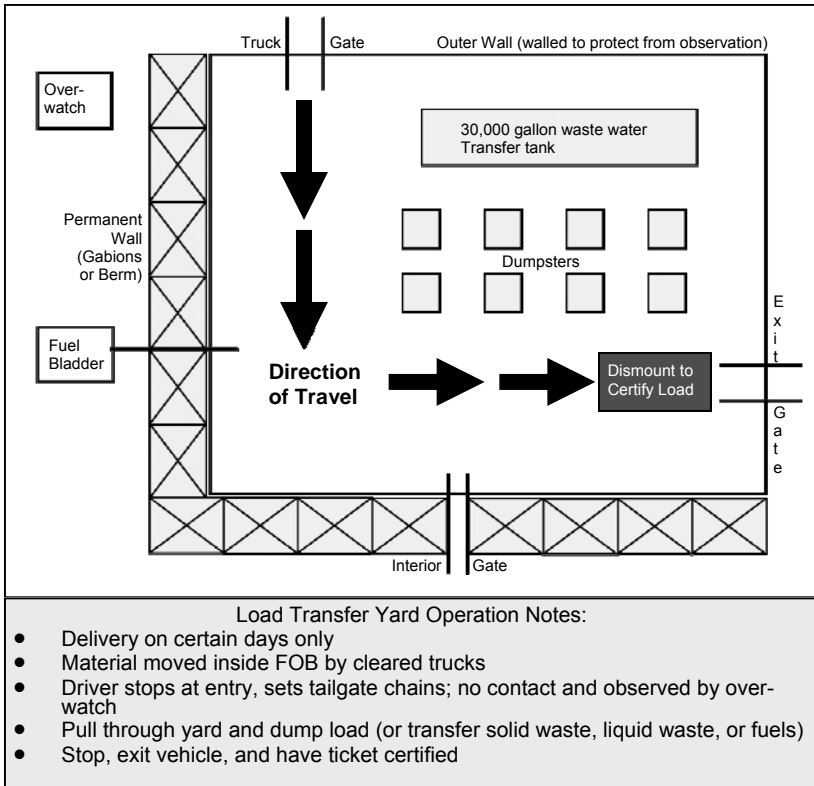


Figure 9-3. Typical Load Transfer Yard.

Planning considerations for receiving gravel or sand in the trans-load yard include:

- Use reinforced perimeter and overwatch positions
- Use signs to direct trucks through the download area and tailgate spread their load at no more than five chain links of space (This applies a thin layer of material incapable of concealing an IED)
- Move trucks forward with their beds up to a check point at the far side of the download area (Dismount driver at checkpoint and recertify load ticket) Conduct overwatch of truck under carriage from a secure position (The majority of the truck under carriage can be seen with the bed up)

These material yards should be developed by the Director of Public Works (DPW) or equivalent and may be required to support several FOBs. They may also require an MCAP Bulldozer (see Figure 9-4) to support the spreading, inspection and stockpiling at the yard. Consult your DPW engineer for specifics on tail gate spreading of material and maintaining trans-load yards.



Figure 9-4. Mine-Clearing/Armor Protection (MCAP) Bulldozer

**A fourth technique, which is the least preferred technique,** is to move trucks containing bulk materials to a holding area and have the driver dismount and move to a waiting area. The waiting areas must be visibly separated from the vehicle to be effective. Vehicles are then searched at random times with the vehicle driver unable to see the operation taking place. Mobile Vehicle and Cargo Inspection System (MVACIS), military working dogs (MWDs), or probes may be required in addition to mirrors and physical checks. This option should only be used if a trans-load area is unavailable. This method will greatly increase cycle time for material delivery.



## Chapter 10

# Protection

### Introduction

Protection is the preservation of the fighting potential of a force so the commander can apply maximum force at the decisive time and place. Protection bears significantly on every aspect of operations and sustainment. Commanders must take great pains to protect the force from attack. Adversaries opposed to US interests, or who seek to destabilize an area, will go to great lengths to expel US forces. They will employ terrorist tactics such as bombings, kidnappings, assassinations, ambushes, and raids. Commanders address force protection during planning and revise their plan as necessary during execution. This does not mean that commanders must isolate their personnel from contact with the indigenous population. Mission degradation, or even increased risk to the force, can result if commanders restrain forces from conducting prudent missions and establishing an active and capable presence in the area.

### Joint Protection Functions

Joint functions are related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct Joint operations. Functions that are common to Joint operations at all levels of war fall into six basic groups — command and control (C2), intelligence, fires, movement and maneuver, protection, and sustainment.<sup>1</sup> A number of subordinate tasks, missions, and related capabilities help define each function. The protection function focuses on conserving the Joint force's fighting potential in four primary ways:

1. active defensive measures that protect the Joint force, its information, its bases, necessary infrastructure, and lines of communication (LOCs) from an adversary's attack;
2. passive defensive measures that make friendly forces, systems, and facilities difficult to locate, strike, and destroy;
3. applying technology and procedures to reduce the risk of fratricide; and
4. emergency management and response to reduce the loss of personnel and capabilities due to accidents, health threats, and natural disasters

There are protection considerations that affect planning in every Joint operation. The greatest risk — and therefore the greatest need for protection

---

1. See Joint Publication 3-0, *Joint Operations*, for a detailed discussion of these functions.

— is during campaigns and major operations that involve large-scale combat against a capable enemy. These typically will require the full range of protection tasks, thereby complicating both planning and execution. Although the operational area and Joint force may be smaller for a crisis response or limited contingency operation, the mission can still be complex and dangerous, with a variety of protection considerations. Permissive operating environments associated with military engagement, security cooperation, and deterrence still require that planners consider protection measures commensurate with potential risks. These risks may include a wide range threats such as terrorism, criminal enterprises, environmental threats/hazards, and computer hackers. Thus continuous research and access to accurate, detailed information about the operational environment along with realistic training can enhance protection activities. Protection measures and related tasks can be found in the references shown in Figure 10-1.

Force Protection

Force protection includes preventive measures taken to mitigate hostile actions against DOD personnel (to include family members), resources, facilities, and critical information. These actions conserve the force’s fighting potential so it can be applied at the decisive time and place and incorporates the integrated and synchronized offensive and defensive measures to enable the effective employment of the Joint force while degrading opportunities for the adversary. It does not include actions to defeat the adversary or protect against accidents, weather, or disease. Force health protection (FHP) complements force protection efforts by promot-

Protection Task Area	Reference
Physical Security	JP 3-10, <i>Joint Security Operations in Theater</i>
Countering theater air and missile threats	JP 3-01, <i>Countering Air and Missile Threats</i>
Defensive Use of Information Operations (IO)	JP 3-13.3, <i>Operations Security</i>
Personnel Recovery	JP 3-50, <i>Personnel Recovery</i>
Chemical, Biological, Radiological, and Nuclear (CBRN) Defense	JP 3-11, <i>Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments</i> ; JP 3-40, <i>Combating Weapons of Mass Destruction</i>
Antiterrorism	JP 3-07.2, <i>Antiterrorism</i>
Combat Identification (CID)	JP 3-09, <i>Joint Fire Support</i>
Force Health Protection	JP 4-02, <i>Health Service Support</i>

Figure 10-1. Protection Tasks and References

ing, improving, and conserving the mental and physical well being of Service members. Force protection is achieved through the tailored selection and application of multilayered active and passive measures, within the air, land, maritime, and space domains and the information environment across the range of military operations with an acceptable level of risk. Intelligence sources provide information regarding an adversary's capabilities against personnel and resources, as well as providing timely information to decision makers regarding force protection considerations. Foreign and domestic law enforcement agencies can contribute to force protection through the prevention, detection, response, and investigation of crime; and by sharing information on criminal and terrorist organizations. Consequently, a cooperative police program involving military and civilian law enforcement agencies is essential.

Security operations protect flanks, LOCs, bases, base clusters, and JSAs. Physical security includes 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. The physical security process includes determining vulnerabilities to known threats; applying appropriate deterrent, control, and denial; safeguarding techniques and measures; and responding to changing conditions. Functions in physical security include facility security, law enforcement, guard and patrol operations, special land and maritime security areas, and other physical security operations like military working dog operations or emergency and disaster response support. Measures include fencing and perimeter stand-off space, land or maritime force patrols, lighting and sensors, vehicle barriers, blast protection, intrusion detection systems and electronic surveillance, and access control devices and systems. Physical security measures, like any defense, should be overlapping and deployed in depth.

## Principles of Defense

The basic principles of defense should always be considered during planning and design of protective systems. These systems should integrate physical protective measures and security procedures to protect assets against threats. The characteristics of integrated systems include:

**Deter.** A potential adversary who perceives a risk of being caught or failing in his mission may be deterred from attacking an asset. The effectiveness of deterrence varies with the adversary's sophistication, the asset's attractiveness, and the aggressor's objective.

**Detect.** A detection measure senses an act of aggression, assesses the validity of the detection, and communicates the appropriate information to a

response force. A detection system must provide all three of these capabilities to be effective. Detection measures at FOBs include detecting an adversary's movement using an intrusion detection system (IDS) or electronic surveillance system (ESS). Detection measures may also include access control elements that assess the validity of identification (ID) credentials and vehicle searches for explosive. These control elements may provide a programmed response (admission or denial), or they may relay information to a response force. Guards and sentries serve as detection elements, detecting intrusions and controlling access. Detection systems should also be used to communicate warnings.

**Defend.** Defensive measures protect an asset by delaying or preventing an adversary's movement toward the asset or by shielding the asset from weapons and explosives. Examples of defensive measures include:

- Delay adversaries from gaining access by using tools in a forced entry
- Prevent an adversary's movement toward an asset
- Protect the asset from the effects of tools, weapons, and explosives

Defensive measures may be active or passive. Active defensive measures are manually or automatically activated in response to acts of aggression. Passive defensive measures do not depend on detection or a response. They include such measures as blast-resistant building components and fences. Guards and sentries may also be considered as a defensive measure.

**Defeat.** Most protective systems depend on response forces to defeat an aggressor. Defense and detection systems should be designed to accommodate (or at least not interfere with) response-force activities.

## Levels of Protection

Level of Protection (LOP) is the degree to which an asset (person, equipment, object, etc.) is protected against injury or damage from an attack. The intent of a LOP is to minimize the possibility of mass casualties. LOPs provided by DoD standards establish a foundation for the rapid application of protective measures applicable to the threat environment.

The key concept of level of protection (LOP) is minimizing injuries and fatalities. The DoD Minimum Antiterrorism Standards for Buildings (UFC 4-010-01) recommends for planning purposes selection of at least a Low LOP for the primary billeting and operations area of the FOB. This means that the majority of personnel may suffer minor to moderate injuries, but fatalities are unlikely. Based on their proximity to the perimeter or other exposure, areas such as fighting positions, guard towers, vehicle parking, etc. may be at higher risk and have a lower LOP.

One issue to remember regarding LOP is that more resources (standoff, construction effort, time, personnel, etc.) are required for higher LOPs. Table 10-1 categorizes facilities by population to assist in establishing risk mitigation priorities. Table 10-2 describes the levels of protection and the potential for structural damage and human injury at each level.

## Protective Construction

One of the elements in an integrated, layered, defense-in-depth plan for the FOB is the use of structures that are designed to protect personnel and other assets from the effects of threat weapons. Protective construction is the process of applying security elements to the development of the FOB in order to mitigate the effects of these attacks.

Protection from VBIEDs and RAMs should be considered during the FOB planning/layout stage rather than trying to include it after the FOB is occupied. There are always constraints on available resources (time, manpower, materials, equipment, funds, etc.) but protective construction should be applied to the extent possible.

If the desired level of protection from VBIEDs and RAMs cannot be provided during the expeditionary and initial stage of the FOB, at a minimum, a plan should be established for implementing and increasing levels of protection as the FOB evolves. To the extent plausible, locations in which personnel routinely work, eat, sleep, or otherwise congregate should be hardened. In addition, hardened positions such as bunkers and foxholes with overhead cover should be provided in immediate proximity to all unprotected areas in which personnel must work or transit within the FOB. The axiom to continue to improve the position for as long as it is occupied remains valid.

**Recommended Sequence For Providing Protection.** The sequence shown in Figure 10-2 is intended to assist in deciding what priority of effort and amount of protection should be included in the plan for protecting a FOB. It is intended ONLY as a guide and is not exhaustive. It is not a substitute for a detailed mission analysis and course of action development process. Each particular situation may require another sequence and other or additional TTPs for protection.

## Mitigation Strategies

It is important to be familiar with different structure types used for FOBs. A wide range of structure types can be used, ranging from buildings to bunkers, barriers and barricades. Buildings include temporary buildings, conventional buildings, and hardened structures. The types of structures

Table 10-1. Summary of Structure Category Definitions (From UFC 4-010-01)

Building Construction	Definition	Minimum Level of Protection
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.	Low
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.	Low
Inhabited Building	Buildings or portions of buildings routinely occupied by 11 or more DoD personnel and with a population density of greater than one person per 40 gross square meters (430 gross square feet). This density generally excludes industrial, maintenance, and storage facilities, except for more densely populated portions of those buildings such as administrative areas. The inhabited building designation also applies to expeditionary and temporary structures with similar population densities. In a building that meets the criterion of having 11 or more personnel, with portions that do not have sufficient population densities to qualify as inhabited buildings, those portions that have sufficient population densities will be considered inhabited buildings while the remainder of building may be considered uninhabited.	Very Low
None of the Above	Buildings not meeting any of the above criteria in this table are not subject to the standoff requirements in UFC 4-010-01	

Table 10-2. Levels of Protection — Expeditionary and Temporary Structures (From UFC 4-010-01)

Level of Protection	Potential Structural Damage	Potential Injury
Below AT Standards <sup>1</sup>	Severe damage. Frame collapse/massive destruction. Little left standing.	Majority of personnel in collapse region suffer fatalities. Potential fatalities in areas outside of collapsed area likely.
Very Low	Heavy damage. Major portions of the structure will collapse (over 50%). A significant percentage of secondary structural members will collapse (over 50%).	Majority of personnel in damaged area suffer serious injuries with a potential for fatalities. Personnel in areas outside damaged area will experience minor to moderate injuries.
Low	Moderate damage. Damage will be unreparable. Some sections of the structure may collapse or lose structural capacity (10 to 20% of structure).	Majority of personnel in damaged area suffer minor to moderate injuries with the potential for a few serious injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience a minor to moderate injury.
Medium	Minor damage. Damage will be repairable. Minor to major deformations of both structural members and non-structural elements. Some secondary debris will be likely, but the structure remains intact with collapse unlikely.	Personnel in damaged area potentially suffer minor to moderate injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience superficial injuries.
High	Minimal damage. No permanent deformation of primary and secondary structural members or non-structural elements.	Only superficial injuries are likely.
Note 1. This is not a level of protection, and should never be a design goal. It only defines a realm of more severe structural response, and may provide useful information in some cases.		

Sequence	Task	Protection
Establish a defended perimeter at a sufficient standoff	Install concertina/razor wire; man perimeter with personnel dug in or in fighting vehicles	Minimal
	Add obscuration at perimeter using netting or opaque screens	
	Add tall barriers to the perimeter such as soil-filled bins or soil-backed concrete T-walls	
	Provide a double wall perimeter with an outer low wall and an inner high wall separated by a minimum 30-foot clear zone; use sensor, lighting and observation/guard towers.	More
Establish access control procedures and entry control facilities	Provide an entry control point with an approach zone comprised of barriers forming a serpentine approach; provide access control zone with armed personnel in fighting positions and an armored vehicle as a control gate	Minimal
	Add dedicated and protected vehicle and pedestrian search areas and vehicle barriers	
	Add response zone with armed response force, overwatch position and a final denial gate.	
	Provide bunkers for increased protection of security personnel	
	Construct a full entry control facility; provide a load transfer yard for material delivery; deny entry to all vehicles inside the FOB; provide protected parking area	More
Enhance Personnel Protection	Disperse personnel so there are no large gatherings in one place at the same time	Minimal
	Provide personnel bunkers at various locations on the FOB	
	Add full height sidewall protection for tents and modular housing units	
	Retrofit existing buildings	
	Compartmentalize structures	
	Add detonation screens and overhead cover for high occupancy facilities	More

Figure 10-2. Protective Construction Priority of Effort.  
Protection enhances (moving from minimal to more; top to bottom)  
as additional tasks within each sequence are accomplished.



that are used depend on the FOB location (urban or remote site), use of any existing available structures, local availability of temporary structures, and access to raw materials and required materials for pre-engineered temporary structures.

There are a variety of protective mitigation strategies available to planners and engineers. For example, perimeter fencing and vehicle barriers provide a controlled perimeter and provide protection against vehicle bomb threats by stopping a moving vehicle and creating standoff to mitigate blast effects. They can also obscure lines of sight into the FOB to hinder the use of direct fire weapons. Barriers at a perimeter may also be capable of stopping bullets and fragments from direct and indirect fire weapons. Bunkers provide a high protection level against small arms and indirect fire weapons. Not all strategies will apply in all situations, and some are clearly better than others. Mitigation strategies discussed in the remainder of this handbook are summarized in the paragraphs below.

**Vehicle-borne Improvised Explosive Device (VBIED).** Vehicle bombs are one of the most effective asymmetric threat weapons. They are capable of delivering a large quantity of explosives to a target and they can cause a great deal of damage. A VBIED is a car or van filled with explosive, driven to a target and then detonated. Vehicle bombs typically use an improvised explosive or incendiary mixture to provide the explosive charge. The bomb can be made at leisure and at a safe distance from the target. The explosives may be concealed in a container such as a beer keg, dumpster, or large suitcase. Once assembled, the bomb can be delivered at a time of the adversary's choosing and with reasonable precision. It can be detonated from a safe distance using a timer or remote control, or it can be detonated on the spot by a suicide bomber. Building a vehicle bomb requires a significant investment of time, resources and expertise. Be-

Table 10-3. VBIED Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Perimeter Protection	Provide sufficient standoff	11
	Provide perimeter barriers and walls capable of stopping vehicles and reducing the effects of a detonation	12; 21
	Provide guard towers and fighting positions to help identify, engage and defeat VBIEDs	20; 21
	Establish access control procedures and entry control structures to deter, detect, deny and protect against VBIEDs	9; 13; 21
Protective Construction	Provide personnel bunkers and/or retrofit existing structures for blast protection	19; 20

cause of this, adversaries will seek to obtain the maximum impact for their investment. They generally choose high-profile targets where they can cause extensive damage, inflict mass casualties and attract widespread publicity. VBIED mitigation strategies are shown in Table 10-3.

**Personnel-borne Improvised Explosive Device (PBIED).** These are usually carried in containers such as rucksacks or briefcases, which are chosen to blend in easily with the target surroundings. Given the requirement to be easily portable, such bombs are unlikely to weigh more than 50 lbs. (25kg), although even an ordinary-sized briefcase can contain about 25 lbs. (12kg) of explosive. A 50 lb. suitcase bomb could destroy a house or cause serious structural damage to larger buildings. Adversaries often increase the effectiveness of their bombs by packing them with nails, nuts and bolts or similar items to act as shrapnel. Such weapons can have a devastating effect in a small space. PBIED mitigation strategies are shown in Table 10-4.

Table 10-4. PBIED Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Perimeter Protection	Provide perimeter barriers / walls capable of stopping personnel	12
	Provide guard towers and fighting positions to help identify, engage and defeat PBIEDs	20
	Provide lighting and sensors to assist in detecting and assessing PBIEDs	17; 18
	Establish access control procedures and entry control structures to deter, detect, deny and protect against PBIEDs	9; 13
Protective Construction	Compartmentalize high occupancy facilities to limit the effects of a PBIED.	15

**Rockets, artillery, and mortars (RAM).** Indirect fire weapons are those that can be fired over obstacles to hit targets. They do not require a clear line of sight as direct fire weapons do, but they do require a clear line of flight. Indirect fire weapons include mortars and small rockets. The small rockets are usually improvised or military rockets with small explosive or incendiary charges on them, which are representative of historical terrorist attacks. Mortars include both military and improvised mortars. Historically, the improvised versions of mortars have carried larger quantities of explosives than the military versions. Employment of large artillery would be limited to combat forces. However, artillery rounds and propellant are commonly used as explosives to damage or destroy facilities or

assets or to kill or injure people. Explosives are particularly attractive because bombs are inexpensive to build and provide a significant psychological and destructive impact. RAM mitigation strategies are shown in Table 10-5.

Table 10-5. RAM Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Protective Construction	Provide personnel bunkers for blast and fragment protection given warning	20
	Provide full height sidewall protection for "soft" structures	14
	Compartmentalize high occupancy facilities to limit the effects of a RAM.	15
	Provide overhead protection to detonate and defeat incoming RAMs	16
	Evaluate and retrofit existing structures for protection from near miss and direct hits of RAMs	19

**Rocket-propelled grenades.** Antitank weapons are fired from a distance and may be directed against facilities, vehicles, or other assets that could be targeted from a distance. These can be used in the same manner as any direct fire weapon. The antitank weapons commonly encountered are shoulder-fired, rocket propelled grenade (RPG) launchers. Typical weapons that have been used by adversaries include the Russian RPG-7, RPG 18, and RPG 22 and the U.S. M-72 Light Antitank Weapon (LAW). RPG mitigation strategies are shown in Table 10-6.

Table 10-6. RPG Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Perimeter Protection	Provide detonation screens and barriers/walls to stop RPG penetration	14
	Provide netting or other screens to obscure potential targets inside the FOB and prevent targeting	14
	Provide detonation screens and barriers/walls around potential targets inside the FOB to stop RPG penetration	14
	Provide bunkers with detonation screens or thick walls to prevent RPG penetration	20

**Small-arms fire.** Small arms include pistols, rifles, shotguns, and submachine guns that can be either military issue or civilian weapons. These direct fire weapons must be aimed directly at a target and the line of sight to the target must be clear to successfully hit it. Adversaries use small arms to attack assets from a distance and may use them to overpower guards and sentries. Small-arms fire mitigation strategies are shown in Table 10-7.

Table 10-7. Small-Arms Fire Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Perimeter Protection	Provide netting or other screens to prevent targeting	14
	Provide perimeter walls to stop ballistic penetration	14
	Provide guard towers and fighting positions to engage and defeat small arms fire	20
Protective Construction	Provide netting or other screens to obscure potential targets inside the FOB	14
	Provide full height sidewall protection for "soft" structures to stop ballistic penetration	14
	Evaluate and use existing structures for protection	19
	Provide bunkers for protection from small arms	20

**Snipers.** Because of the realities of both foreign and domestic terrorism and guerilla-type asymmetric warfare, a sniper is anyone who fires a rifle at someone else from a concealed position. Traditionally, snipers are trained, experienced professionals with special weapons. They are excellent marksmen, and masters of camouflage and concealment. Snipers are independent operators noted for their pro-activeness, patience and calculating nature. Sniper mitigation strategies are shown in Table 10-8.

Table 10-8. Sniper Threat Mitigation Strategies

Protective Concepts	Mitigation Strategy	Reference Chapter
Perimeter Protection	Provide netting or other screens to prevent targeting	14
	Provide perimeter walls to stop ballistic penetration	14
Protective Construction	Provide netting or other screens to obscure potential targets inside the FOB	14
	Provide full height sidewall protection for "soft" structures to stop ballistic penetration	14
	Use existing structures for protection	19
	Provide bunkers for protection from sniper fire	20

## Chapter 11

# Standoff

### Introduction

In general, the best technique to reduce the risks and effects of an enemy attack using explosives, especially one involving VBIEDs is to keep the attack as far away as possible from the FOB and inhabited structures. Generally, the cost to provide protection will decrease as the distance between an asset and a threat increases. Ideally, maximum standoff should be a primary consideration when personnel are deciding where to locate a FOB. However, increasing stand-off also requires more land and more perimeter to secure with barriers.

If standoff around the FOB is not possible, the next best solution is to maximize standoff around individual inhabited structures within the FOB. Even with adequate space, standoff must be coupled with appropriate operational security procedures (such as access control) in order to be effective. Allowances for standoff distance should also provide opportunities to upgrade structures in the future to meet increased threats or to accommodate higher levels of protection.

### Physics of an Explosion

An explosion is an extremely rapid release of energy primarily in the form of a blast wave. When an explosion is initiated the blast wave is formed by the following sequence of events:

1. A rapid chemical reaction characterized by a detonation wave travels at velocities of 5,000 to 30,000 ft/sec from the point of initiation through the explosive compound (See figure 11-1).
2. This rapid chemical reaction converts the explosive compound into an extremely hot, high pressure gas with temperatures of 5,000-7,000 °F and pressures of 1,500,000–4,500,000 psi.
3. The hot gaseous fireball expands rapidly displacing the air around it. It transfers its momentum to the surrounding air as a layer of highly compressed air. This forms the shock or blast wave (See figure 11-2). This blast wave contains most of the energy released by the explosion. As the fireball expansion slows its overpressure falls to zero and due to overexpansion goes negative creating a suction phase in the blast wave before finally returning to zero.

The blast wave travels radially outward from the source at supersonic velocities. As it expands, the pressure of the compressed air falls rapidly

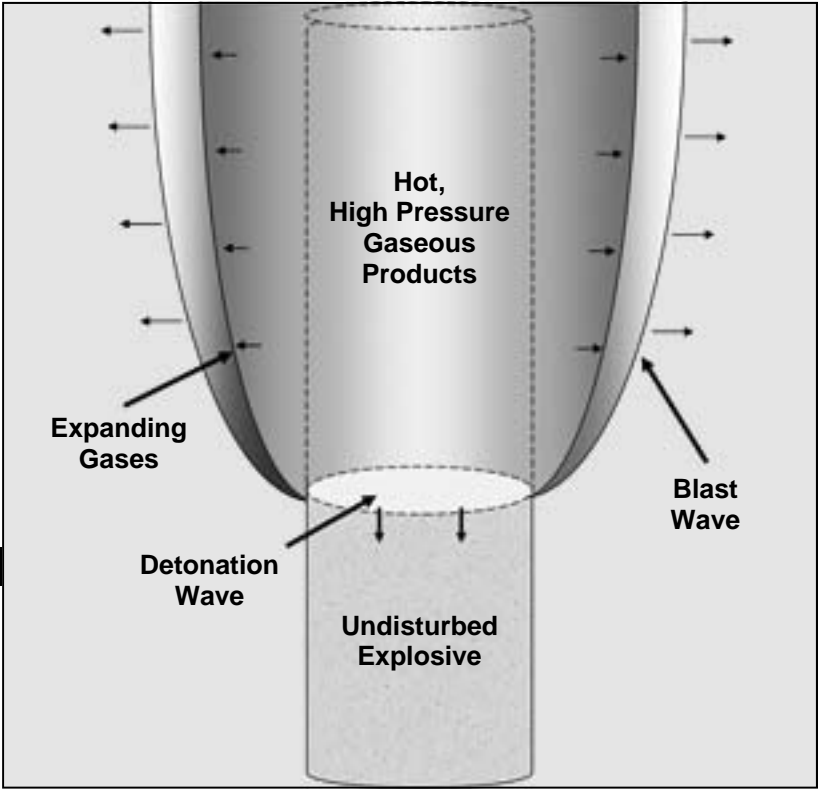


Figure 11-1. Detonation Process in a Solid Explosive



Figure 11-2. High-speed camera sequence showing blast wave formation

with increasing distance (Figure 11-3). However, if the wave meets a surface that is perpendicular to the direction it is traveling (such as a building), it is reflected and amplified by a factor of up to thirteen. Figure 11-4 shows how pressures behind the wave front also decay rapidly over time (exponentially) and have a very brief span of existence, measured typically in thousandths of a second (or milliseconds). Following the positive phase, the shock wave becomes negative, creating suction. In an external

explosion, a portion of the energy is also imparted to the ground, creating a crater and generating a ground shock wave similar to a high-intensity, short-duration earthquake.

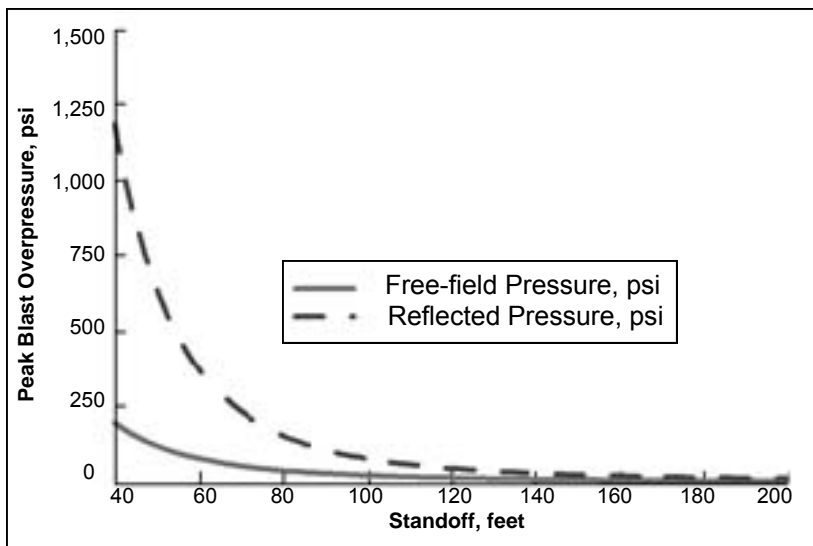


Figure 11-3. Graph of blast wave decay with distance. Data is from detonation of 4,000 lbs TNT.

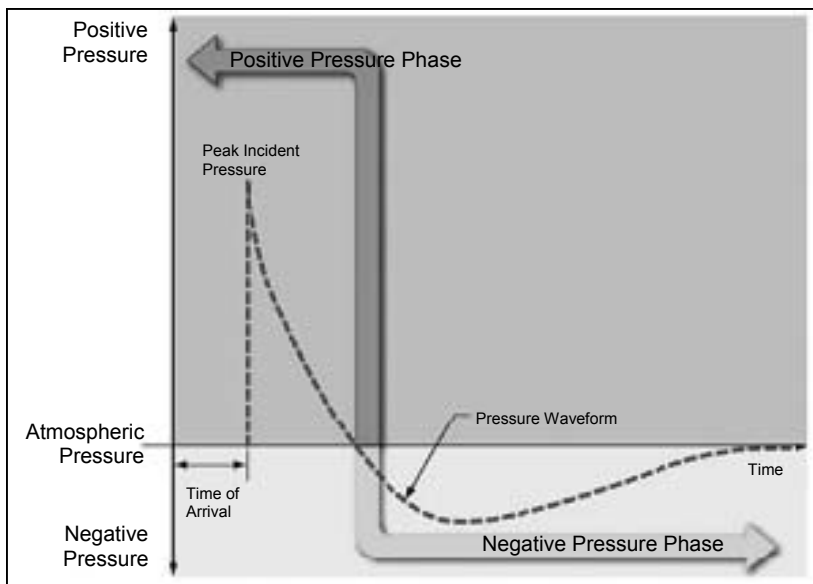


Figure 11-4. Depiction of blast pressure response with time

**Blast Effects**

Objects near the detonation and in the path of the blast wave may be damaged in a variety of ways.

**Fragmentation.** Close-in to the detonation the extreme pressures and rapid fireball expansion will cause most materials to fragment and be projected outward at high velocities. Fragments from mortar shells or rocket warheads have velocities on the order of 4,000-5,000 ft/sec. Fragments from vehicles are on the order 1,000 ft/sec. Concrete T-walls located 5-10 feet away from large vehicle bombs may be breached creating hazardous debris (see Figure 11-5). Personnel will not survive close to the detonation.

**Traumatic Injuries.** Outside the fireball, there are four basic mechanisms for blast injures to personnel as shown in Table 11-1. Figure 11-6 gives an example of how lung damage varies with standoff. This graph shows that increasing the standoff from 60 to 120 feet reduces that chance of severe lung damage from 90% to 10%.

**Building Damage.** The blast wave is the primary damage mechanism for a building. Because of the high reflected pressures on the side of the building facing the explosion, damage on this face may be significantly

Table 11-1. Classification of Personnel Blast Injuries

Category	Characteristics	Types of Injuries
Primary	Results from the impact of the blast wave with body surfaces.	Blast lung (pulmonary barotrauma), Eardrum rupture and middle ear damage, Abdominal hemorrhage and perforation.
Secondary	Results from flying debris and bomb fragments.	Penetrating ballistic (fragmentation) or blunt injuries
Tertiary	Results from individuals being thrown by the blast wind.	Fracture and traumatic amputation, Brain injury
Quaternary	All other explosion-related injuries.	Burns, Crush injuries, Brain injury, Asthma or other breathing problems from dust, smoke, or toxic fumes



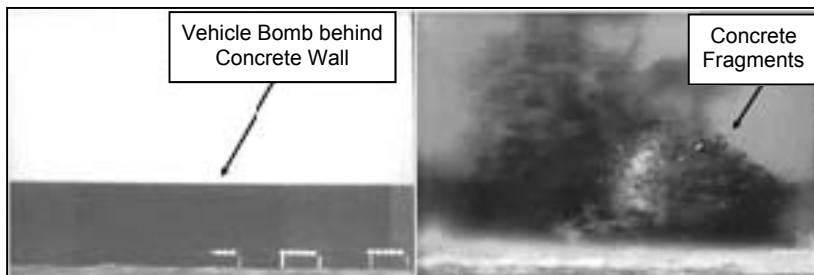


Figure 11-5. Depiction of a vehicle bomb breaching a concrete wall (Left: vehicle bomb behind concrete wall; Right: concrete fragments)

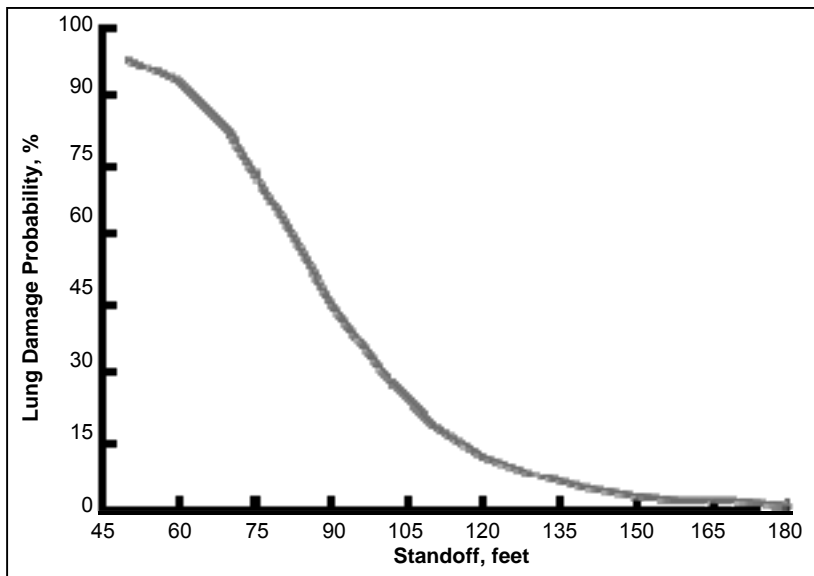


Figure 11-6. Probability of severe lung damage - vs. - Standoff for a 4,000 lb. blast

more severe than on the sides away from the detonation. The blast load may be several orders of magnitude greater than the loads for which the building is designed. In terms of sequence of response, the blast wave first impinges on the exterior envelope of the building. Glass is often the weakest part of this envelope, breaking at low pressures compared to other components such as the walls, floors or columns. Glass breakage may extend for miles in large explosions and high-velocity glass fragments are a major cause of injuries. Walls are generally the next weakest component. When they fail, the large pieces of debris that are generated may cause serious blunt trauma injuries. In addition, if the walls are the primary load bearing elements, failure may lead to building collapse. For detonations close to the building (near the fireball), structural components such as columns and girders may fail leading to potential progressive col-

Table 11-2. Standoff Distances and Separation for Expeditionary and Temporary Structures  
(From UFC 4-010-02)

Location	Structure Category	Standoff Distance or Separation Requirements			
		Applicable Level of Protection	Fabric Covered/ Metal Frame Structures <sup>1</sup>	Other Expeditionary and Temporary Structures <sup>1,2</sup>	Applicable Explosive Weight (TNT) (FOUO) <sup>3</sup>
Controlled Perimeter or Parking and Roadways without a Controlled Perimeter	Billeting	Low	31 m (102 ft.)	71 m (233 ft.)	I 100 kg (220 lb.)
	Primary Gathering Structure	Low	31 m (102 ft.)	71 m (233 ft.)	I 100 kg (220 lb.)
	Inhabited Structure	Very Low	24 m (79 ft.)	47 m (154 ft.)	I 100 kg (220 lb.)
Parking and Roadways within a Controlled Perimeter	Billeting	Low	14 m (46 ft.)	32 m (105 ft.)	II 25 kg (55 lb.)
	Primary Gathering Structure	Low	14 m (46 ft.)	32 m (105 ft.)	II 25 kg (55 lb.)
	Inhabited Structure	Very Low	10 m (33 ft.)	23 m (75 ft.)	II 25 kg (55 lb.)

Trash Containers	Billeting	Low	14 m (46 ft.)	32 m (105 ft.)	II	25 kg (55 lb.)
	Primary Gathering Structure	Low	14 m (46 ft.)	32 m (105 ft.)	II	25 kg (55 lb.)
	Inhabited Structure	Very Low	10 m (33 ft.)	23 m (75 ft.)	II	25 kg (55 lb.)
Structure Separation <sup>4</sup>	Separation Between Structure Groups	Low	18 m (59 ft.)	18 m (59 ft.)	III	1 kg <sup>5</sup> (2.2 lb.)
	Separation Between Structure Rows	Low	9 m (30 ft.)	9 m (30 ft.)	III	1 kg <sup>5</sup> (2.2 lb.)
	Separation Between Structures in a Row	Very Low	3.5 m (12 ft.)	3.5 m (12 ft.)	III	1 kg <sup>5</sup> (2.2 lb.)
<ol style="list-style-type: none"> <li>1. See Definitions [in UFC 4-010-01 or 4-010-02] for a complete description of these structure types.</li> <li>2. For container structures, Appendix B in UFC 4-010-01 applies.</li> <li>3. When the explosive specific weights in this column are moved from this table, the table is no longer For Official Use Only.</li> <li>4. Applies to Billeting and primary Gathering Structures only. No minimum separation distances for other inhabited structures.</li> <li>5. Explosive for building separation is an indirect fire (mortar) round at a standoff of half the separation distance.</li> <li>6. Refer to Appendix A of UFC 4-010-01 for definitions necessary for application of this table.</li> </ol>						

lapse of the entire building. Building collapse is the major cause of fatalities and situations where this can occur should be avoided by ensuring enough standoff and not occupying buildings with load-bearing walls (See Figure 11-7 for an example of building blast damage).



Figure 11-7. Building damage resulting from the 1996 Khobar Towers attack

**Standoff Guidelines**

Table 11-2 shows minimum standoff distances required by UFC 4-010-01. These distances are intended to provide Low or Very Low levels of protection for building occupants as defined in the table. Geographic combatant commanders may establish different construction standards for a specific deployment area. Refer to the specific construction standards for your deployment area.

To assist in the site selection and layout planning process, the following tables provide recommended standoff distances. Select the appropriate table based on the following scenarios:

<u>Personnel Location</u>	<u>Use Table</u>
In open, exposed to airblast	11-3, p. 11-9
In open, exposed to debris from concrete perimeter wall	11-4, p. 11-9
In tents exposed to airblast	11-5, p. 11-10
In building with glass windows	11-6, p. 11-10
In building exposed to wall debris and other damage	11-7, p. 11-11

Table 11-3. Expected Lung Damage

Charge Weight (lbs, TNT Equivalent)	Estimated Standoff (feet) *			
	Very Low LOP, 10% Fatality	Low LOP, 5% Fatality	Medium LOP, 1% Fatality	High LOP, Threshold
220	23	25	26	44
500	34	36	38	60
1,000	45	47	49	80
4,000	78	82	85	134
10,000	109	114	119	189
* Minimum standoff distance required to achieve specified LOP.				

Table 11-4. Expected Concrete Wall Debris Hazard

Charge Weight (lbs, TNT Equivalent)	Estimated Standoff (feet) *			
	Very Low LOP, 10% Fatality	Low LOP, 5% Fatality	Medium LOP, 1% Fatality	High LOP, Threshold
500	80	85	100	110
2,000	810	860	1,000	1,100
4,000	1,350	1,440	1,600	1,800
10,000	3,000	3,200	3,600	4,000
* Assumes a 1-foot thick wall located 10 feet from the charge.				

Table 11-5. Expected Tent Damage

Charge Weight (lbs, TNT Equivalent)	Estimated Standoff (feet) *		
	Low LOP, 10-50% of tent collapses, Serious Injuries, Possible Fatalities	Medium LOP, Fabric tears, minor frame damage, no collapse Minor to moderate Injuries	High LOP, Loose fabric, Superficial injuries
220	102	158	215
500	150	227	292
1,000	198	303	378
2,000	257	400	485
4,000	333	515	618
10,000	464	721	847
* Modular General Purpose Tent System - Injuries caused by impact from tent frame and debris from furniture inside tents.			

Table 11-6. Expected Glass Fragment Hazard

Charge Weight (lbs, TNT Equivalent)	Estimated Standoff (feet) *		
	Low LOP, High Hazard Severe to Very Severe lacerations, Potential Fatalities	Medium LOP, Low Hazard, Large number of lacerations, hospitalization may be required	High LOP, Break Safe, Small cuts and abrasions, medical aid needed but no hospitalization
220	257	363	491
500	350	500	670
1,000	450	660	870
4,000	750	1,090	1,430
10,000	1,030	1,480	1,970
* Minimum standoff distance required to achieve specified LOP, based on a 2 ft x 4 ft, 5/32-in. thick annealed glass window.			

Table 11-7. Expected Building Damage Hazard

Charge Weight (lbs, TNT Equivalent)	Estimated Standoff (feet) *			
	Very Low LOP, 10% Fatality	Low LOP, 5% Fatality	Medium LOP, 1% Fatality	High LOP, Threshold
500	40	50	70	90
1,000	90	110	150	170
4,000	250	290	300	440
10,000	450	510	640	750
* Based on BICADS runs for a 2 Story 75-ft. x 75-ft. reinforced concrete frame building with 8 in. brick infill walls consisting of 25 rooms per floor and 2 people per room. Personnel in the interior 9 rooms on each floor were not analyzed. Building analyzed had no windows.				

Table 11-8 shows standoff distance needed to prevent modular concrete barrier wall failure from explosive threats. Barrier walls with higher strength concrete can resist breaching at smaller standoff distances than those shown. More information on concrete barriers can be found in Chapter 12.

Table 11-8. Standoff Distance Needed to Prevent Concrete Wall Failure from TNT-Equivalent Explosive Threat Weights  
(From DRAFT UFC 4-027-01).

Wall Thick- ness	Standoff needed to Prevent Breaching,* inch (cm)					
	220 lb (100 kg)	440 lb (200 kg)	1,000 lb (454 kg)	2,200 lb (1,000 kg)	4,400 lb (2,000 kg)	22,000 lb (10,000 kg)
12 in (30 cm)	20 (6.1)	25 (7.7)	33 (10.1)	43 (13.2)	54 (16.6)	93 (28.5)
16 in (40 cm)	15 (4.7)	25 (7.7)	33 (10.1)	43 (13.2)	54 (16.6)	93 (28.5)
20 in (50 cm)	11 (3.3)	21 (6.5)	33 (10.1)	43 (13.2)	54 (16.6)	93 (28.5)
24 in (60 cm)	8 (2.4)	16 (4.9)	33 (10.1)	43 (13.2)	54 (16.6)	93 (28.5)
28 in (70 cm)	6 (1.8)	13 (3.9)	28 (8.6)	43 (13.2)	54 (16.6)	93 (28.5)
* For barrier concrete with 2,000 psi (13.8 MPa) compressive strength. All information is for bare concrete wall barriers without soil backing or other material to mitigate breaching.						

More refined calculations of structure damage and resulting human injury can be done using blast effect software such as AT Planner, BEEM, or VAPO (See Figure 11-8). However, it is highly recommended that a trained structural engineer (preferably one familiar with blast effects) be involved in this process so that the building structural characteristics are modeled correctly in the software.

#### **Antiterrorism (AT) Planner**

AT Planner is a digital analysis tool used for evaluating the damage to buildings and injury to occupants resulting from explosive threat scenarios. The emphasis is on the evaluation of structural components, windows, personnel, and a few other assets. Structural components are defined for columns, walls, and roofs, including common construction materials. The software is available from the U.S. Army Engineer Research and Development Center at <https://atplanner.erd.c.usace.army.mil> (Accept the security certificate presented and log in with User Name **atpuser** and Password **4u2plan**. Follow the instructions on the site to obtain the software and an activation key).

#### **Blast Effects Estimation Model (BEEM)**

BEEM is an assessment tool for modeling the effects of various types of explosive devices and indicates the degree of damage to personnel and buildings nearby. BEEM incorporates versions of the AT Planner Tool (see description above) and the Force Protection Tool. BEEM can be used to assess blast and fragmentation effects. BEEM is available from the U.S. Army Corps of Engineers Protective Design Center at <https://pdc.usace.army.mil/software/beem/>. Follow the instructions on the site to obtain the software.

#### **Vulnerability Assessment Protection Option (VAPO)**

VAPO is designed to support force protection evaluators and planners with the ability to address modern asymmetric threats such as improvised IEDs and chemical and biological weapons. VAPO uses fast running, physics-based algorithms to predict cratering, fragmentation, blast damage and subsequent collateral effects resulting from chemical or biological agent dispersion. It calculates the blast and fragmentation environment for urban scenes, to include effects of reflection and diffraction of blast pressures off and around structures. It also models progressive collapse of buildings. All VAPO requests must be done on the Defense Threat Reduction Agency, Assessment of Catastrophic Events Center (ACECenter) web site at <https://acecenter.cntr.dtra.mil/acecenter/>.

Figure 11-8. Blast Effect Analysis Software



# Barriers and Obstacles

## Introduction

Throughout the range of military operations, Joint forces may encounter, or be required to employ obstacles of any type. In any type of offensive or defensive operation, obstacles can help Joint forces protect personnel, equipment, and facilities. Joint forces conducting military engagement, security cooperation, and deterrence activities sometimes use obstacles to enhance deterrence and demonstrate resolve.<sup>1</sup> In operations such as humanitarian and civic assistance, the very purpose of the operation might be focused on the reduction or elimination of obstacles. Such obstacles may have been emplaced years prior to the operation or by someone other than a current adversary. In major operations and campaigns, and some crisis response and limited contingency operations, Joint forces will be involved in armed conflict. They use obstacles offensively and defensively to attack the mobility of adversaries, enhance the effects of friendly fires, deny adversaries the use of terrain, disrupt sustainment operations, and inflict damage to (and casualties upon) enemy forces.

Obstacles can be either natural or man-made (or a combination of both), as shown in Figure 12-1. Natural obstacles are terrain features, such as rivers, forests, or mountains. Man-made obstacles can be explosive or non-explosive. Nonexplosive obstacles do not contain explosives (although explosives may be detonated to create the obstacle). They include cultural, constructed, or demolition obstacles. Cultural obstacles are man-made terrain features that were not created for the purpose of obstructing military forces (for example, towns, canals, or railroad embankments). Constructed obstacles are created without the use of explosives (such as wire obstacles and antitank ditches). Demolition obstacles are created by the detonation of explosives (examples include bridge demolition, road craters, and abatis). Explosive obstacles contain explosives and include mines, IEDs, UXO, and other explosive hazards.<sup>2</sup>

1. In some cases, though, the use of obstacles constitutes an act of war. It is critical that Joint forces carefully consider them when developing rules of engagement (ROE) and that staff judge advocates review them for legal sufficiency. All commanders and staff should be familiar with the specific ROE.

2. The use of some obstacles, especially mines, is governed by numerous international laws, US laws, and US policies. The United States regards mines as lawful weapons when employed in accordance with accepted legal standards. Mine warfare and emplacement is not covered in this handbook. Refer to JP 3-15, *Barriers, Obstacles, and Mine Warfare for Joint Operations*, for further information and guidance.

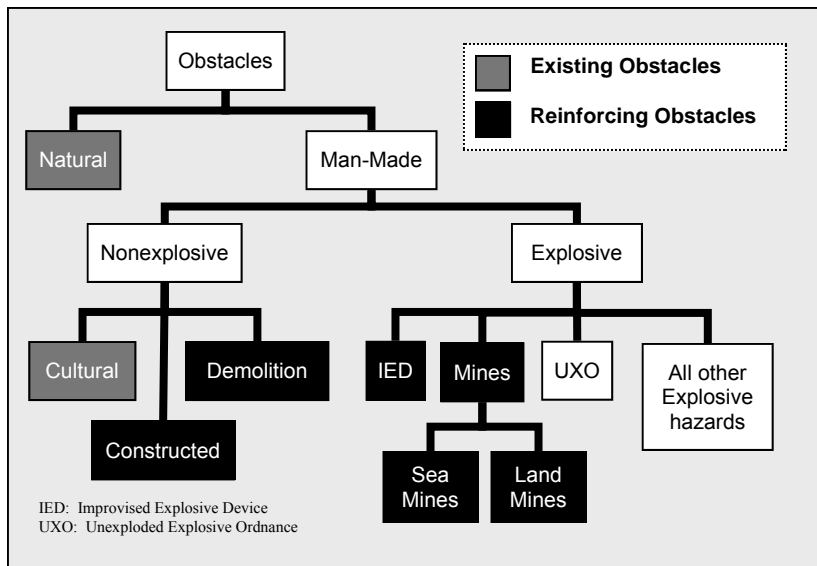


Figure 12-1. Types of Obstacles  
(From JP 3-15, *Barriers, Obstacles, and Mine Warfare for Joint Operations*)

Barriers are an integral part of the perimeter security system and serve to facilitate control of pedestrian and vehicle access. Physical barriers are used at the FOB perimeter to perform several functions:

- Define the perimeter of the FOB
- Establish engagement zones
- Establish a physical and psychological deterrent to attackers and individuals from attempting unlawful or unauthorized entry
- Deny access and protect against VBIED and PBIED attacks
- Help conceal and shield FOB activities from direct observation, surveillance, and targeting
- Provide ballistic protection from small arms and RPGs
- Optimize use of security forces
- Enhance detection and apprehension opportunities by security forces
- Channel the flow of personnel and vehicles through designated entry control points (ECP) in a manner which permits efficient operation of the personnel and vehicle identification and control system
- Detour vehicles away from the perimeter
- Block or close high-speed avenues of approach or reduce the approach speed of vehicles

## Antipersonnel Barriers

Antipersonnel barriers are designed to deter personnel on foot from entering a FOB. These barriers protect against infiltrators who may try to place small explosive charges, tamper with supplies and equipment, or attack friendly personnel or critical assets once they are inside the FOB. Typical antipersonnel barriers include chain link fences with barbed wire outriggers, triple-strand concertina fences, wire obstacles, concrete walls, and barbed wire fences. In most instances, antipersonnel barriers can be penetrated by the enemies' climbing over them or using wire cutters. Consequently, antipersonnel barriers must remain under constant observation.

**Chain Link and Metal Mesh Fences.** Chain link fences provide a moderate level of security for the FOB against infiltration by enemy personnel (See Figure 12-2). Chain link fences are cost effective, have a low profile, and are readily available. These fences are particularly effective if coupled with other barriers, either man-made (a canal) or natural (a lake or a river). However, chain link fences can be effectively breached by the enemies' cutting holes through the fence or tearing down the outriggers with a grappling hook and climbing the fence. The height [up to 8 ft (2.4 m)] of the fence or the degree of enhancements used has little effect on this time. In general, fence material can be easily cut or climbed over. Metal mesh fences are generally more difficult to climb. The enemy can bypass improperly installed fencing by climbing the fence or burrowing under it. These actions can be deterred if the security force tops the fence with outriggers and laces horizontal wire through the fence at the base.

**Triple-Strand Concertina Fence.** Triple-strand concertina fences are easy to set up and can be rapidly emplaced by unskilled labor (See Figure 12-3). Triple-strand concertina fences can be breached by an intruder's cutting the wire, disassembling the fence, or flattening down the concertina with a board or similar object. A poorly constructed concertina fence (for instance, one with no horizontal support wire) is especially susceptible to the latter two methods. The most common mistakes security forces make in constructing concertina fences are spacing engineer stakes too far apart, not using intermediate short pickets, neglecting to add horizontal wire, and failing to tie the concertina together.

**Concrete Walls.** Concrete and concrete masonry unit (CMU) walls can be effective anti-personnel barriers and can also prevent observation of the FOB, but they are costly and take considerable time to build. In order for these walls to be most effective, they should be smooth-faced, topped with outriggers or other material (razor wire, general purpose tape obstacle (GPTO), barbed concertina wire) and be at least 9 feet tall. While a wall

provides more structural support for someone climbing the wall than chain link fence, it provides fewer handholds for the climber. However, explosives can breach a concrete wall. Table 12-1 shows wall thickness needed to resist explosive breaching. This information is applicable to bare concrete wall barriers without soil backing or other material to mitigate breaching.

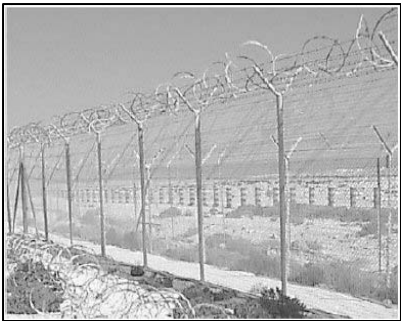


Figure 12-2. Metal mesh fence with razor wire and barbed-wire outriggers



Figure 12-3. Concertina wire fence (U.S. Navy photo)

Chain Link and Metal Mesh Fence Considerations

	Fences should not be located so that terrain features or structures (buildings, utility tunnels, light and telephone poles, ladders, etc.) allow passage over, around, or under them.
	Chain link and metal mesh fences should be anchored with metal posts placed in concrete at intervals no greater than 9 feet.
	Fences should be topped with razor wire, general purpose tape obstacle (GPTO), barbed concertina wire, or barbed wire outriggers (listed in order of most effective to least effective).
	Fence height, including outriggers, should be a minimum of 8 feet.
	Horizontal wire should be laced along the bottom and top of the fence to keep the edges rigid.
	The bottom edge of the fence should not rise more than 4 in. above the ground. The preferred installation method makes use of a concrete footing that encases the bottom of the fence around the entire perimeter. This method prevents an intruder from lifting the bottom of the fence, delays him from burrowing under it, and diminishes erosion
	A synthetic screen can be woven into the fence to prevent observation of the FOB, but care should be taken to ensure that the screen does not also block observation from within
	Additional information and specific guidance can be found in MIL-HDBK-1013/10, <i>Military Handbook Design Guidelines for Security Fencing, Gates, and Guard Facilities</i> .

Table 12-1. Concrete Barrier Wall Thicknesses Needed to Prevent Debris from Explosive Threat Weights  
(From DRAFT UFC 4-027-01).

Standoff ft (m)	Wall Thickness to Prevent Breaching,* inch (cm)					
	220 lb (100 kg)	440 lb (200 kg)	1,000 lb (454 kg)	2,200 lb (1,000 kg)	4,400 lb (2,000 kg)	22,000 lb (10,000 kg)
0 (0)	43 (110)	55 (140)	76 (194)	No data	No data	No data
4.9 (1.5)	30 (76)	44 (111)	67 (170)	No data	No data	No data
8.2 (2.5)	23 (59)	35 (88)	55 (140)	No data	No data	No data
16.4 (5)	15 (38)	23 (59)	39 (98)	62 (157)	No data	No data
32.7 (10)	9 (23)	15 (37)	25 (63)	41 (104)	52 (133)	137 (347)

\*For barrier concrete with 2000 psi (13.8 MPa) compressive strength.

**Drainage Culverts and Utility Openings Under Fences.** Special anti-personnel protective measures must be designed for culverts, storm drains, sewers, air intakes, exhaust tunnels and utility openings. Openings that pass through cleared areas, traverse under or through security fences, or have a cross-sectional area of 96 sq. in. (0.06 sq. m) or greater with the smallest dimension being more than 6 in. (150 mm) should be protected by securely fastened grills, locked manhole covers, or other equivalent means that provide security penetration resistance of approximately 2 min. (See Figures 12-4 and 12-5). MIL-HDBK-1013/10 (*Military Handbook Design Guidelines for Security Fencing, Gates, and Guard Facilities*) provides detailed design options.

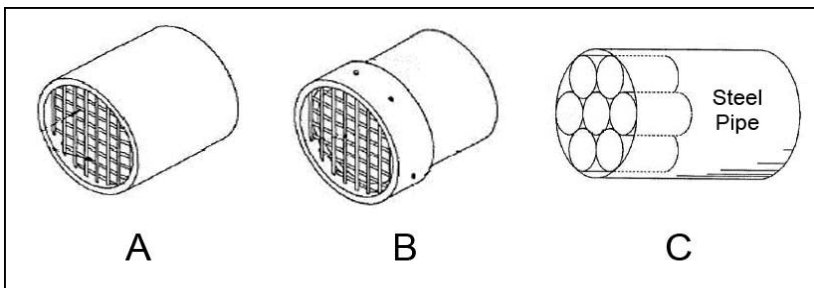


Figure 12-4. Culvert grill examples (A: Steel culvert grill; B: Concrete culvert grill; C: Large culvert with short honeycomb pipes) (From MIL-HDBK-1013/10)

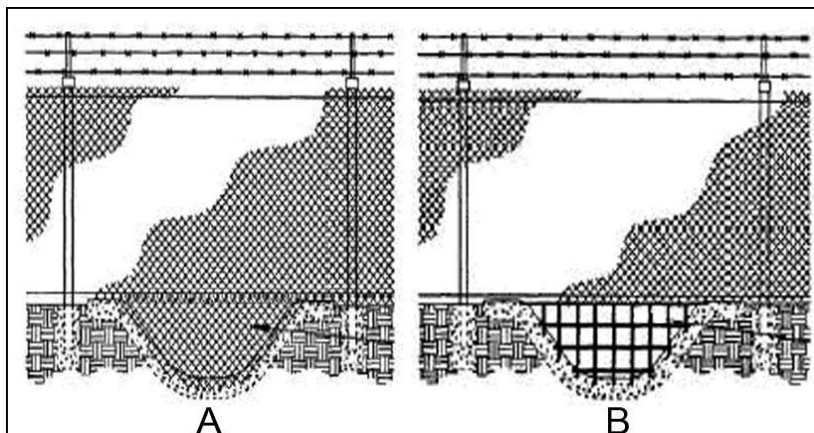


Figure 12-5. Under-fence utility opening examples (A: Swale crossing with ground stakes; B: Bar grill embedded in concrete) (From MIL-HDBK-1013/10)

### Anti-Vehicle Barriers

Anti-vehicle barriers are designed to stop vehicles at the perimeter of a FOB. They also assist in establishing standoff distance from protected assets. When placing anti-vehicle barriers, attention should be focused along high speed avenues of approach outside the perimeter. When selecting the type of barriers, consideration must be given to secondary debris and fragmentation created by explosives in close proximity to concrete barriers or concrete walls.

It is possible to breach anti-vehicle barriers, but breaching methods require considerable time and equipment. Anti-vehicle barriers can be penetrated by several methods: intruders can use explosives to breach walls or jersey barriers, eliminate berms or ditches with bulldozers or high-pressure water hoses, sever cables in cabled fences with a cutting torch or explosives, or move concrete barriers with a forklift. Since these barriers can possibly be penetrated, they need to remain under constant observation and should be coupled with combinations or layers of barriers. Typical anti-vehicle barriers are outlined below. Figure 12-6 provides an anti-vehicle barrier design and selection questionnaire.

**Concrete Barriers.** Concrete barriers (Jersey, Texas, Alaska, or Bitberg) are the most widely used anti-vehicle barriers. These barriers are readily accepted by host nation (HN) countries because of their temporary nature. Concrete barriers are typically employed for counter-mobility or explosive blast/fragment mitigation at entry control points (ECPs) and along avenues of approach. Concrete barriers employed in this fashion can be effective in stopping primary debris, if they are sufficiently tall. However, they also

## Anti-Vehicle Barrier Design and Selection Questionnaire

Use this questionnaire to ask the pertinent questions relating to design and selection of anti-vehicle barriers. MIL-HDBK-1013/14 (*Selection and Application of Vehicle Barriers*) and UG-2031-SHR (*User's Guide on Protection Against Terrorist Vehicle Bombs*) provide more detailed vehicle barrier selection processes.

### DESIGN FACTORS

- What is the explosive threat?
- What is the weight of the threat vehicle?
- Is there sufficient standoff distance between the planned barrier and critical structures?
- What is the expected speed of the threat vehicle?
- Can the speed of the vehicle be reduced?
- Have all impact points along the perimeter been identified?
- Have the number of access points requiring vehicle barrier installation been minimized?
- What is the most cost-effective barrier available that will absorb the kinetic energy developed by the threat vehicle?
- How many barriers are required at each entry point to meet throughput requirements?
- Will the barriers be subject to severe environmental conditions?
- Will barriers interfere with established clear zone requirements?
- Will active barriers fail to open or close in the event of power failure?
- Is this a temporary or permanent FOB?

### SELECTION FACTORS

- Will the barrier need to be aesthetically pleasing?
- Are appropriate safety features being considered?
- Will there be sufficient lighting at the barrier location?
- Has the selected barrier been crash-tested or approved for use?
- Is the selected barrier designed to resist corrosion or other environmental effects?
- Is the barrier the most cost-effective option available?
- Will barriers be under constant surveillance/observation?
- Have combinations of barriers been selected to provide a layered effect and redundant protection?

Figure 12-6. Anti-Vehicle Barrier Design and Selection Questionnaire

may become secondary debris hazards in the immediate vicinity of a large explosion and could cause additional damage (debris hazard distance charts can be found in Air Force Handbook 10-2401, *Vehicle Bomb Mitigation Guide*). Soil-backed concrete barriers provide better protection against secondary debris hazards (see Figure 12-7). The smaller concrete barriers (Jersey) are most effective when cabled together (See Figure 12-8). The cabling causes a ramming threat vehicle to push the weight of a wall of concrete barriers instead of a single concrete barrier. Concrete barriers cabled together should use at least a 3/4-in. aircraft cable. If the potential impact angle from a threat vehicle is expected to exceed 30 degrees, then the selected concrete barriers should be anchored to a concrete foundation. NOTE: this barrier is not sufficient to prevent a large or double VBIED attack. See discussion in Chapter 21.

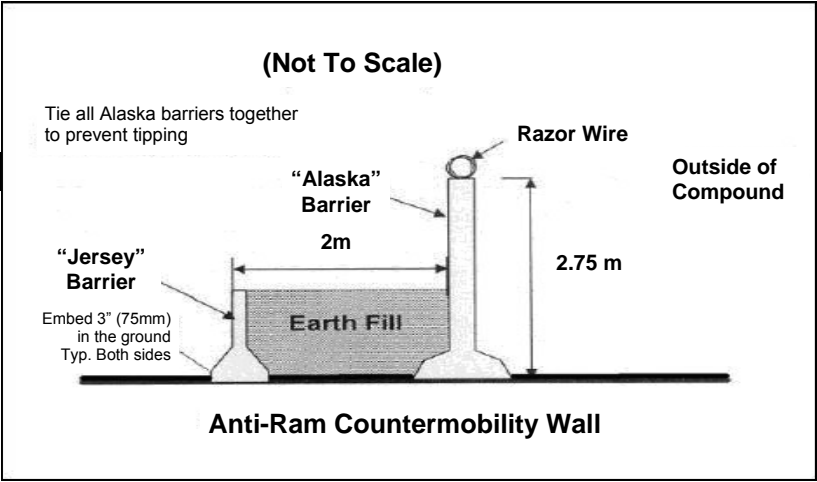


Figure 12-7. Soil-backed Concrete Barrier Concept



Figure 12-8. Cabled Jersey Barriers



**Cabled Concrete Blocks.** Like concrete barriers, non-reinforced concrete blocks (See Figure 12-9) can be used effectively to slow the speed of on-coming vehicles along the perimeter of a FOB or on an access road into an ECP. These blocks can be cast in place and should be anchored together with at least a 3/4-in. aircraft cable so that movement or removal is difficult. Concrete blocks are most effective when placed in a serpentine ('S') pattern.

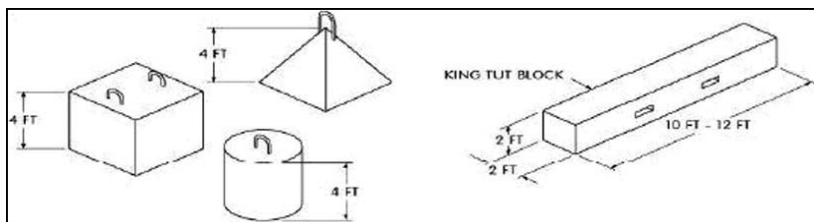


Figure 12-9. Typical Cabled Concrete Blocks (From MIL-HDBK-1013/14)

**Cable-Reinforced Chain Link Fences.** Chain link fences can be transformed into anti-vehicle barriers by reinforcing the existing fence line with steel cable (See Figure 12-10). This measure can be a relatively low-cost, low-profile option. Fences should be reinforced with two 3/4-in. steel cables woven into the fence at heights of 30 in. and 35 in. above the ground. Each end of the cables should be attached to a concrete deadman anchor. Posts placed at 4 ft intervals further reinforce fences, making them better able to hinder vehicle penetration. Crash tests performed on a chain-link fence reinforced with a 3/4 in. (19.1 mm) aircraft cable restricted penetration of a 2 ton (1814.4 kg) vehicle traveling at 50 mph (80.5 km/h) to 26 ft (7.9 m).

**Guardrails.** Standard highway guardrails installed on a FOB perimeter can be effective vehicle barriers. Guardrails are specifically designed with an angled impact of less than 25 degrees to deflect the energy of larger vehicles (This is the normal impact angle for highway design and the one most likely to produce vehicle rollover at high speeds). Typical guardrail types and dimensions are (See Figure 12-11):

**Cable**—consists of H-beams [2-1/4 in. (5.7 cm) x 4.1lb/ft (6.1 kg/m)], spaced at 16 ft. (4.9 m) on center, with two or three 3/4 in. (1.9 cm) diameter steel cables, spaced 8 in. (20 cm) apart. The height at the center cable is 26 in. (66 cm). The cables should be secured to a reinforced concrete deadman anchor at 200 ft. (61 m) intervals.

**W-Beam**—consists of H-beams spaced on 12.5 ft. (3.8 m) centers with steel “W” sections bolted to the H-beam. The height of this guardrail is 27 to 30 in. (68 to 76 cm).

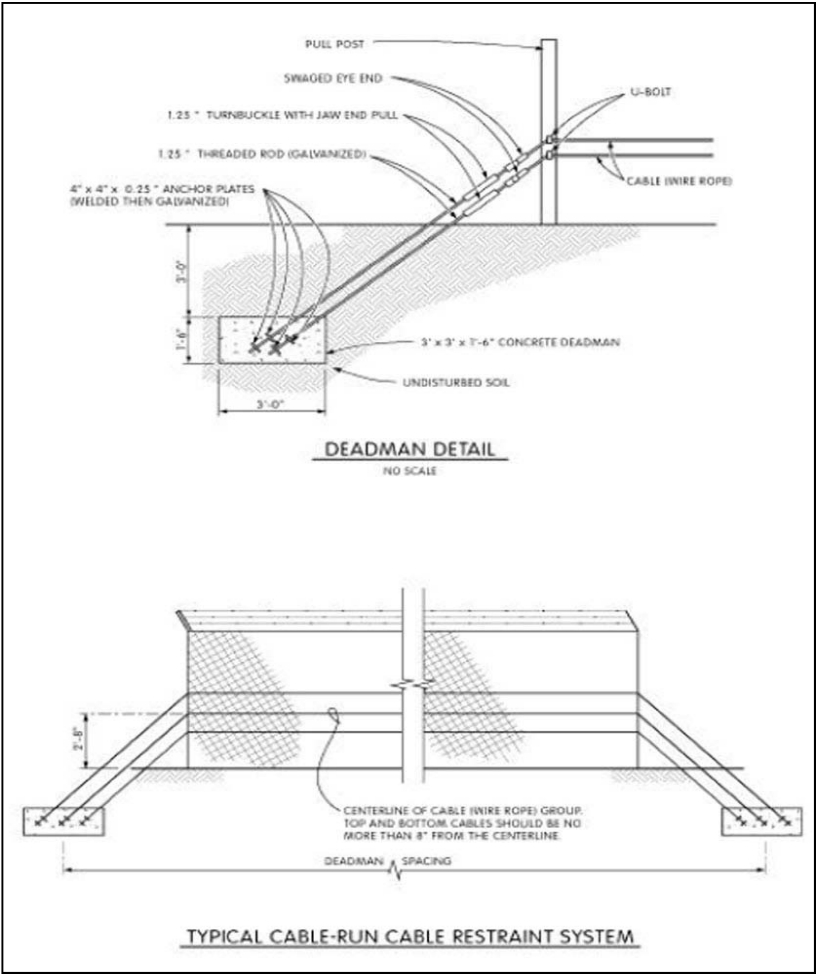


Figure 12-10. Typical Cable-Reinforced Chain-Link Fence  
(From MIL-HDBK-1013/14)

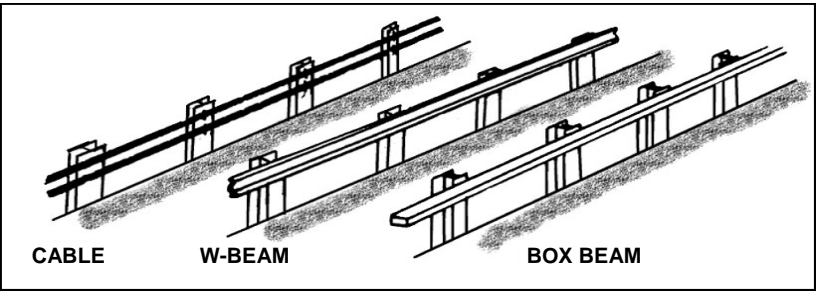


Figure 12-11. Typical Guardrail Construction (From MIL-HDBK-1013/14)

**Box Beam**—consists of H-beams, spaced on 4 to 6 ft (1.2 to 1.8 m) centers with a 6 by 6 in. (15 by 15 cm) steel tube bolted to the H-beams. The height of this guardrail is 27 to 30 in. (68 to 76 cm).

**Reinforced Concrete Walls.** Concrete walls can be a costly, yet effective, low-profile anti-vehicle barrier. In order to be effective, a wall should consist of at least 6 in. of reinforced concrete and have a 3 ft. deep footer. Tests<sup>3</sup> have shown that in order to stop a 15,000 lb. vehicle traveling 30 mph, a reinforced concrete wall must be 21 in. thick with a 4 ft footer (depending on local soil conditions). Refer to Table 12-1 for wall thickness needed to resist explosive breaching.

**Berms and Ditches.** Berms and ditches (See Figure 12-12) can be used to effectively stop vehicles from penetrating the FOB perimeter. Triangular ditches and hillside cuts are easy to construct and are very effective against a wide range of vehicle types. Hillside cuts are variations of the triangular ditch adapted to hillside locations and have the same advantages and limitations. A trapezoidal ditch requires more construction time but is more effective in stopping a vehicle. With this type of construction, a vehicle will be trapped when the front end falls into the ditch and the undercarriage is hung up on the leading edge of the ditch, rendering it inoperable. Native soils and rock can also be effective in explosive blast/ fragment mitigation since they have the ability to absorb large amounts of kinetic energy.

**Bollards.** Bollards are metal or concrete columns which are anchored into the ground (See Figure 12-13). Bollards can be used as active or passive barriers. Active bollards can be pulled out of the ground by hand or raised and retracted by a hydraulic system to control entry at a FOB ECP. An effective passive bollard system consists of 7 ft- (2.1 m) long steel pipes, a minimum of 8 in. (20 cm) to 10 in. (25 cm) in diameter filled with concrete. The pipes should be spaced 2 ft to 4 ft (0.6 - 1.2 m) off center and anchored into a 4-ft footing, so they project 3 ft. (0.9 m) above ground. The footing should be continuous, but individual footing depth should be at least twice the width, and the width should be three times the diameter of the pipe. Bollards can be placed on either the inside or the outside of existing fences.

**Cabled Steel Hedgehogs.** Also known as star barriers, hedgehogs are designed to roll underneath a ramming vehicle and destroy the driveshaft and undercarriage (See Figure 12-14). When cabled to adjacent jersey barriers, they can help stop a vehicle. To be effective, hedgehogs should

3. See MIL-HDBK-1013/14, *Selection and Application of Vehicle Barriers*, p. 80.

be of sturdy construction and used on paved areas.

**Expedient Barrier Systems.** Common construction items, such as large diameter concrete culverts, steel pipes, and large construction vehicles (for example, dump trucks and earth moving equipment) that have large mass

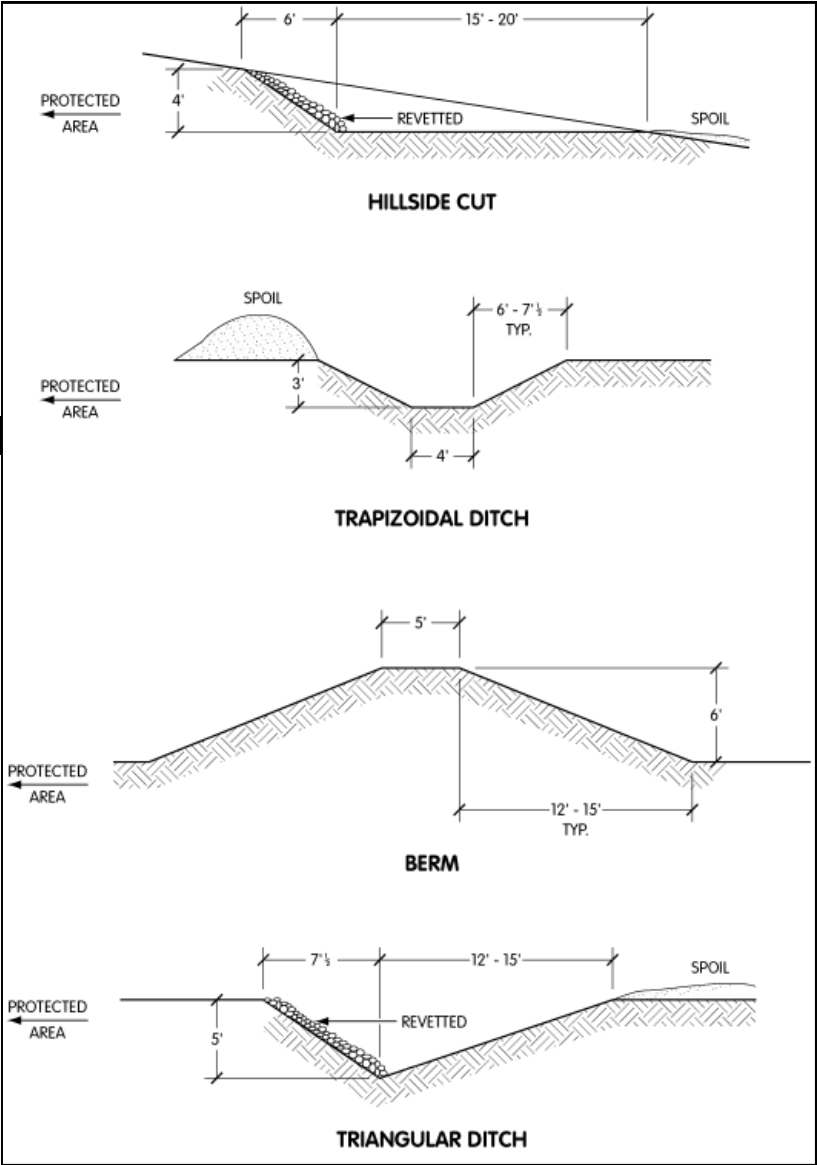


Figure 12-12. Berm and Ditch Designs (From MIL-HDBK-1013/14)

and size can be used as expedient barrier systems. If used, these expedient barriers should be stabilized and anchored to prevent displacement by a threat vehicle. Typical expedient barrier techniques include:

- Three-foot (0.9 m) sections of large-diameter, corrugated metal pipe or reinforced concrete culvert can be placed on end and filled with sand or earth.
- Steel pipe can be stacked and welded together in a pyramid.
- Construction or military vehicles can be anchored together with cable or chain. To increase effectiveness, the cable or chain can be anchored to adjacent anti-vehicle barriers such as concrete barriers.
- Destroyed or captured enemy vehicles can also be used as expedient anti-vehicle barriers.
- Heavy-equipment tires, 7 to 8 ft (2.1 to 2.4 m) in diameter, half-buried in the ground and tamped so they are rigid can be effective vehicle barriers (See Figure 12-15). Buried equipment tires were tested<sup>4</sup> against a 3,350 lb. (1,523 kg) vehicle, traveling at 51 mph (82 kph). The vehicle penetrated the barrier 1 ft. (0.3 m). The tires were 36-ply with an 8-ft. (2.4 m) diameter. They weighed 2,000 lb. (909 kg) each.

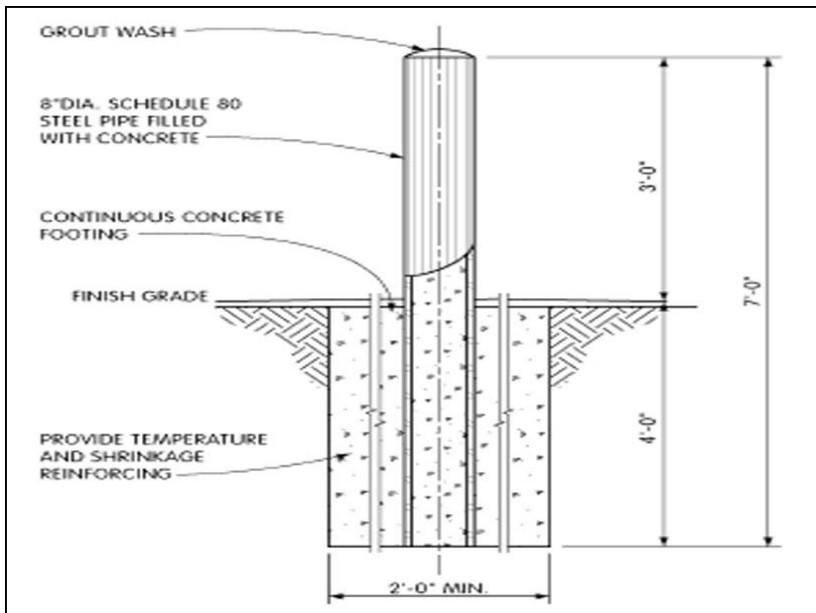


Figure 12-13. Typical Bollard Construction Detail  
(From MIL-HDBK-1013/14)

4. See MIL-HDBK-1013/14, *Selection and Application of Vehicle Barriers*, p. 67.



Figure 12-14. Typical Cabled Steel Hedgehog Obstacle

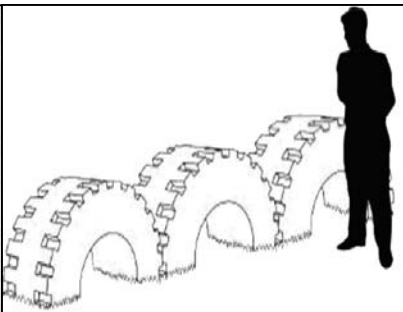


Figure 12-15. Typical Heavy Equipment Tire Barrier Construction  
(From MIL-HDBK-1013/14)

## Soil-Filled Barriers

Soil-filled barriers are typically employed at a FOB to provide blast and fragment damage protection. As fragment protection, these barriers work extremely well. For blast mitigation purposes these barriers reduce structural damage only slightly by reducing reflected pressures to incident pressure levels. However, soil-filled barriers can also be effective as anti-vehicle barriers. See Appendix D for additional soil-filled container applications.

**Wire and Fabric Container.** Wire and geotextile fabric containers can be used to construct anti-vehicle barriers and are often favored because of their capability to minimize transportation weight and volume requirements, while optimizing the provided level of threat protection. When utilized as an anti-vehicle barrier, the barrier is normally built with a two-row-wide base and at least a second level in order to provide sufficient mass to stop a vehicle (see Figure 12-16). Tests by the USAF Force Protection Battlelab<sup>5</sup> showed that this design effectively stopped a 15,000 lb. truck traveling at 30 mph.

**Metal Container Revetment.** Metal container materials can also be used to construct anti-vehicle barriers (See Figure 12-17). Like the wire/fabric container, these barriers have the capability to minimize transportation weight and volume requirements, while optimizing the provided level of threat protection. The advantage of using this material is that the metal material can be collapsed and stacked during transport and expanded and filled at the final destination.

5. See Lauritsen and McKay, "Design and Evaluation of Novel Counter-Mobility Barrier Systems," pp. 3-4.

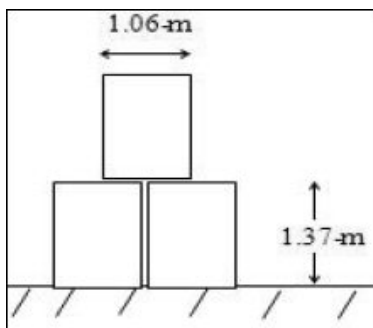


Figure 12-16. Wire and Fabric Container Barrier Concept



Figure 12-17. Typical Metal Container Revetment Barrier

## Gates

Gates facilitate control of authorized traffic and its flow. They establish specific points of entrance and exit to an area defined by fences. They also function to limit or prohibit free flow of pedestrian or vehicle traffic, while establishing a traffic pattern for restricted areas. Gates, as a part of perimeter fences, must be as effective as their associated fence to provide an equivalent deterrent. Gates will normally require additional hardening features because of their location across entrance roads and the inherent vulnerability of their hinges and latches. Gates are known to be the weakest point in the perimeter security fence and as such, planners must pay attention to their requirements when designing security fencing.

**Personnel Gates.** Personnel gates should be designed to permit only one person to approach security personnel at any time. Examples of personnel gates include single swing gates, double swing gates and turnstile gates. For pedestrian use, single swing gates should be considered as the second alternative to turnstile gates (See Figure 12-18). Operational and security personnel requirements should be considered to determine the best type of personnel gate for a FOB.

**Turnstile (Rotational) Gates.** Turnstile gates (See Figure 12-19) are manufactured as single or tandem units. Only full height turnstile gates should be considered. Direction of travel can be set for clockwise, counterclockwise or bi-directional. Automated access control systems, such as card readers, push button and wireless remote can be incorporated into turnstile gates. Tubing should be at least 1-1/2 in. diameter, 14 gauge (38 mm). Overall exterior height is 91 in. (2.3 m) with a pedestrian walk-through height of 84 in. (2.1 m).

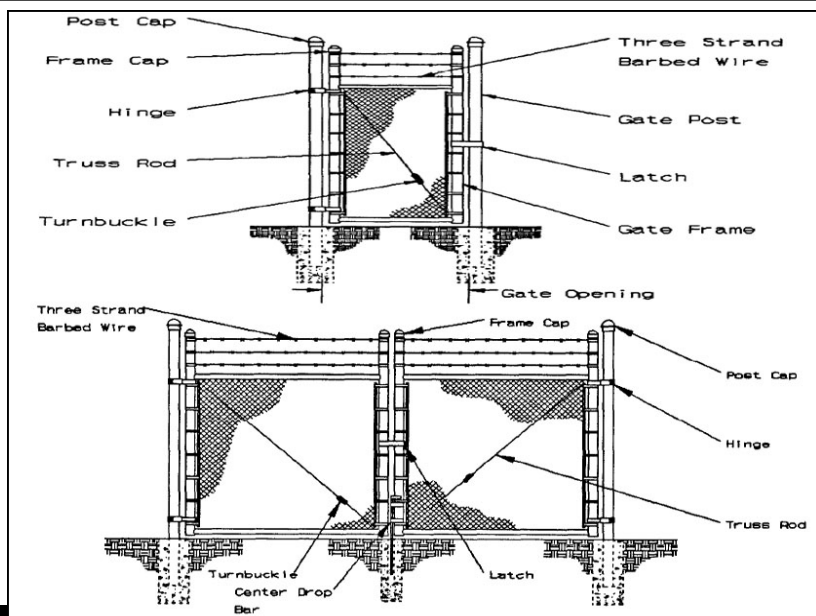


Figure 12-18. Typical Personnel Gates (Top: Single-Swing; Bottom: Double-Swing)  
(From MIL-HDBK-1013/10)

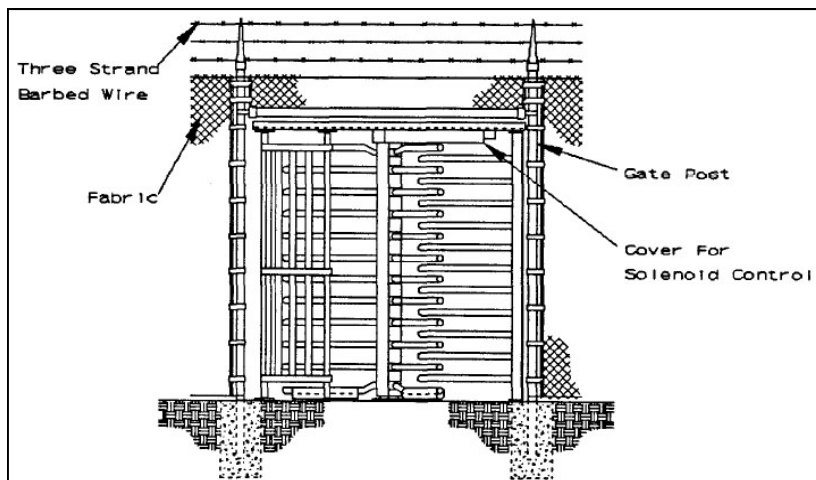


Figure 12-19. Typical Turnstile (Rotational) Gate  
(From MIL-HDBK-1013/10)

**Cabled Crash Beam and Drop-Arm Barriers.** This is the most commonly used active barrier at FOBs. One end of the barrier is anchored to surrounding Jersey barriers to add weight and strength to the barrier. The crash beam is kept in the lowered position with the bolt engaged in the cable loop on the free end of the crash beam and connected to another Jer-



sey barrier system. The crash beam is raised only to allow authorized entry. See Figure 12-20 for examples.

**Metal Crash Gates.** High-impact gate designs should be installed in the ECP if the speed of approaching vehicles is expected to be great. Crash gates are specifically designed to resist heavy vehicle impact (See Figure 12-21). These systems are typically used where a wide opening is required or where appearance is an issue. They may be electromechanically operated. Since they are designed to resist vehicle impact, they are typically constructed of heavy steel and require extensive construction to successfully implement them. They have successfully stopped heavy (15,000

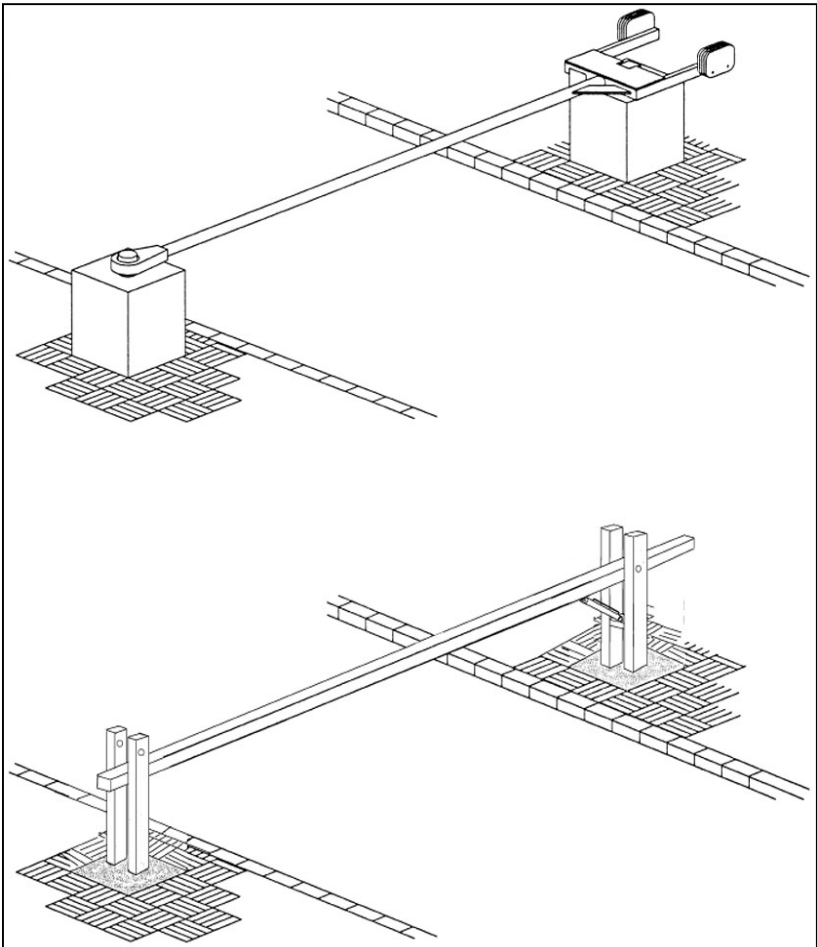


Figure 12-20. Typical Drop-Arm Barriers (Above: Delta TT212; Below: SEMA-4)  
(From MIL-HDBK-1013/14)

lb/6,818 kg) vehicles traveling at speeds of less than 40 mph (65 kph). A USAF Force Protection Battlab design stopped a 15,000 lb. truck traveling at 50 mph.

**Cable-Reinforced Chain Link Fence Gates.** If cable-reinforced chain link fence gates are used to secure a FOB, then wheel-supported or cantilever sliding gates are the best selection for vehicle security (See Figure 12-22). Swing gates are the least desirable because they require a large arc of space for operation. That large sweeping arc can cause the ECP to be more vulnerable.

**Military Vehicle/Heavy Equipment/Trucks.** If conventional barriers are not available, a military vehicle, truck, or other heavy vehicle (bulldozer, dump truck) can be used to block an entrance. To increase its effectiveness, a cable should be run through the frame of the truck and anchored to adjacent barriers.

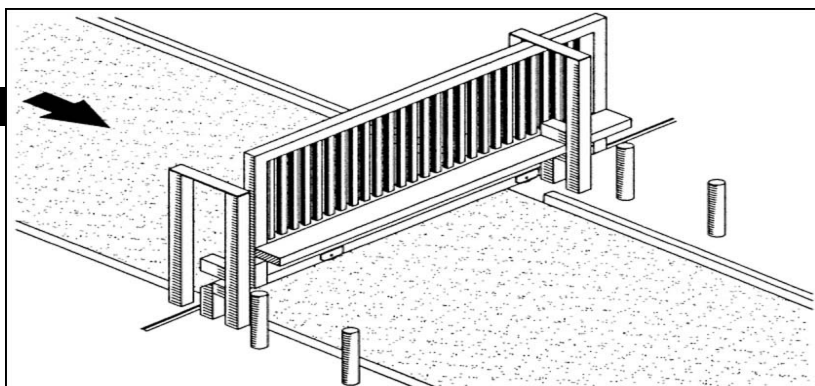


Figure 12-21. Typical Crash Gate (From MIL-HDBK-1013/14)

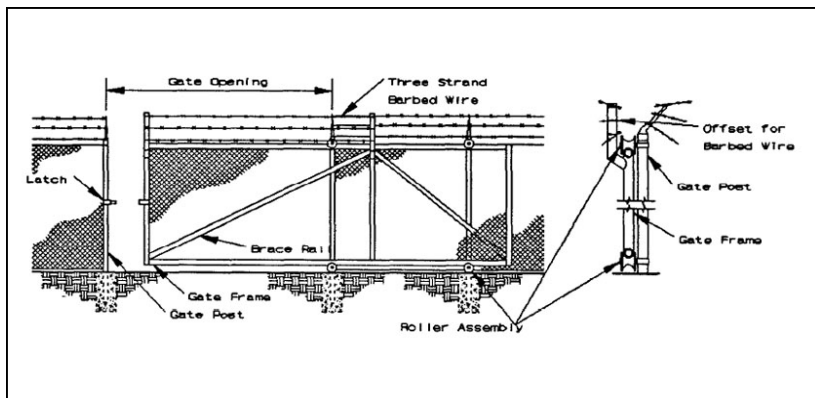


Figure 12-22. Single Cantilevered Gate (From MIL-HDBK-1013/10)

## Physical Barriers Considerations

Barriers should be emplaced in concert with each other, the natural terrain, and any man-made obstructions. In many instances when a single barrier cannot stop a vehicle, a combination of barriers can. Combinations or layers of barriers are more effective than a single barrier in high threat environments. The recommended combination of barriers for the small FOB is a double perimeter wall system (see discussion for Joint Combat Outposts in Chapter 21).
Combinations or layers of barriers are more effective than a single barrier in high-threat environments.
If used in combinations, barriers must afford an equal degree of continuous protection along the entire perimeter of the FOB.
Combinations or layers of barriers should be separated by a minimum of 30 feet (9.15 m) for optimum protection and control.
When a section or sections of natural/man-made barriers provide less than optimum protection, other supplementary means to detect and assess intrusion attempts should be used.
Barriers should be augmented by security force personnel or other means of observation and assessment.
An unobstructed area or clear zone should be maintained on both sides of and between physical barriers.
Barriers should be positioned far enough away from other structures (trees, telephone poles, antenna masts, or adjacent structures) that may be used as aids to circumvent the barrier.
Barriers should not be placed where vehicles can park immediately adjacent to them, thereby affording attackers a platform from which to mount an attack.
Additional toppings on barriers should be considered, both for outer and inner perimeter walls. These include concertina wire, multiple-strand razor or barbed wire, or other devices that inhibit adversary efforts to vault or go over the top of the barrier.
Barriers should be considered as excellent platforms on which to mount surveillance systems and intrusion detection devices.
The potential for debris and fragment hazard should be considered when concrete barriers are used; soil-backed concrete barriers help to mitigate debris and fragments.
Barriers should be continuously monitored and kept under observation by security force personnel and patrolled frequently; perimeter barriers can be assessed by intrusion detection systems, if available; overwatch and final protective fires should be integrated into and fully support the perimeter barrier system.

	<p>Temporary walls or rigid barriers should be considered. They deny access and protect against high-speed vehicle penetrations. Types of materials for consideration include:</p> <ul style="list-style-type: none"> <li>• Concrete barriers (Jersey, Texas, Alaska, Bitberg barriers)</li> <li>• Concrete or sand-filled oil drums</li> <li>• Concrete bollards or planters</li> <li>• Steel or steel-reinforced concrete posts</li> <li>• Sand or water-filled plastic vehicle barriers</li> <li>• Soil-filled barriers (wire/fabric barriers; metal revetments)</li> </ul>
	<p>Vehicles in all sizes and configurations should be considered as expedient barriers. Parked bumper-to-bumper, vehicles provide an effective barrier to personnel. Large construction-type vehicles or armored vehicles (including destroyed and captured enemy vehicles) can be very effective as supplemental barriers behind gates to FOBs or as a temporary serpentine in entry control points.</p>
	<p>Barriers installed in clear zones must be designed so that they do not provide adversaries with a protective hiding place or shield.</p>
	<p>Perimeter barriers should be kept under observation and patrolled frequently.</p>
	<p>The placement of barriers should maximize standoff; for example, perimeter barriers should be located as far from critical assets as possible to mitigate blast effects.</p>
	<p>Barriers should be fully integrated to form a continuous obstacle around the FOB, capable of stopping possible vehicle threats.</p>
	<p>Barriers, sensors, and final protective and overwatch fires should be integrated and should fully support each other. In many instances when a single barrier cannot stop a vehicle, a combination of barriers can.</p>
	<p>Barriers can be compromised through breaching (cutting a hole through a fence or placing explosive near a concrete barrier) or by nature (berms eroded by the wind and rain); therefore, barriers should be inspected and maintained frequently.</p>
	<p>Barriers at the perimeter can help conceal and shield FOB activities from direct observation and surveillance.</p>
	<p>If possible, barriers should not be placed where vehicles can park immediately adjacent to them. A vehicle bomb adjacent to a concrete barrier can break the barrier into "secondary" fragments that are thrown at high velocity into the FOB and occupied structures.</p>

# Entry Control Structures

## Introduction

Entry control points (ECPs) and facilities<sup>1</sup> must remain functional and an essential aspect of the FOB access control system regardless of the level of threat. The type of access<sup>2</sup> provided at the ECP should be a principal factor in the design of the ECP. Numerous factors should be considered when commanders are determining the type of access at a FOB, including threat, FOB mission, FOB operations, and available security personnel. The preferred type of access for an ECP is one that limits all pedestrian and vehicle access to mission-essential personnel only. The ECP design should anticipate increased traffic volume and should support the employment of required force protection condition (FPCON) measures and random antiterrorism measures (RAMs). The total number of ECPs should be kept to a minimum.

## Functional Zones

An entry control point should be subdivided into functional zones, each encompassing specific functions and operations. These zones are described below.

**Approach Zone.** The approach zone is the initial interface between the off-site road network (public highways) and the FOB. The length of the approach zone should be based on available land, distance required for queuing and performing traffic sorting, and the space required for additional lanes of traffic to prevent traffic from backing up excessively onto adjacent public highways. Space may also be required to support additional speed management techniques to mitigate high-speed threats. The approach zone should include design elements that accomplish the following functions and operations:

- Reduce the speed of incoming vehicles
- Sort traffic by vehicle type
- Allow for verification of authorized access of personnel and vehicles
- Provide adequate stacking distance for vehicles waiting for entry
- Provide the first opportunity for early warning to identify potential

1. In this handbook entry control structures refer to physical structures (gates, roads, fences, barriers, etc.) and facilities (buildings, inspection areas, etc.). ECP generally refers to a location on the perimeter that facilitates entry to a FOB.

2. Refer to Chapter 9 for more details on access control procedures.

threat personnel/vehicles, including those attempting entry through the outbound lanes of traffic

**Access Control Zone.** The access control zone is the main body of the ECP. It includes guard facilities, vehicle and personnel inspection areas, and traffic management equipment used by the security forces. The design of the access control zone should be flexible enough to ensure the infrastructure can support future inspection demands, access control equipment, and technologies. The access control zone should include design elements that support the following functions and operations:

- Verification of personnel identification
- Random or 100-percent inspection of personnel and vehicles
- Visitor control (issue of visitor/vehicle passes)
- Overwatch for approach zone
- Maintenance of vehicle speed management/reduction techniques

**Response Zone.** The response zone is the area extending from the end of the access-control zone to the final denial barrier or gate to the FOB. This zone defines the end of the ECP. The response zone should be designed so security personnel can carry out the following functions:

- Provide time to react to a threat, operate the final denial barriers, and close the gate, if necessary
- Monitor overwatch for the entire entry control facility
- Define the FOB perimeter

**Safety Zone.** The safety zone extends from the passive and active barriers in all directions to protect site personnel from an explosion at the ECP. Acceptable standoff distance, or safety zone, must be determined by an assessment of the threat (specifically, expected weight of the explosive charge) and the FOB or asset to be protected. If an adequate safety zone or standoff distance cannot be achieved to produce acceptable damage and injury levels, other alternatives must be evaluated or a decision made to accept additional risk.

The diagram in Figure 13-1 is an example of the functional zones and design concepts that should be incorporated into an ECP located in an expeditionary environment. For illustration purposes, this example can be considered a multi-purpose ECP since several types of entry control operations are combined in one location.

### Overwatch

An overwatch position is a manned position that provides observation and has the ability to employ deadly force against vehicles and attackers at-

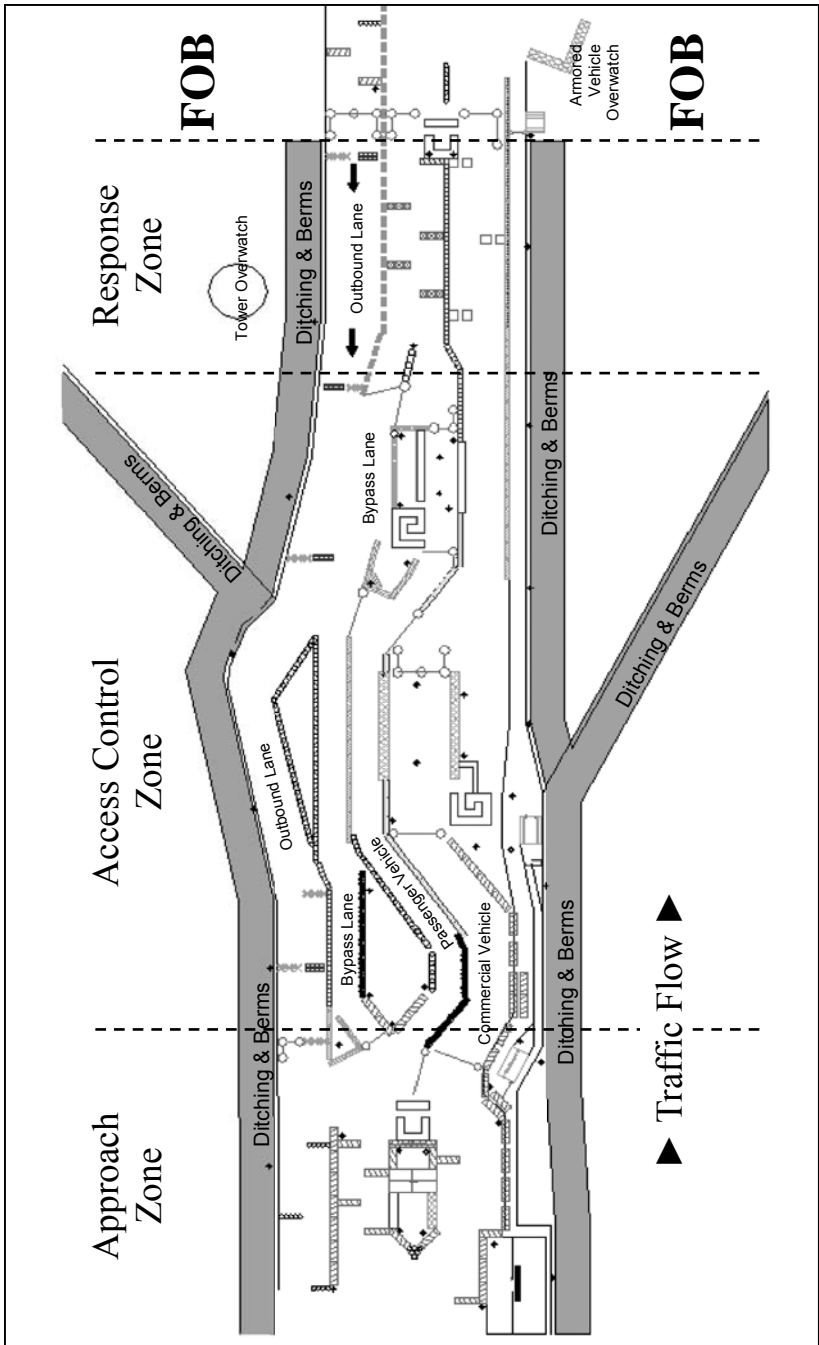


Figure 13-1. Example of Entry Control Functional Zones Concept  
(From USACE ERDC)

tempting to bypass, ram, or otherwise run through an entry control point (ECP). The overwatch should be planned and designed with the same considerations as those used against an ambush--fix the enemy in place so they can be killed. *First*, establish a kill zone where the overwatch can engage hostile vehicles. *Second*, place barriers to slow down the hostile vehicle and keep it in the kill zone as long as possible. *Third*, position the overwatch to provide effective engagement of the target in the kill zone

The overwatch should be equipped with a weapon that can stop a vehicle by disabling it or killing the driver. The preferred weapon system should be no smaller than a medium machine gun (usually M60 or M240G). Heavy guns (for example, the M2 .50-caliber machine gun or MK19 40-mm grenade launcher) are also likely to stop a vehicle. Antitank weapons such as the M136 AT-4 light antitank weapon could also be used for overwatch purposes.

Once the kill zone is established, the maximum range of the weapon system's field of fire should be evaluated to determine the risk to friendly guard posts, HN buildings, and personnel possibly in the likely field of fire (range fan). All overwatch positions should have range cards that denote the weapon system's principal direction of fire (PDF), distances to key terrain features or landmarks, and the final protective line (FPL). The use of range cards will enhance the gunner's ability to quickly zero in on a target, determine ranges, and estimate ranges to other targets. Some weapon systems have a required minimum range to activate the round. The kill zone must be beyond that minimum range for all weapon systems designated for the overwatch position.

The overwatch weapon system should require minimal traverse and elevation (T&E) adjustments to continually bring fire on the kill zone. Large and strong firing stakes should be used if a T&E device is not available to define the fields of fire for the gunner during darkness or periods of low observation.

Finally, rules of engagement criteria should be well defined and readily available for the overwatch position. In determining a location for the overwatch, security forces should consider the questions in Figure 13-2.

### **Design Concepts**

Entry control design should not detract from the FOB's mission and operations. The following design concepts should be consistent with all ECPs:

**Security.** The FOB perimeter is the first line of defense. The first priority of an ECP is to maintain perimeter security. The ECP must be designed to



## Overwatch Consideration Questionnaire

- Can the overwatch clearly observe the ECP and its barriers?
- Is the overwatch able to clearly determine the circumstances under which he is authorized to employ his weapon?
- Is the overwatch able to engage a hostile vehicle while it is at least 100 meters away?
- What is the effective causality radius (ECR) of the ammunition used in the overwatch weapon system?
- What are the maximum and minimum ranges of the ammunition?
- Are friendly troops (to include HN troops and civilians) located within the operational zone of the weapon system?
- Will rounds ricochet or skip towards friendly troops?
- Can the overwatch employ weapons in less time than it takes a vehicle to drive through the kill zone?
- Will the overwatch be able to engage the target for 10 – 15 seconds?
- How much distance does the overwatch have to engage the target vehicle?
- Can the weapon bring enfilade fire to bear on the hostile vehicle?

Figure 13-2. Overwatch Considerations Questionnaire

have security features that protect against vehicle-borne threats and illegal entry. The ECP must be designed so that it does the following:

- Facilitate access control
- Enhance the defense-in-depth concept
- Provide effective risk mitigation
- Accommodate random antiterrorism measures (RAMs) for sustained operations
- Operate during all force protection conditions (FPCONs), including 100% vehicle inspections

**Safety.** ECPs must have a working environment that is both safe and comfortable for FOB security personnel. Security personnel safety includes provisions for personal protection against attack and errant drivers.

**Capacity.** The ECP must maximize vehicle traffic flow to eliminate undue delays that would affect FOB operations while maintaining vigilance against attacks.

**Image.** The ECP must be designed to impart an immediate impression of professionalism and commitment to excellence and to convey the FOB's commitment to the protection and safety of personnel.

**Roadways.** Entry roads to FOBs and to individual buildings should be designed so that they do not provide direct or straight-line vehicle access to high-risk assets. Parking areas should be located away from high-risk FOBs and critical assets to minimize blast effects from potential VBIEDs. Signs identifying high-risk FOBs and critical assets should be kept to a minimum. ECPs should have a dedicated right-of-way protected from encroachment by buildings, trees, and other objects.

A major factor in determining the type of ECP should be the size of vehicles requiring entry. The minimum lane widths for an ECP should be 10 ft. (3.0 m). The preferred lane width is 12 ft. (3.6 m). Lanes approaching the gate should be 12 ft. (3.6 m) wide, plus another 2 ft. (0.61 m) on each side for the curb and gutter.

The ECP design should provide a way for an unauthorized vehicle that enters the ECP to be rejected and for an authorized vehicle that enters the wrong ECP to be redirected with minimal impact on traffic flow. The following are recommended turnaround dimensions.

- Locations serving only passenger vehicles: 15 to 30 ft. (4.57 to 9.14 m); preferred width is 20 ft (6.1 m)
- Corners where RVs, SUVs, or similar vehicles turn: 35 ft. (10.67 m)
- Intersections where large trucks (WB-50), including semi-trailers (WB-67) turn: 150 ft. (5.24 m)
- Turnarounds for large trucks: 65 ft. (19.81 m)

**Sidewalks.** When pedestrian access control is required, the ECP design should ensure that proper sidewalk and safety provisions direct pedestrian traffic to the approach zone and separate it from vehicle traffic and ensure pedestrian walkways are integrated into the existing site layout. Pedestrian walkways should maintain a minimum width of 4 ft (1.2 m). Pedestrian access control should be designed with limited obstructions to ensure that security personnel can maintain visual contact with the pedestrians as they approach the ECP.

**Gates.** The ECP typically ends at the FOB perimeter. The ECP should have a gate or final denial barrier, enabling the ECP to be closed at the FOB perimeter when not in use. The gates at ECPs should maintain a level of security equivalent to that of the adjacent perimeter fence/barriers. The most common active barriers are cabled crash-beam barriers, also known as drop-arm barriers. Other active barriers include hydraulic rams

and metal crash gates. At a minimum, fence gates should be reinforced with cables to increase resistance to a moving vehicle threat. Gates should be capable of denying access to both vehicles and personnel. Gates are discussed in detail in Chapter 12.

## **Perimeter Barriers**

Barriers can be used to accomplish many of the design concepts required for ECPs in high-threat environments, to include containment, segregation and compartmentalization of vehicles, rejection of unauthorized vehicles, and vehicle speed management. In order to minimize cover and concealment positions for aggressors, barriers should have a limited profile. Barriers are not, in and of themselves, final security solutions. They complement the employment of other physical and procedural security requirements. The most effective barrier designs use a combination of speed management techniques. More information on barriers can be found in Chapter 12.

ECPs should provide full containment and control of vehicles. Barriers should be arranged to ensure that a vehicle does not circumvent the ECP once the vehicle has entered the approach zone. Barriers should encompass a contiguous perimeter around the ECP, with the final denial barriers completing the containment. Roadway containment is necessary to prevent unauthorized vehicle access and should extend from the approach zone to the response zone or final denial barrier in order to be effective. The selection of passive and active anti-vehicle barriers should be based on their capacity to stop threat vehicles.

Containment may also be accomplished with natural or constructed barriers. Natural barriers may consist of a dense tree stand, berms, or drainage ditches on either side of the roadway; berms and ditches should have slopes that prevent vehicles from passing over the obstruction. Constructed barriers may include cable-reinforced fencing, concrete walls, etc. Consideration should be given to the potential debris hazard produced by passive barrier systems exposed to blast during a potential attack and the effect on nearby personnel, buildings or assets.

Barriers around a search area should force the driver to ram through a gate or barrier, clearly demonstrating hostile intent to the overwatch. Anti-vehicle barriers must not obstruct fields of vision or fields of fire for the overwatch or backup security forces.

Breaks may be provided in the passive barriers surrounding the ECP to allow pedestrian access to the ECP. Any break in the passive barrier

should not exceed 3 ft. (1 m) in width. Access control systems (primarily turnstiles) should be considered and incorporated, if possible. If included, they should ensure control and prevention of possible tailgating.

If the ECP incorporates electronic barriers, lighting, or communication systems, an electrical design must be prepared. Design considerations include power requirements for future traffic control devices, identification equipment, and other devices associated with potential automation of the ECP. In the event of a loss of the primary electrical source, a reliable alternate power source is necessary to ensure continuous operation of the ECP. A standby generator or other equivalent means should be used as the alternate electrical power source.

**Tire Shredders/Puncture Strips.** These systems should not be considered vehicle barriers and are included here only as an option for slowing a vehicle either prior to its impact with a barrier or in an area where two to three times the required standoff distance between the entry point and the protected structure is available. A vehicle which speeds over shredders/puncture strips will identify itself to the overwatch as having hostile intent. Tire shredders/puncture strips also prevent friendly vehicles from accidentally running through an ECP and receiving fire from the overwatch. Although tire shredders/puncture strips will not stop a vehicle, they may help cause a vehicle to lose control when combined with other obstacles. These systems may not be effective against modern “run flat” tires, heavy-duty, off-road truck tires, or extra-wide tires that can bridge over two or more spikes (See Figure 13-3).

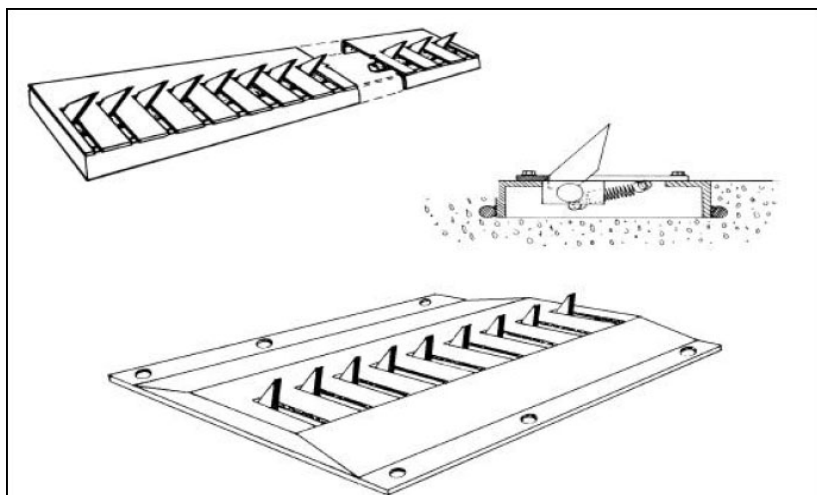


Figure 13-3. Typical Tire Shredders  
(From MIL-HDBK-1013/14)

## Search and Inspection Areas

Search requirements for trucks/commercial vehicles and passenger vehicles differ significantly. When possible, truck/commercial and passenger vehicle traffic should be segregated and compartmentalized, with separate search areas constructed for each. Separate search areas help avoid congestion and improve the efficiency of searches during 100% inspections.

If space is available, inspection/search areas should be exclusive, separate, and offset from traffic lanes – this layout facilitates the by-pass of vehicles, if needed. The minimum width should be 18 ft. (5.5 m) to facilitate the safe inspection of vehicles. The length of a pull-off area or inspection area should be a minimum of 40 ft. (12.2 m) or the length required to support the largest vehicle expected at the ECP, whichever is larger.

As a minimum, the FOB should provide the following inspection areas:

- For standard vehicles: 15 x 25 ft. (4.5 x 7.2 m) inspection bays that can be enclosed, if necessary, to protect inspection equipment in the event of bad weather
- For commercial vehicles: 18 x 80 ft. (5.5 x 24.4 m) wide by 17 ft. 6 in. (5.4 m) high inspection bays that can be enclosed to protect inspection equipment in the event of bad weather

Concepts that should be incorporated into ECP search area design include the following:

**Parking Area.** A parking area should be established outside the ECP and search area. This location will help to discourage and restrict vehicles from requesting access into the FOB. Personnel who do not need to drive into the FOB should park in this area, thus limiting traffic to mission essential vehicles. The parking area should remain under constant observation by security personnel and should be regularly searched with MWDs. The parking area should be at a distance that provides adequate standoff for inhabited areas.

**Staging Area.** Enough space (distance from Approach Zone to Access Control Zone) should be available to stack and stage vehicles awaiting search. If possible, personnel awaiting search should not be able to observe the search procedures.

**Blast Mitigation.** Berms or earth-filled barriers should be placed around the search pit to protect nearby personnel from fragmentation should a bomb-laden vehicle explode while being searched.

**Obscured Search Area.** Berms, camouflage netting, or other types of screening should be used to obstruct observation of the search area from personnel outside the FOB.

**Driver and Passenger Holding and Search Area.** The driver and passengers of a vehicle should be staged where they cannot observe search procedures. This holding area should not protect the driver and passengers from an explosion. Drivers and passengers should be searched while in this holding area and should be kept under constant observation by an armed guard not involved in searching them or the vehicle.

**Military Working Dog (MWD) Rest Area.** Extreme heat and sun cause fatigue and reduce the effectiveness of the MWDs. Those not actively engaged in searching vehicles should be kept in an air-conditioned tent or room to extend their effectiveness. Other measures to improve dog endurance include cold collars, cooling-mist fans and dog shoes.

**Shade.** In order to maximize the effectiveness of security personnel and MWDs, the search area should have overhead protection from the sun.

**Ramps/Search Pit.** Vehicle ramps and a mechanic's (search) pit should be provided to allow searchers the most effective means to visually inspect the undercarriages of vehicles. This method is the only way to thoroughly search the underside of vehicles. However, the use of automated under vehicle inspection systems, rather than mirrors or search pits is recommended to remove security forces from danger.

**Mirrors.** Though less thorough than vehicle ramps or pits, mirrors should be used to detect poorly or hastily concealed explosives placed near the outer edges of a vehicle. The mere act of searching underneath a vehicle can be a psychological deterrent to terrorists.

**Floor.** If no search pit is available, the floors of search areas should be flat and hard to allow searchers to crawl underneath vehicles on a creeper. Flooring which would create a suitable surface is asphalt, concrete, AM2 matting, or plywood. Astroturf or other similar matting placed over the floor helps protect MWDs' feet from the heat of the ground.

**Illumination.** Search pits should be well illuminated to allow searchers to see all portions of the vehicle. Lighting mounted on ramps or in a mechanic's pit helps searchers conduct detailed underbody searches. Security personnel should have flashlights or extension lamps available for use.

**Closed Circuit Television (CCTV).** CCTV can record vehicles entering an ECP for observation by another post and for later review. Cameras

should be positioned to prevent vehicle or perimeter lights from blinding the camera. Cameras placed outside should be protected from the environment.

**Electronic Bomb Detection Devices.** There are many commercially available bomb detection devices available that utilize backscatter or transmission imaging. These can be used at ECPs to augment bomb detection capabilities.

## Exit Points

Approaches to all vehicle exit points should be designed so that high-speed approach from outside the perimeter is not possible. The goal is to ensure to the maximum degree possible that attackers cannot simply enter the FOB by going against the flow of exiting vehicle traffic.

An active barrier should be used to maintain positive control over an exit lane and to prevent someone from entering the FOB through the exit. The active barrier should be bounded by measures (such as serpentine and speed bumps/tables) that slow vehicle traffic from both outside and inside the installation before it reaches the active barrier. All entry-exit points should be constructed with protection against a ramming-vehicle attack. Passive vehicle barriers can be incorporated to make ramming attacks difficult. Additional vehicle barriers can be installed behind the gates to provide defense in depth against such attack.

## Speed Management Techniques

Two elements affect a vehicle's ability to breach an obstacle: speed and weight. The speed of a hostile vehicle can be managed by use of techniques in the design that force the vehicle to slow down in order to enter or negotiate the traffic lanes. Speed management techniques and considerations include: sharp 90-degree turns into the ECP from surrounding road network, traffic circles leading into the ECP, and nonlinear lane designs.

An attacking vehicle's velocity at impact will depend on its engine and transmission system and the distance over which the vehicle accelerates before impact. In addition to velocity, the approach angle of the vehicle is important. This angle can be dictated by the layout of the compound and the surrounding roads and buildings.

In many situations, an attacking vehicle will have to turn before a final straight-line approach. In these cases, the impact speed will be restricted by the maximum cornering speed. After completing its final turn, the at-

tacking vehicle can then accelerate in a straight line until it strikes a barrier. Steep grades also factor into the velocity calculations: an uphill grade will reduce the vehicle's impact velocity, while a downhill grade will increase the velocity.

As an example, a typical 2.5 ton truck can reach a speed of 30 mph in 170 feet along a straight level section of concrete road and can maintain that speed through a 60 foot radius curve. Similarly it can reach a speed of 50 mph in 470 feet and take a 170 foot radius curve.

A very effective yet simple speed management technique involves the use of a serpentine obstacle pattern. A layout of lanes with anti-vehicle barriers (such as concrete barriers, concrete blocks, earth-filled barriers, and cabled steel hedgehogs; See Chapter 12) forces vehicles to slow down as they traverse the obstacles. For example, a road with a 30 ft width would require a barrier separation distance of 40 ft (12.2 m) in order to slow a vehicle to a maximum speed of 20 mph. See Table 13-1 and Figure 13-4 for other combinations of road width and vehicle speed. The tighter the serpentine or "S" turns, the more the vehicle must slow down.

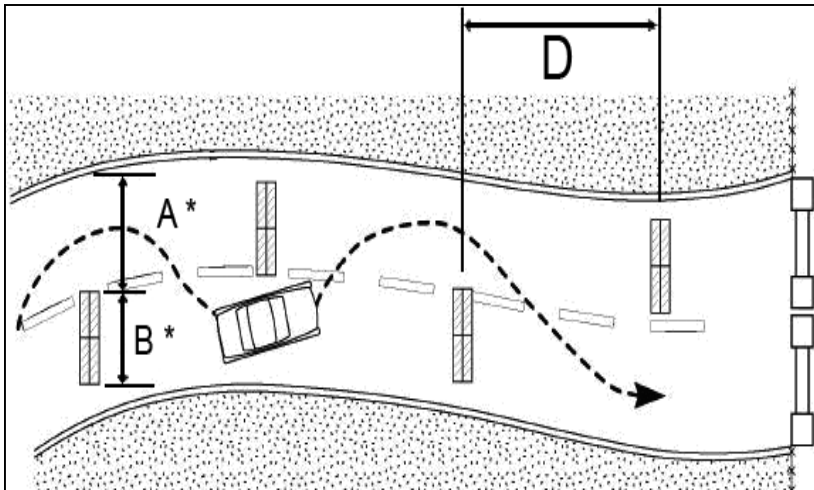
Speed bumps and tables are large enough to cause small vehicles to bottom out, thus slowing the vehicle or denying access through the lane. Speed tables slow vehicles to a lesser degree than speed bumps do.



Table 13-1. Separation Distance (D)\* for Barriers to Reduce Speed on a Straight Path in Feet (meters)  
(From MIL-HDBK-1013/14)

Achievable Speed of Vehicle on a Curve ► Road Width ▼	20 mph (32 kph)	30 mph (48 kph)	40 mph (64 kph)	50 mph (80 kph)	60 mph (97 kph)
20 ft (6.2 m)	28 (8.5)	43 (13.1)	58 (17.7)	73 (22.2)	87 (26.5)
30 ft (9.3 m)	40 (12.2)	63 (19.2)	86 (26.2)	108 (32.9)	130 (39.6)
40 ft (12.4 m)	47 (14.3)	77 (23.5)	106 (32.3)	134 (40.8)	161 (49.1)
50 ft (15.3 m)	51 (15.5)	87 (26.5)	122 (37.2)	155 (47.2)	187 (57.0)
60 ft (18.3 m)	54 (16.5)	96 (29.2)	135 (41.1)	172 (52.4)	209 (63.7)

\* Based on Friction Coefficient (f) = 1.0



\*A — 12 Feet Maximum; \*B — Varies Depending on Road Width

Figure 13-4. Barrier/Block Serpentine Layout to Reduce Speed  
(Use with Table 13-1 above)  
(From MIL-HDBK-1013/14)

### ECP Site Selection Considerations

Site selection for a new ECP begins with an extensive evaluation of the following:

Anticipated demand/usage

Traffic origin and destination and patterns

Capability of the surrounding road network to tie-in to the ECP, including its capacity to handle additional traffic

Future expansion and modifications necessitated by increased demand or revised security measures

Space for parking

Buffer and transitional space between ECP elements

Standoff requirements

The existing terrain and available space

ECP function (ECP categories include *Primary* (open continuously); *Secondary* (regular hours, closed at times); or *Pedestrian Access* (hours vary))

Additional key concepts that should be incorporated into an ECP design:

Layered defense

Nonlinear design

Maximized protection for ECP personnel (multiple guardhouses)

Maximized standoff

Traffic and pedestrian segregation and channeling

Multiple vehicle turn around/rejection areas

Vehicle speed management/reduction through the use of serpentine and vehicle barriers

Segregated search areas with line-of-sight denial from possible external surveillance

Overwatch positions (hardened fighting positions)

Hardened perimeter gate access (final denial barrier)

Further details can be found in UFC 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*.

# Sidewall Protection

### Introduction

Sidewall protection involves walls or barriers designed to stop fragments and reduce blast effects from near-miss impacts of RAM rounds (See Figure 14-1). Revetments are simply walls designed for this purpose. The primary uses of revetments on the FOB are (1) as walls and vehicle barriers along the FOB perimeter and at entry control points; (2) as a means of providing full-height sidewall protection for soft-sided structures such as tents and trailers; and (3) as free-standing walls to protect mission-critical equipment. One of the most efficient materials for stopping fragments is a dense granular soil such as sand. Thus, most revetment designs are just variations of techniques to hold the soil in a vertical position. Some revetment designs can also function as vehicle barriers.

### Sandbags

Sandbags are a traditional method to provide protection from fragmentation. A sandbag wall can be constructed to be either freestanding or supported on one side by the structure it is protecting. For tents, a freestand-



Figure 14-1. Full-height sidewall protection example

ing wall 6 to 7 ft. high should be constructed. For trailers, the wall may need to be higher (8 to 9 ft.) to account for the additional crawl space under the trailers. One sandbag requires about 0.3 cubic feet (0.011 cubic yard) of sand. Twelve bags provide a wall 1 foot high by 4 feet long.

*Performance.* Numerous tests have shown that a minimum of two layers (wall approximately. 16 in. thick) of sandbags should be used for protection from the blast and fragmentation of near-miss (4 ft.) hits of the 82- and 120-mm mortars and 122-mm rocket.

*Construction Procedure.* Fill sandbags with clean dry sand or any granular material (Loose gravel or crushed rock is prohibited since it can become a secondary fragment source in the event of a high-explosive threat). Stack filled sandbags in the manner indicated in Figure 14-2. Be sure to stagger joints and use header layers for a more stable wall. Tamp the top of each sandbag with a flat object to stabilize the wall. Always place the closed end of the bag and side seams inward and away from the direction of the threat. Construct the sandbag wall high enough to protect the asset from incoming projectiles and fragment spray. The only equipment required is shovels.

*Limitations.* Constructing a sandbag wall is manpower intensive and time consuming. Depending on climate and sandbag material, sandbags may deteriorate rapidly. In some cases in Iraq, sandbags have been known to fail after only two months. The proximity of the fill sand area to the site will greatly affect the speed of construction and the final cost. Caution should be used when constructing walls over 4 ft high since they may become unstable.

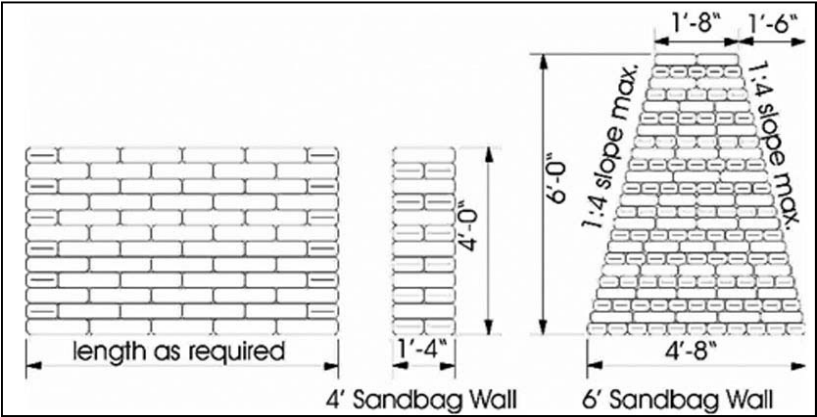


Figure 14-2. Freestanding sandbag revetment details

## Soil-Filled Wire and Fabric Containers

These wall sections consist of a series of large, linked, self supporting cells (See Figure 14-3). Each cell consists of collapsible wire mesh lined with a geotextile fabric. The cells are connected at the corners with spiral wire hinges that allow the wall sections to be expanded from a compact, folded storage configuration. The advantage of using this material is that during transport the cells are collapsed, and upon arrival at the final destination, expanded and filled. This allows the walls to be transported at only 5 percent of the as-constructed volume. The wall sections can be connected to form longer walls, separated to form shorter sections, or stacked to increase wall height.

*Performance.* Numerous tests have shown a 2 ft. thickness is adequate to stop all fragments from 60-mm mortar through 122-mm rocket and 155-mm artillery rounds.

*Construction Procedure.* Each shipment comes with detailed instructions. It is important to follow these instructions as closely as possible to ensure that the construction is stable, long-lasting and requires minimal maintenance. Choose or provide a level surface with a sub grade of sufficient strength and drainage to support the structure. Otherwise, the earth-filled barrier may tip over and will have to be rebuilt. Units come flat-packed. Be sure to place them in the desired location and orientation BEFORE expanding them in the desired direction. The ideal fill is a dry sand/gravel mixture. Place fill in 6 in. to 12 in. (150 mm to 300 mm) lifts and then compact.

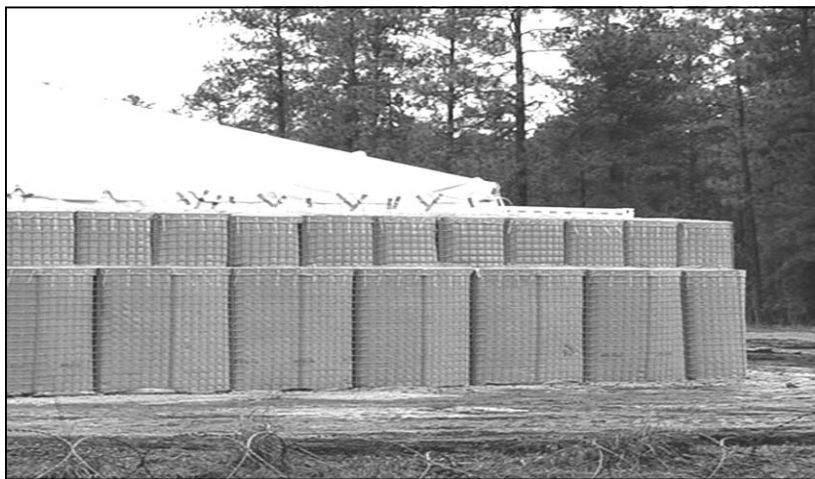


Figure 14-3. Soil-filled wire and fabric containers used for sidewall protection

*Limitations.* The wall requires a well-drained, flat, level, and stable site to prevent sagging and tipping. If anticipated use is longer than 6 months, use an improved foundation. The proper placement of the sand infill is critical to the performance of the structure. Make sure it is compacted or the wall will sag and collapse in a few months or have a deformed appearance. Like sandbags, the fabric material liner is UV sensitive and will degrade over time.

## **Soil-Filled Metal Containers**

These revetments can be utilized for supplemental sidewall protection or in the construction of protective positions (See Figure 14-4). Revetment kits are shipped flat in an unassembled state to be assembled on-site and filled to construct the desired protective structure. Each kit will consist of side, end, cross, and brace panels, connecting pins, flaring tools, and corner containment materials. Revetment systems are based on the USAF Metal Revetment Kit, Type B-1, which has been employed in some fashion since the Vietnam War era. The Engineer Research and Development Center (ERDC) developed a smaller version of this kit for use in FOBs. This kit will provide protection from blast loadings and shielding from primary fragments from RAMs (Refer to Appendix D for additional information on soil-filled container applications).

*Performance.* Numerous tests have shown the 2 ft. thickness is adequate to stop all fragments from near-miss 60 mm mortars through 122 mm rockets. By themselves, metal bin revetments will not defeat the effects of an anti-tank RPG. However, tests by ERDC have shown that these revetments can defeat an RPG-7 if used in conjunction with a vertical “pre-detonation screen” at sufficient standoff. Contact ERDC for information on the types of material and construction that can be used for a screen and the recommended standoff distances to prevent perforation.

*Construction Procedure.* See the *Metal Revetment Assembly Construction Guide* for detailed guidance on assembling individual metal bins. If protection is needed from near-miss of 122-mm rockets, laterally brace walls shorter than 24 ft. in length to prevent wall toppling. Lateral bracing can be provided by 3 in. diameter, schedule 40 (minimum) steel pipe (See Figure 14-5). Other materials possessing adequate strength, such as 4 x 4 timbers, can also be used. To prevent wall toppling in either direction, apply bracing on both sides of the wall.

*Limitations.* A well-prepared foundation is vital for the performance and durability of the revetment. It is essential that the ground surface be level, well compacted and exhibit sufficient strength and stability to support the structure for its intended lifespan. If construction will not take place on an

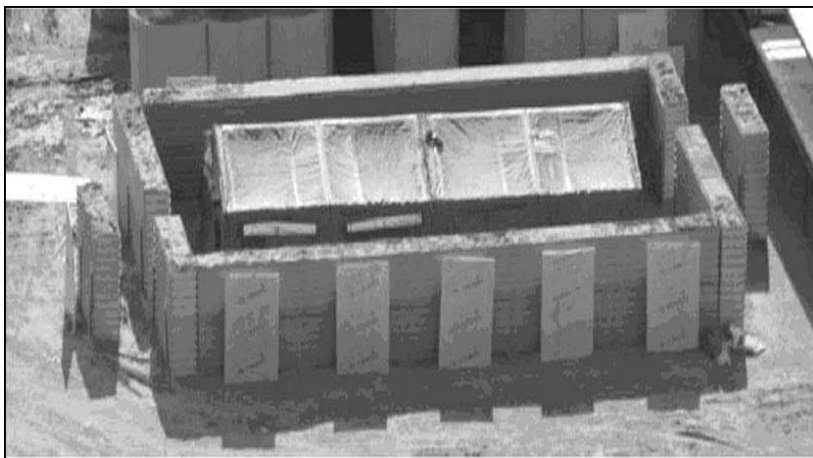


Figure 14-4. Soil-filled metal containers used for sidewall protection



Figure 14-5. Bracing metal revetment walls for near-miss 122-mm rocket threat. Bracing here is provided by steel pipe; 4 x 4 timbers can also be used.

improved surface (concrete paving, asphalt paving, stabilized soil, etc.), the foundation area must be properly prepared.

## Modular Reinforced Concrete Walls

Prefabricated, reinforced concrete barrier walls (See Figure 14-6) are readily available at some locations in Iraq and can be used for full-height sidewall protection around tents and trailers. These barrier sections are fabricated in a wide variety of sizes and configurations. The minimum recommended height for these walls is 6 ft. but taller units may be needed for trailers with crawl spaces. Prefabricated reinforced concrete barrier walls can also be used for physical anti-personnel barriers and obscuration along

the FOB perimeter. They can also be used as anti-vehicle barriers, or as part of the entry control point to channel traffic, mitigate blast/fragmentation, and protect personnel.

*Performance.* At 4500 PSI and 6 in. thickness, concrete walls will stop all fragments from 60-mm mortar through 122-mm rocket at standoff distances of 10-ft. or greater. Detonations within 10 ft. may pose a hazard for blast/fragmentation induced back-face spall. For additional protection a spall liner of sheet steel (for example, 16 gauge) can be used to reduce spall and increase fragment penetration resistance.

*Construction Procedure.* Provide level stable surface for placement. Ensure no gaps between wall sections. Construct sections so that they can be connected together with cables if possible. Consider bracing tall sections to prevent toppling. To prevent gaps at corners, use sections with chamfered footings (Figure 14-7).

*Limitations.* A level, stable foundation is required for prefabricated concrete walls. Fragments can penetrate gaps between wall sections. Close-in detonations of large mortars and rockets may breach the wall.

### E-Glass and U-Picket Walls

Another option that has been tested and shown to provide low-height fragment protection for tent sidewalls is the use of multiple (3 to 6) layers of ballistic-grade E-glass panels (NSN 9340-01-533-3758). The individual panels are 4 ft. x 8 ft. x 1/2 in. thick (nominal) and are positioned with the



Figure 14-6. Modular reinforced concrete barriers used for sidewall protection



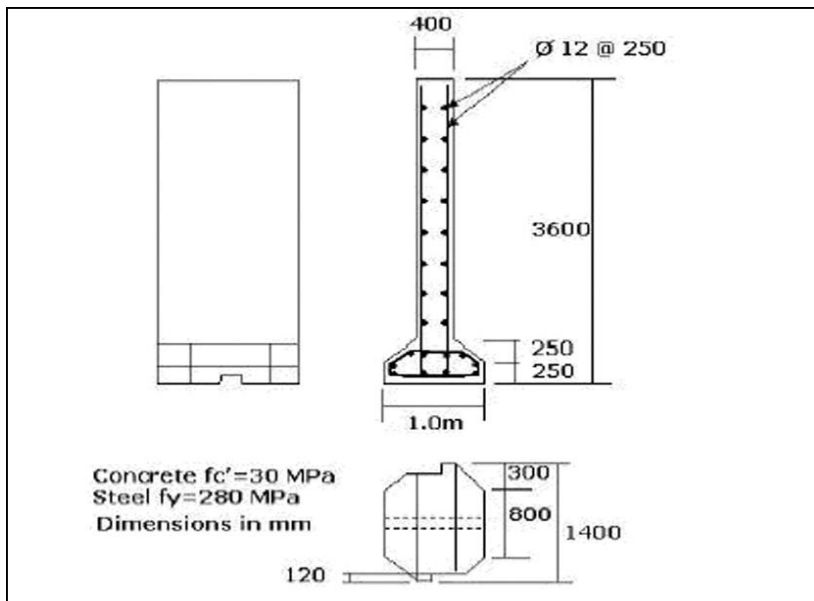


Figure 14-7. Overlapping concrete revetment with chamfered footings example

4 ft. dimension vertical (See Figure 14-8). This protection technique can be used inside or outside tents, but is limited in height. A similar compartmentalization concept is discussed in Chapter X.

**Performance.** In testing this concept with 120-mm mortars, 3-layers and 6-layers of E-glass stopped 97% and 100%, respectively, of the fragments from the mortar detonating 10 to 13 feet away. Some movement/rotation of the walls occurred due to the blast. Based on tests of other E-glass concepts with 122-mm rockets, 3-layers and 5-layers of E-glass will stop 95% and 99%, respectively, of the fragments from the rocket warhead detonating 10 feet away. However, the configuration using U-pickets for support was not tested and it is not known whether they will be sufficient to prevent walls overturning from the blast effects.

**Construction Procedure.** Walls are constructed with 4-ft-tall by 8-ft-long panels that are supported approximately every 3.5 feet by steel U-picket fence posts (NSN 5660-00-270-1587 or similar) driven a minimum of 12 inches into the ground. The fence posts are fastened to the E-glass by self-tapping screws or complete thru bolts with nuts on the back side.

**Limitations.** Only 4 vertical feet of fragment protection is provided.



Figure 14-8. E-glass and U-picket walls used for low height protection

### Modular Protective Systems

The modular protective system (MPS) consists of an expandable steel frame that accepts fragment-resistant E-glass or super high strength concrete panels (See Figure 14-9). The frame contains Z bar clips that allow the panels to be slid in. The E-glass and concrete panels are designed to stop fragments from mortars and provide protection from small arms fire. The MPS can be set up with as few as two people and requires a level site. The system is portable and can easily be set up and taken down. It can be configured to protect straight line areas or go around corners.

There are no equipment requirements, assuming a relatively level construction platform/foundation. Each 4 ft. x 4 ft. x 5 ft. unit, including armor panels (for significant threat), weighs approximately 680 lbs. All MPS units, including armor panels, can be collapsed and carried on a standard 463L pallet. An estimated 10 frames (25 ft. long x 8-ft. tall wall) and the associated components can be easily packaged on a 463L pallet. With a 4-person team, plan on 18 minute deployment and 10 minute recovery for each 10 ft. long x 8 ft. tall MPS section.

More information on the MPS is available from the Survivability Branch, Geotechnical and Structures Laboratory, USACE ERDC in Vicksburg Mississippi. See <http://gsl.erdcl.usace.army.mil> or contact the GSL Survivability Branch at 601-634-2711/2750, DSN 446-2711/446-2750.

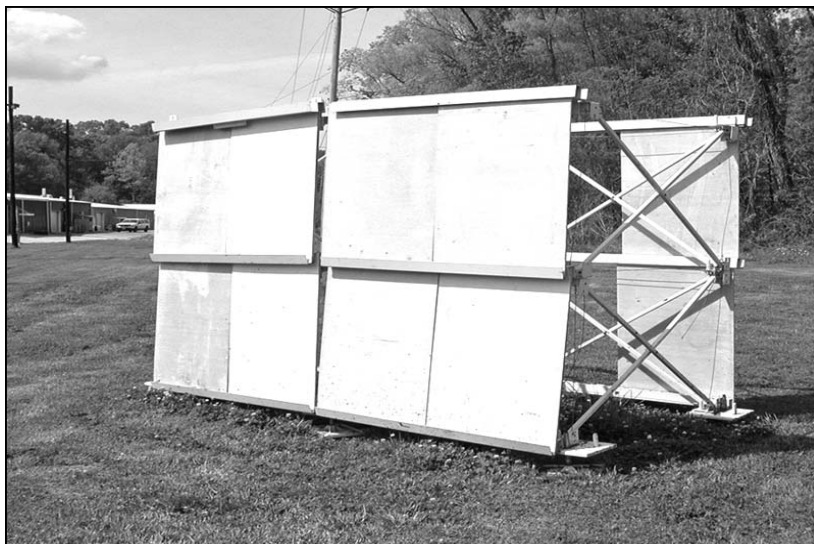


Figure 14-9. Modular Protective System

## Sniper Screens

The nature of sniping carries a significant and personal terror element. However, single acts of sniping seldom have a widespread psychological impact unless they eliminate key military, national, or religious leaders. Cumulative attacks, over time, may have an extensive psychological impact. This impact can affect individual behaviors; tactics, techniques and procedures; operational and strategic positions.

In an operational environment, the sniper can pose a significant threat. The *Joint Sniper Defeat Handbook* (GTA 90-01-013) is a collection of current Joint Service validated sniper defeat lessons learned, tactics, techniques and procedures. This field handbook provides recommended TTPs and material solution applications to leverage current counter sniper capabilities and minimize the impact of sniper threats to U.S. Forces. Counters include rehearsed responses, reconnaissance and surveillance, and cover and concealment. ROE should provide specific instructions on how to react to sniper fire, to include restrictions on weapons to be used. Units can use specific weapons, such as sniper rifles, to eliminate a sniper and reduce collateral damage.

Use T-walls and earthen barriers to cover building entrances and exits and where personnel might gather. T-walls and earthen barriers are usually an elevated measure of force protection, although in certain high value target

(HVT) areas they can serve dual purposes against indirect fire, IEDs, and snipers.

Apply netting to areas where personnel can be observed. Netting can be an expedient obscuration method for temporary targets (See Figure 14-10). When hard stand buildings are not available, tentage can be used as concealment for a variety of combat operations. (for example, maintenance, logistics, food service, and religious service activities).



Figure 14-10. Netting used for obscuration  
(from the *Joint Sniper Defeat Handbook*)

# Compartmentalization

### Introduction

Compartmentalization is a technique to reduce casualties in high population-density areas (such as dining facilities and recreation facilities) from the threat of fragmenting weapons detonating within the facility. The ultimate objective of compartmentalization is to divide a large area, occupied by high numbers of personnel into smaller compartments (See Figure 15-1). Constructing protective walls capable of providing ballistic protection creates the compartments, and thus a weapon's fragmentation effects are confined to an area smaller than one that would have been affected if the walls were not in place. Since, by definition, the primary threat of a fragmenting weapon is its capability to generate fragmented projectiles, the primary objective of compartmentalization is to contain these fragmentation effects.

For weapons of concern in most adversary environments (120-mm mortar and 122-mm rocket), the fragmentation effects will pose a far more significant threat to compartment occupants than blast. Tests and analysis have shown that the limits of significant blast hazard will not generally extend beyond the compartment in which the weapon detonates. In addition to compartmentalization, the facility also needs fragmentation barriers around the outside to mitigate blast and fragmentation from near misses. Minimum height for interior walls and exterior walls is 5 feet and 8 feet respectively. Several barriers that have been tested for use in construction of interior walls for compartmentalization are discussed here. Table 15-1 summarizes their selection consideration.

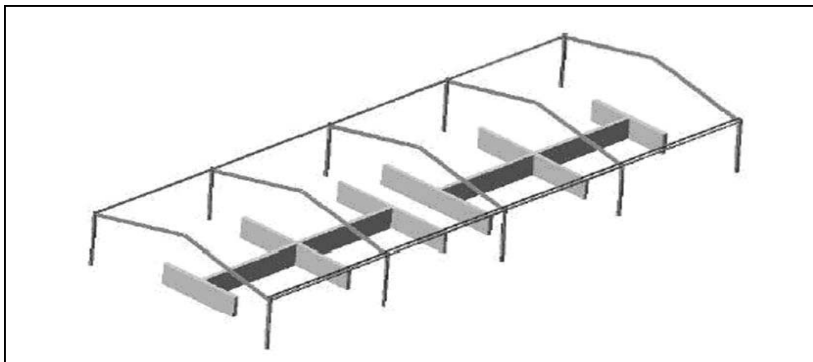


Figure 15-1. Compartmentalization concept

Table 15-1. Compartmentalization Selection Guidelines

Strategy	Space Needed	Standoff Protection	Construction Effort	Relative Cost	Aesthetics	Maintenance Effort	Limitations
Soil-Filled Container Wall	4 (24")	1	1	1	4	4	4
Soil-Filled Plastic Bin Wall	3 (10")	3 (10 ft)	3	3	1	2	3
Wooden Partition Wall	2 (8")	2 (7 ft)	4	2	3	3	2
E-Glass Wall	1 (< 1")	4 (10-13 ft)	2	4	2	1	1
The internal compartment mitigation strategies are prioritized by the highest probability to defeat the fragmentation effects of weapons ranging from a 60-mm mortar through 122-mm rocket. The characteristics are ranked 1-Most Preferred to 4-Least Preferred. The rankings are for the most part relative and not absolute.							

Soil-Filled Plastic Bin Wall

The primary construction element is a plastic wall unit approximately 7 ft. long, 5 ft. tall, and 10 in. wide. The wall unit is hollow and is filled with sand or other ballistic resistant materials to generate the necessary protection. Walls are keyed at each end to allow for interlocking construction. Threaded caps at the bottom provide a way to empty contents when necessary. Figure 15-2 shows an application and Figure 15-3 is a concept drawing of the plastic soil bin wall.

*Performance.* The plastic barrier material with 10 in. of soil fill will stop all fragments from 60-mm mortar through 122-mm rockets detonating 10 ft. from the soil bin.

*Construction Procedure.* Prior to construction of interior protective walls, ensure that the floor material (concrete slab, plywood, soil, etc.) has been evaluated to ensure that it can support the wall material. When filled with sand, the wall will weigh approximately 425 to 500 lb./ft. Two persons can easily carry empty plastic soil bins. Install intersecting walls at about every 21 ft. to provide stability. Place steel angle or other supports at the free ends of the walls to reduce wall motions. It is important to minimize dynamic motion of these walls since their moving mass creates a hazard



Figure 15-2. Plastic soil bin revetments used for compartmentalization

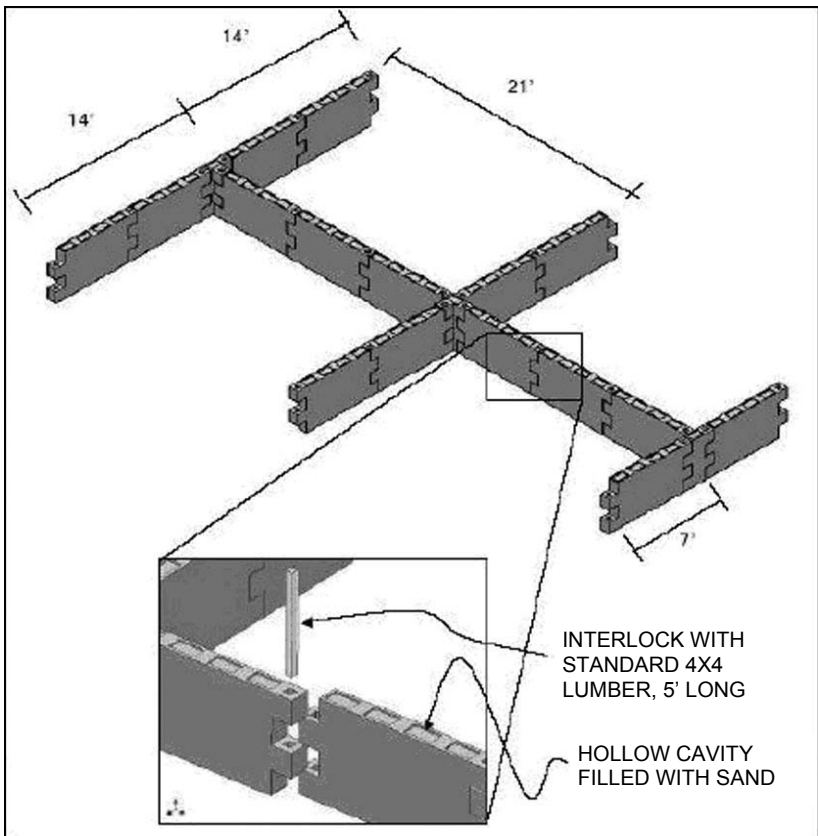


Figure 15-3. Concept drawing of a plastic soil bin wall

for personnel located in the adjacent compartment. Fill material can greatly affect the fragment-defeating capability of the wall. The most effective material is compacted dry sand. Tap all sides of the walls with hammers as they are being filled. This promotes compaction of the fill material and accelerates settling. It is important to begin this process as soon as the wall begins to be filled or else the lower fill material will not be properly compacted, thus reducing its ballistic resistance.

*Limitations.* The wall panel attachments are weak points for fragment penetrations. Test results show that fragments impacting the main body of the wall were stopped (where the sand fill was properly placed with no voids). However, some fragments impacting the 4 x 4 connections and void portions of the attachment joints were able to pass through.

### Wooden Partition Wall

The wooden partition wall (See Figure 15-4) is constructed of 3/4 in. plywood over 2 in. x 8 in. x 57 in.-long studs with 2 in. x 4 in. whaling along the outside. The 7-1/2 in. cavity formed is filled with soil and capped with 2 in. x 8 in. lumber. The fill material is the primary element for stopping weapon fragmentation. The walls are attached to the floor of the facility to provide stability and prevent overturning from the blast of weapon detonation.

*Performance.* The 7-1/2 in. soil-fill and plywood barrier material will stop all fragments (excluding those that may perforate wooden studs) from 60-mm mortar through 122-mm rockets at a 7 ft. standoff.

*Construction Procedure.* Prior to construction of interior protective walls, ensure that the floor material (concrete slab, plywood, soil, etc.) has been



Figure 15-4. Wooden Partition Wall (Inset: Corner Joint Detail)



evaluated to ensure that it can support the wall material. When filled with sand, the wall will weigh approximately 325 to 400 lb./ft. Install intersecting walls about every 20 ft. to provide stability. In addition, anchor the wall to the floor at its ends and midpoints. It is important to minimize dynamic motion of these walls since their moving mass creates a hazard for personnel located in the adjacent compartment. Fill material can greatly affect the fragment-defeating capability of the wall. The most effective material is compacted dry sand. Tap all sides of the walls with hammers as they are being filled. This promotes compaction of the fill material and accelerates settling. It is important to begin this process as soon as the wall begins to be filled or else the lower fill material will not be properly compacted, thus reducing its ballistic resistance.

*Limitations.* During testing, two fragments from a 120-mm mortar penetrated the 2 in. x 8 in. spacers separating the plywood panels. During the 122-mm rocket test several fragments passed through the wooden cap at the top of the wall, a result of the reduced ballistic performance of wood. A mini loader is needed to place soil in the small opening at the top of the wall.

## E-Glass Walls

These are multi-layered (3- to 6-layer) wall panels of ballistic grade E-glass (NSN 9340-01-533-3758) supported by custom manufactured steel stands (See Figure 15-5).

*Performance.* In tests with 120-mm mortars, 3-layers and 6-layers of E-glass stopped 97% and 100%, respectively, of the fragments from the mortar detonating 10-13 feet away. In tests with 122-mm rockets, 3-layer and 5-layer E-glass panels stopped 95% and 99%, respectively, of the fragments from the rocket warhead detonating 10 feet away.

*Construction Procedure.* Walls are constructed with 4 ft. wide by 5 ft. tall

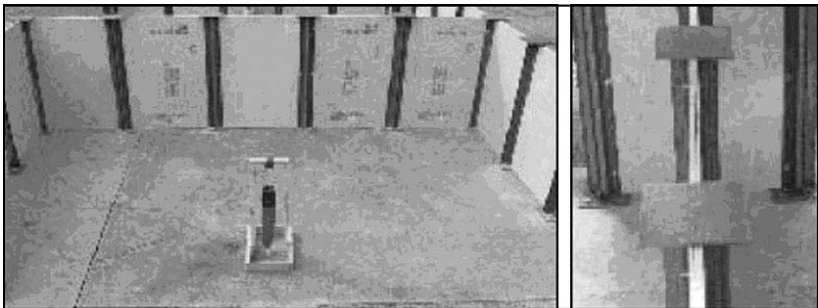


Figure 15-5. E-glass and steel stands used for compartmentalization

panels that are supported at each edge in steel stands. The steel stands are attached to the foundation with 3/4 in. diameter anchors.

*Limitations.* For larger weapons (such as the 122-mm rocket) it is difficult to provide sufficient support to prevent overturning of walls anchored in wooden floors.

### Soil-Filled Container Walls

Soil-filled containers can also be used for compartmentalization. Figure 15-6 shows a small dining facility compartmentalized with 2 ft. thick soil-filled containers. Metal containers of similar size can also be used for this application. Refer to Appendix D for construction details.

*Performance.* A 2 ft. thickness is adequate to stop all fragments from 60-mm mortar through 122-mm rocket.

*Construction Procedure.* Installation instructions are identical to the procedures outlined for sidewall earth-filled barriers. These walls do not need to be anchored to the floor for stability.

*Limitations.* Wire and fabric containers 2 ft. x 2 ft. x 4 ft. can be stacked 6 ft. tall. The recommended height for compartmentalization walls is 5 ft. Since these walls are much thicker and taller than wooden or plastic soil bin walls, the protected area behind the walls is about the same. These walls will require about three times the fill material and will occupy about four times the space of the wooden or plastic soil bin walls. In addition, they are not practical for raised floor systems because of their significant weight. Hygiene is also a consideration in a food service environment; a consequence of the presence of loose soil in the containers.



Figure 15-6. Soil-filled container walls used for compartmentalization

# Overhead Cover

### Introduction

Overhead cover for areas with large concentration of personnel can help protect personnel from indirect fire mortars. The basic concept (shown in Figure 16-1) is to provide a “pre-detonation” layer and “shielding” layer over the personnel being protected. The pre-detonation layer causes the fuse of the incoming mortar round to function and detonates the round before it can penetrate inside the facility (assuming a “super-quick” fuse setting). The shielding layer (located approximately 5 ft below the pre-detonation layer) mitigates the fragments resulting from round detonation. Overhead protection should always be used in conjunction with adequate sidewall protection to protect from near misses. Material options for both pre-detonation and shielding layers are given in Tables 16-1 and 16-2.

Based on guidance provided from operations in Iraq and others, the research used to develop this information was targeted at protecting “less than permanent” facilities. As a result, the focus is on light-weight, cost-effective solutions that provide significant mitigation of weapon effects but do not constitute fully hardened structures. Because of the lightweight nature of these protective structures, they will not have the capability to stop high-mass projectiles such as duded mortars, rocket motors which continue to travel after detonation, and delay-fused weapons. To provide a protective layer sufficient to stop these types of high-energy projectiles would easily constitute a fully hardened structure and thus falls beyond this scope. Therefore, the hazard posed to facility occupants from these types of high-mass-projectile threats will generally still remain.

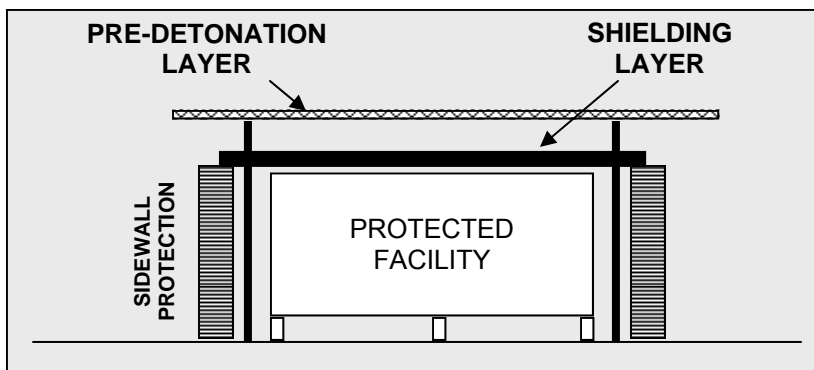


Figure 16-1. Overhead cover protection concept

Table 16-1. Material Options for Pre-Detonation Layers  
(From USACE ERDC)

Pre-Detonation Layer Material	60 mm Mortar	82 mm Mortar	120 mm Mortar
¾ in. Plywood		YES	YES
½ in. Plywood			YES
2 in. Foam Sandwich Panel	YES	YES	VARIABLE <sup>1</sup>
4 in. Foam Sandwich Panel		YES <sup>2</sup>	YES <sup>3</sup>
22 ga. Corrugated Metal Deck, Type 1.5B		YES	NO
¼ in. Steel Plate		YES	YES <sup>4</sup>
1 Layer of Ballistic E-Glass (NSN 9340-01-533-3758)		YES	
Expanded Metal Mesh			NO
Nylon Net			NO
Welded Wire Mesh (1/2 in. aperture)		NO	
Double Layer Chain Link Fence			NO
Solar Shade, Type I (NSN 5410-01-519-7041)			NO
Tent Fabric (MGPTS)			NO
Tent Fabric (16'x16', Frame Type Expandable, NSN 8340-00-782-3232)		NO	NO
<p>Results of Live-Fire Tests of mortar rounds ("YES" indicates round detonated, "NO" indicates the round did not detonate, a blank indicates no test was conducted).</p> <ol style="list-style-type: none"> <li>1. August 2005 live-fire experimentation has shown that 2 in. thick foam sandwich panel will not consistently initiate the 120 mm mortar. Under experimentation, 3 of 10 quick-fused 120 mm mortars were successfully initiated.</li> <li>2. The 82 mm mortar has not been live-fire validated against the 4 in. foam sandwich panel, but based on results of the 2 in. panel it is highly expected that the 4 in. thick material will produce the same results.</li> <li>3. Based on results of August 2005 live-fire experimentation. Under experimentation, 1 of 1 quick-fused 120 mm mortars was successfully initiated.</li> <li>4. Potentially hazardous secondary debris may be generated when the 120 mm mortar pre-detonates on steel plate.</li> </ol>			

Table 16-2. Material Options for Shielding Layers

Shielding Layer Material	60 mm Mortar	82 mm Mortar	120 mm Mortar
3 ½ in. Sand	YES	YES	YES <sup>1</sup>
¼ in. Steel Plate	YES	YES	NO
5/8 in. Steel Plate	YES	YES	YES
2 Layers of Ballistic E-Glass (NSN 9340-01-533-3758)	YES	YES	NO
3 Layers of Ballistic E-Glass <sup>2</sup> (NSN 9340-01-533-3758)	YES	YES	YES
<p>Results of live-fire tests of mortar rounds ("YES" indicates fragments were stopped, "NO" indicates fragments penetrated). It is Important that pre-detonation be included to achieve these results.</p> <ol style="list-style-type: none"> <li>Experiments have shown that 3 ½ in. sand will stop approximately 90 percent of the fragments and 7 in. will stop near 100 percent of the fragments.</li> <li>Assumes 5' or greater space between Pre-det and shielding layers. For spacing between 3.5' and 5', use 4 Layers. For spacing between 2.5' and 3.5', use 5 layers.</li> </ol>			

### Internal Protection

As shown in Figures 16-2 through 16-4, the internal protection approach is generally utilized for large metal buildings that are used for dining facilities, exchanges, etc. They are characterized by insulated foam panel walls and roofs and are typically surrounded by concrete barriers at some relatively large distance away. The approach to overhead protection here is to construct a steel frame within the facility and place ballistic grade E-glass on top of the new frame to shield occupants from fragments. This construction technique is due to the size of the metal building. The size of a structure needed to go over the top would be prohibitive in terms of cost and effort.

The results of numerous experiments indicate the existing roof material (foam panel) may act as a pre-detonation layer for the threat weapons. However, note that foam panel with different thickness will generate different degrees of reliability for 82-mm mortars and 120-mm mortars (See Table 16-1). If the existing roof material does not provide the recommended pre-detonation reliability, then augment or replace it with appropriate material.

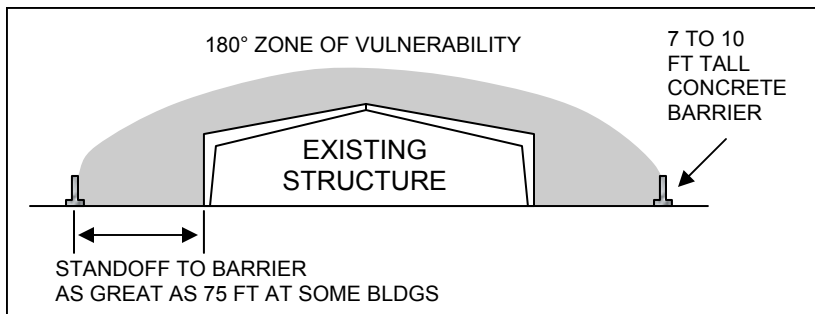


Figure 16-2. Internal protection example of existing conditions showing no overhead cover. The zone of vulnerability (gray-shaded arc) extends 180 degrees around the structure.

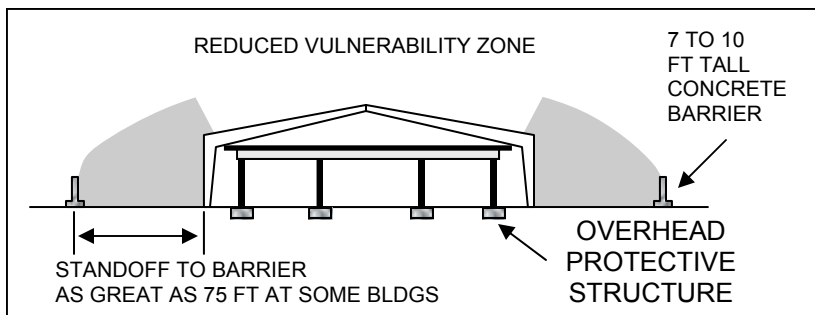


Figure 16-3. Internal protection example of overhead cover installed providing protection without tight sidewall protection. Note the zone of vulnerability (gray shaded arcs) is reduced directly above the structure, but still extends to either side of the structure.

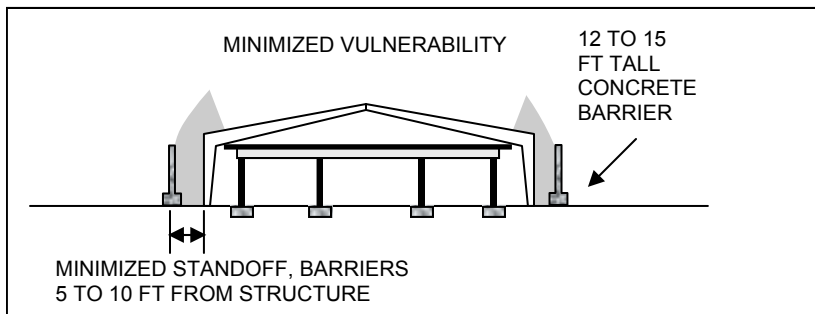


Figure 16-4. Internal protection example of overhead cover installed providing protection with tight sidewall protection. Note the greatly reduced zone of vulnerability (gray shaded arcs) around the structure.

*This cover does not fully provide protection from the overhead threat. As shown in Figure 16-3, with exterior barriers placed as much as 75 ft. away from the facility, there still exists a very large area where mortars and rockets can detonate. Therefore, it is recommended that in addition to the overhead cover construction, place barrier walls of sufficient height tightly against the side of the buildings. By doing so, as shown in Figure 16-4, this significantly diminishes the area over which the facility is vulnerable to attack.*

## **External Protection**

As shown in Figures 16-5 through 16-7, the external protection approach is utilized for structures such as tents, modular trailer complexes, or small metal buildings. Because of their smaller size, it is feasible to construct a steel frame around the existing facility for use in supporting a pre-detonation layer and a fragment-shielding layer.

As the figures show, overall protection from the overhead threat is not solely based on the construction of an overhead structure but is also largely dependent upon the proper placement of sidewall protection. *Do not assume that existing barriers placed at a distance from the structures should be relocated.* The reason for this is that the existing barriers may likely be serving to provide protection from other threats (such as VBIEDs ) and, if moved, would simply expose the building to a different threat. Therefore, consider all viable threats posed to each facility and determine whether existing barriers can be relocated, or whether new barriers must be acquired. When considering barrier locations, consider entry/exit and maintain viable accessibility for normal use and in the case of an emergency.

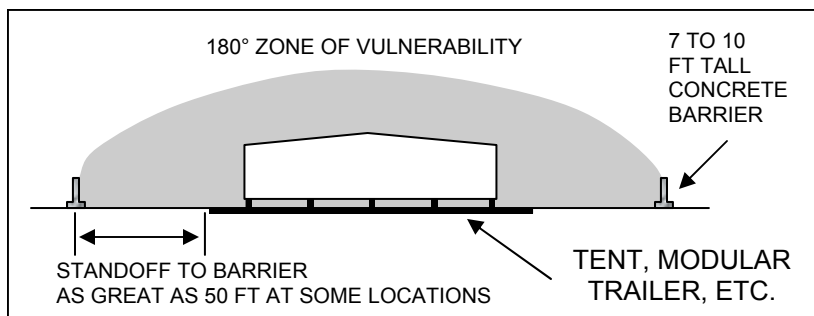


Figure 16-5. External protection example of existing conditions showing no overhead cover. The zone of vulnerability (gray-shaded arc) extends 180 degrees around the structure.

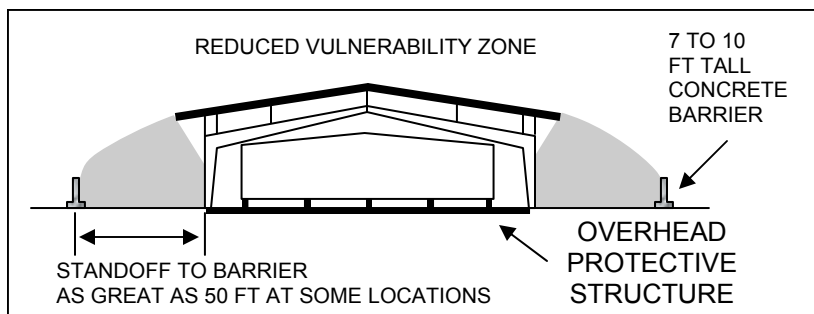


Figure 16-6. External protection example of overhead cover installed providing protection without tight sidewall protection. Note the zone of vulnerability (gray shaded arcs) is reduced directly above the structure, but still extends to either side of the structure.

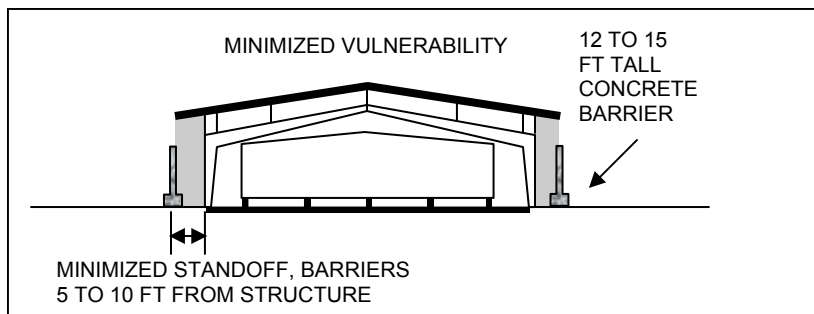


Figure 16-7. External protection example of overhead cover installed providing protection with tight sidewall protection. Note the greatly reduced zone of vulnerability (gray shaded arcs) around the facility.



## SEAhut Overhead Cover Retrofit

Figure 16-8 shows an example of applying the overhead cover concepts to retrofit the standard theater construction management system (TCMS) 16 ft. x 32 ft. South East Asia hut (SEAhut). The retrofit consists of adding three layers of ballistic-grade E-glass as a shielding layer. The E-glass is supported by steel beams beneath the roof joists. The steel beams rest upon full height sidewall protection constructed from 4 ft. thick metal revetments. The existing 1/2 in. plywood roof is utilized as a sacrificial pre-detonation layer.

*Performance.* This retrofit provides very near 100 percent protection from near-miss rockets and mortars and good protection from direct hit mortars.

*Construction Procedure.* Construct 10 ft. tall, 4 ft. thick load-bearing revetment walls around the SEAhut. Insert steel (W6x9) beams through the SEAhut sidewalls every 4 ft. and rest them upon the revetments. Three layers of E-glass are then fastened to the steel beams every 12 in. with self tapping screws before the roof joists are installed. Finally the remaining roofing material for the SEAhut can be installed as usual.

*Limitations.* In tests using 120-mm mortars, only one fragment penetrated the 3-layer E-glass shielding layer. As a result of inadequate fasteners, one E-glass panel fell from the supporting beams. If a greater number of screws had been used to fasten the e-glass to the beams, possibly little to no damage would have occurred inside the structure (this has not been confirmed experimentally). For larger weapons such as the 122-mm rocket, a much more robust support system must be used (This retrofit has not been tested against the 122-mm threat).

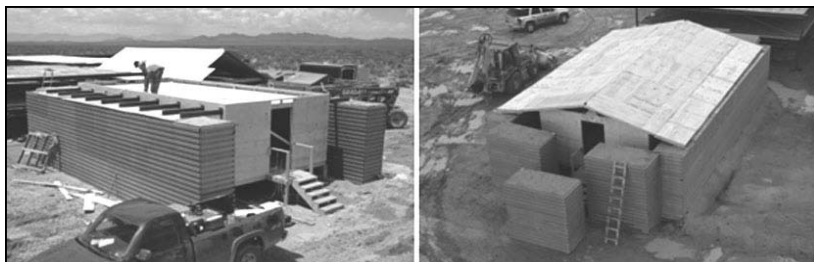


Figure 16-8. SEAhut retrofit (Left, placing the shielding layer; Right: Retrofit for overhead protection)

This page intentionally blank

# Lighting

### Introduction

Protective lighting enables security force personnel to observe activities around or inside the FOB without disclosing their presence. Adequate lighting at all approaches to a FOB not only discourages unauthorized entry attempts but also reveals persons within the area. Lighting should not be used alone. It should supplement other measures such as fixed security posts or patrols, fences, and alarms. Lighting aids threat detection, assessment, and interdiction. Lighting may also have value as a deterrent. Lighting increases the effectiveness of guards and closed-circuit television (CCTV) by increasing the visual range during periods of darkness or by illuminating an area where natural light is insufficient.

Light discipline will determine the type of lighting utilized for perimeter security and at entry control points (ECPs). With the enforcement of strict light discipline, the type of lighting used may be limited. Exterior security lighting is typically located along exterior perimeters and entry points of the site and buildings. Each facility presents its particular deployment problems based on physical layout, terrain, weather conditions, and security requirements.

### Concepts

Security forces may need to see for long distances at differing low-level contrasts, identify indistinct outlines of silhouettes, and must be able to spot an intruder who may be exposed to view for only a few seconds. Higher levels of brightness improve all of these abilities. When planning security lighting, security forces should consider the following concepts:

- Security lighting is most effective when it adequately provides glaring light in the eyes of the intruder but does not illuminate security forces
- High-brightness contrast between intruder and background should be the first consideration
- The volume and intensity of lighting should vary according to the surfaces to be illuminated
- Dark, dirty surfaces, or surfaces painted with camouflage paint require more illumination than surfaces with clean concrete, light brick, or glass
- Rough, uneven terrain with dense underbrush requires more illumina-

tion to achieve a constant level of brightness than do desert landscapes

- In cases where light discipline is strictly enforced, an alternative to bright illumination is the use of night vision devices and infrared detection systems

## Configurations

**Continuous Lighting.** Continuous lighting (the stationary lamp) is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during the hours of darkness with overlapping cones of light. The two primary methods of using continuous lighting are glare projection and controlled lighting.

**Glare Lighting.** Glare lighting uses lights slightly inside a security perimeter and directed outward. It is considered a deterrent to a potential intruder because it makes it difficult for him to see inside the area being protected. It also protects guards by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter.

**Controlled Lighting.** Controlled lighting is used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railroads, navigable waters, or airports. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence and a narrow strip outside, or floodlighting a wall or roof. Unfortunately, this method of lighting often illuminates or silhouettes security personnel as they patrol their routes. Controlled lighting may provide either direct or indirect illumination.

**Direct Illumination** involves directing light down to the ground. Its goal is to provide a specified intensity of illumination on intruders, facilitating their detection by CCTV or security patrols.

**Indirect Illumination** involves backlighting the intruders against a facility. This may be done by placing lighting away from a structure and directing it back toward the walls so the threat will cast shadows. Such applications are most effective if the lights themselves are near ground level. This indirect concept is also aesthetically pleasing, illuminating the architecture during darkness.

**Standby Lighting.** A standby lighting system differs from continuous lighting since its intent is to create an impression of activity. The lights

are not continuously lighted but are either automatically or manually turned on intermittently or responsively when activity is detected or suspected by the security force or intrusion detection systems (IDS). Lamps with short restrike times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

**Intermittent Lighting.** A lighting system can be developed to turn lights on at random times as a deterrent to some threats. It can use either direct or indirect illumination concepts. While an intermittent lighting system can involve a duty cycle of 10 to 50 percent, it may increase operational and maintenance costs, it may force the use of inefficient lamps, or reduce lamp life. Deterrence can actually be higher for such a system because of its appearance of activity. Lights may be controlled individually or as a group.

**On-Demand Lighting.** Rather than randomly activating the lights, an IDS sensor can be used to turn on the lights when an intruder is detected. This type of active lighting system provides maximum deterrent value at a low duty cycle. Such a responsive area system is subject to the same nuisance and false alarms of any sensor system.

## Specifications

Minimum lighting criteria is shown in Table 17-1. This table provides general guidance for footcandles as a function of location type and for the amount of area that should be illuminated. Lighting levels range from 0.2 footcandles (fc) [2.1 lux] near boundaries and perimeter fencing, increasing to 2 fc (21 lux) at entry areas. A lighting specification for visual guard surveillance to specific locations is also shown.

Lighting requirements for CCTV are considerably higher than those needed for direct visual surveillance. The entire assessment zone must have an average initial horizontal illumination level of 2 fc (21.5 lux) at 6 inches (150 mm) above the ground. The uniformity of illumination in the assessment zone must meet the following requirements:

1. the overall ratio of brightest to darkest regions of the assessment zone must not exceed eight to one, and
2. the overall ratio of the average brightest to darkest regions of the assessment zone must not exceed three to one.

Several methods are presently used in achieving these illumination levels. These employ high pressure sodium vapor roadway lights spaced to meet

both the CCTV and other security illumination requirements. The most common variety of lights is the 250-watt (W) unit, while some facilities employ a 400-W unit. Some installations have opted for 150-W lights with an instant restrike capability.

### Energy Considerations

Virtually every lighting system has come under scrutiny to identify energy savings. Protective lighting systems are no exception. This scrutiny is probably as much related to the conspicuousness of security lighting as to the amount of energy consumed. While the only energy consumption statistics available on lighting pertain to the energy needed to maintain street lighting systems, protective lighting uses considerably less energy. Recently, the direction of the security community to reduce energy costs in security lighting has resulted in replacing lights to increase source efficacy by changing to high-pressure sodium (HPS) lamps. HPS lamps produce more lumens per watt than either mercury vapor or incandescent lamps. Table 17-2 presents the relative efficiencies and restrike times of some typical lamps.

**Restrike Time.** The differences in restrike time among the various lamps (see Table 17-2) influence the selection of security lighting systems and concepts. For example, high-pressure sodium lamps are the primary light source of most security systems because of their efficiency (140 lumens/W). However, these lamps are not without deficiencies. From a cold start, a high-pressure sodium lamp warms up to full light output in about 10 minutes. It will usually restrike in less than 1 minute and warm-up in 3 to 4 minutes.

During this warm-up interval, the lamp cannot be expected to operate at full light output, and this reduced capacity may be important in many high-security applications. Because of this restrike interval, incandescent lamps are sometimes used as the emergency backup light source because of their short restrike time. The evaluation of any security lighting system, particularly one requiring continuous illumination, requires careful analysis of lamp life, energy consumption, and restrike time. The security engineer who has determined that short restrike time is a critical performance parameter should determine whether it is economically feasible in relation to increased lamp replacement and energy costs.

Table 17-1. Minimum Lighting Criteria for Unaided Guard  
Visual Assessment (From MIL-HDBK-1013/1A)

Application			Illuminated Width, feet (m)		Minimum Illumination				
Type	Lighting	Area	Inside	Outside	Footcandles (lux) (a)	Location			
Boundary	Glare	Isolated	25 (7.6)	150 (46)	0.2 (2.1) (b)	Outer Lighted Edge			
	Controlled	Semi-isolated	10 (3.0)	70 (21)	0.4 (4.3)	At Fence			
					0.2 (2.1)	Outer Lighted Edge			
					0.4 (4.3)	At Fence			
					0.4 (4.3)	Outer Lighted Edge			
Inner Area	Controlled	Non-isolated	20-30 (6.1-9.1)	30-40 (9.1-12.2)	0.5 (5.4)	Within			
					0.2 - 0.5 (c)	Entire Area			
					Area	All	--	0.2-0.5 (c)	Entire Area
						50 (15)	--	(2.1—5.4) 1 (11)	Out from Structure
	Entry Point	Controlled	Pedestrian	25 (7.6)	25 (7.6)	2 (21)	Entry		
Vehicle			50 (15)	50 (15)	1 (11)	Pavement and Sidewalk			
(a) Horizontal plane at ground level unless otherwise noted.									
(b) Vertical plane, 3 feet (0.9m) above grade.									
(c) Use higher value for more sensitive areas.									

Table 17-2. Relative Efficiencies and Restrike Times of Light Sources (From MIL-HDBK-1013/1A)

Lamp Type	Efficiency (Lumens/watt)	Restrike Time (minutes)
Theoretical Maximum	683	—
Ideal White Light	220	—
Incandescent	10-16	<1
Tungsten-Halogen	17-25	<1
Mercury Vapor	30-65	3-7
Fluorescent	33-77	<1
Metal Halide	75-125	Up to 15
High-Pressure Sodium	60-140	1 (restrike); 3-4 (warm-up to full output)
Low-Pressure Sodium	180	7-15

Security Lighting Considerations

	Provide adequate illumination or compensating measures to discourage or detect attempts to enter the FOB or restricted areas and to reveal the presence of unauthorized persons within such areas.
	Avoid glare that handicaps security force personnel or is objectionable to air, rail, highway or navigable water traffic.
	Direct illumination toward likely avenues of approach and provide relative darkness for patrol roads, paths and posts. To minimize exposure of security force personnel, lighting at entry points should be directed at the gate and the guard should be in the shadows. This type of lighting technique is often called glare projection.
	Illuminate shadowed areas caused by structures within or adjacent to restricted areas.
	Provide overlapping light distribution. Equipment selection should be designed to resist the effects of environmental conditions, and all components of the system should be located to provide maximum protection against intentional damage.
	Avoid drawing unwanted attention to restricted areas.
	Be expandable so that future requirements of electronic security systems and recognition factors can be installed. Where color recognition will be a factor, full-spectrum (high pressure sodium vapor, etc.) lighting vice single color should be used.
	Use lights that illuminate the ground or water but not the air above. These lights must penetrate fog and rain.



# Sensor Systems

**NOTE:** The Joint Base Expeditionary Targeting and Surveillance Systems-Combined (JBETSS-C) Quick Reaction Test is investigating sensor system integration for expeditionary-type bases. The results of this test program will affect future sensor system deployment and implementation. Contact the Joint Test and Evaluation Program Office (jpo@jte.osd.mil) for more details on the JBETSS-C Test Program.

### Introduction

When data is collected from a sensor and processed into an intelligible form, it becomes information and gains greater utility. Information on its own is a fact or a series of facts that may be of utility to the commander, but when related to other information already known about the operational environment and considered in the light of past experience regarding an adversary, it gives rise to a new set of facts, which may be termed “intelligence.”

Figure 18-1 shows a conceptual layout for an intrusion detection sensor system. A sensor is simply a device that receives and responds to a signal or other stimulus. Sensors and defensive positions are employed on the base boundaries to provide indications and warning or detect and defeat an adversary. A primary use of a sensor is to compensate for capability loss during periods of limited visibility. While sensors are NOT by themselves a layer of defense, they can greatly improve the effectiveness of security forces.

### Intrusion Detection and Surveillance Systems

The function of a perimeter intrusion detection system (IDS) is to detect a threat and initiate a response by security personnel. IDS should be an essential part of an integrated and layered approach to force protection.

IDS are used to accomplish the following:

- Permit more economical and efficient use of security personnel
- Provide additional controls at critical areas or points
- Enhance the security force capability to detect and defeat intruders
- Provide the earliest practical warning to security forces of any attempted penetration of protected areas

- Provide expedient perimeter security at austere sites through use of battery-operated, wireless communication IDSs prior to and during construction of permanent security measures (berms, fences, etc.)

### IDS Selection Considerations

The requirement for an IDS must be identified and determined during the JCOB site selection and layout planning process. The IDS cannot be completely identified until the proposed JCOB layout plan has been developed. To ensure an effective system is selected, the performance parameters should include:

- Completeness of coverage
- False and nuisance alarm rates
- Probability of detection
- Zone at which the alarm occurred
- Delay time

The U.S. Army Engineer Research and Development Center/Cold Regions Research and Engineering Laboratory (CRREL) has, as part of the base camp sensors program, developed a Weather Vulnerability Assessment Tool (WVAT), Security Technology Decision Tree Tool (STDTT) and

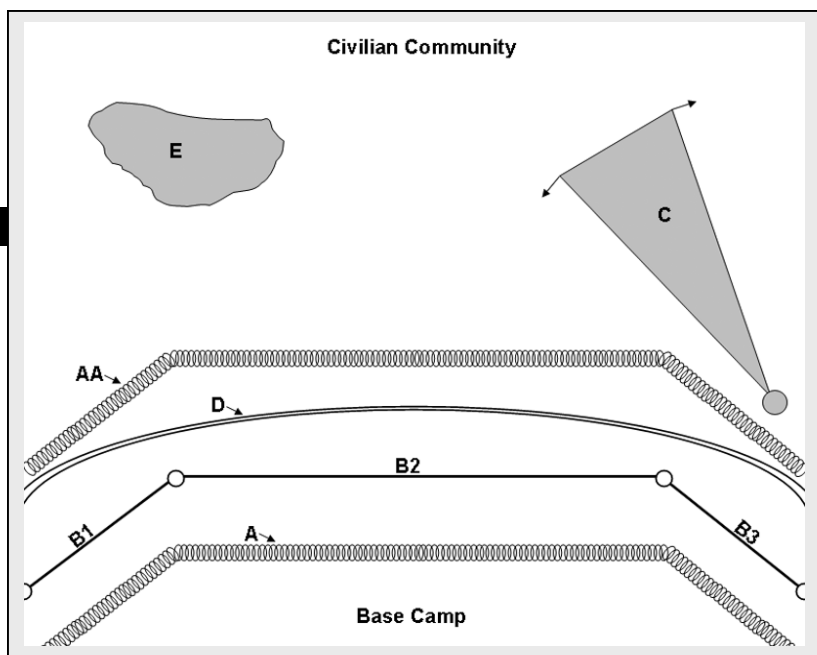


Figure 18-1 Diagram of Intrusion Detection System Concept

**Object AA** represents a chain link fence at the perimeter of a base camp or surrounding an asset within the base camp perimeter. If the fence is of suitable quality, an intrusion detection system (IDS) could be mounted to it. **Object A** shows a second chain-link fence that, with object AA, defines a clear zone. Fence-mounted IDS typically would only be on the inner fence. An advantage to this plan is it avoids alarms caused by non-threatening people or animals interacting with the outer fence.

**Other types of sensors (objects B, D)** can be located within the clear zone to detect intruders as soon as they pass the outer fence. Requiring a combination of sensors in the clear zone and a sensor on the inner fence establishes redundancy in the system and is a means of eliminating many weather related nuisance alarms.

**Taut wire** is an alternative to the combination of chain link fence plus fence-mounted IDS. Object AA in the figure could be replaced with a taut-wire system. Options include:

- Full height taut-wire system (ground to 8 ft. high, or higher)
- Taut-wire array on top of an existing barrier, such as a berm, to add a detection capability to the barrier
- Short taut-wire array on top of a chain link fence, to extend barrier height and detection

**Long-range surveillance camera** and/or long-range radar detection system are/is depicted as **object C**. These systems are appropriate when the extent of open area in front of the base camp perimeter allows their range to be fully exploited. Vegetation, aboveground structures, or gullies/depressions that could conceal an intruder defeat the purpose of such systems, rendering them not cost effective.

**Terrain-following sensors are shown as object D** in the figure. These sensors are normally buried systems that can accommodate moderate changes in topography (ground need not be level) as well as orientation (can follow around fence corner). Sensing technologies include fiber optic cable and ported coaxial cable. Once installed, buried line sensors are unobtrusive.

**Above ground sensors are shown as object B.** These sensors include passive infrared, microwave radar and near-infrared beam-break IDSs. They are line-of-sight sensors requiring level ground (or at least constant slope ground); their detection zones cannot extend around corners. The three zones labeled B in the figure are meant to indicate that the same extent of coverage attained with one zone of buried IDS D requires at least three zones of a line-of-sight sensor due to topography and the change in perimeter orientation.

**Unattended ground sensors (UGS)** are self-sufficient (battery operated, wireless alarm communication), unobtrusive sensors that can provide advance awareness of activity outside the perimeter at a small fraction of the cost of a scanning radar/imager. In the figure, **object E** is instrumented with UGS. Seismic UGS cannot function well in the vicinity of legitimate sources of ground motion (cultural activity, base camp activity). More use should be made of passive infrared UGS, magnetic UGS, and near-infrared beam break UGS.

Figure 18-1 Diagram of Intrusion Detection System Concept (continued)

Force Protection Sensor Selector (FPSS)—3rd CRREL computer application to assist in the selection of IDS and surveillance systems. The Sensor Selection Tool is shown in Table 18-1.

Sensor rankings are based primarily on probability of detection (Pd) of intruders and secondarily on likelihood of nuisance alarms (NA) caused by weather or terrain factors. In planning sensor use at a FOB, FPSS should be run to assess expected Pd and NA occurrence and to generate site specific sensor guidance.

**Types of IDS.** Several types of sensors (microwave, passive/active infrared, seismic, magnetic) are in common use. Types of IDS sensors include the following:

**Passive Infrared.** Passive infrared (also known as thermal infrared) alarms are generated by a change of thermal radiance within the detection zone.

**Microwave Radar.** These sensors generate an alarm when the receiver detects a change in the microwave field. There are two types of microwave radar sensors: bistatic systems have separate transmitter and receiver units; monostatic systems combine transmit and receive functions in one unit.

**Near-Infrared Beam Break.** Near-infrared beam break sensors are active systems that alarm when a near-infrared beam (between transmitter and receiver units) is interrupted for a certain duration. The beams are not visible to the eye, but may be seen with night vision devices. Multiple beams are arranged vertically to provide line-of-sight detection to the height desired. Their vertical spacing defines the detection pattern; detection width is narrow ( $< 1$  m), marking this IDS suitable for use in close proximity to legitimate activity. The distance of the detection zone can vary from 300 to 1200 feet. Beam break sensors located near the ground, in order to detect a crawling intruder, can be vulnerable to nuisance alarms caused by blowing drifts of sand or vegetation growing into the beam.

**Fence-Mounted.** This is a broad category of sensors that are designed to alarm when the security fence to which they are attached is being cut or climbed.

**Taut Wire.** Taut wire sensors alarm at the displacement of a strand of wire under tension. This IDS is installed as a physical barrier consisting of a vertical arrangement of wires (parallel to the ground) with

additional wires on angled outriggers.

**Ground Motion.** Buried ground motion sensors consist primarily of fiber optic cable. The cable sensor detects ground motion optically by changes in the pattern of standing waves of light in optical fiber cables buried at a shallow ( $\sim 5$  to 9 cm) depth.

**Ported Coaxial Cable.** Buried electromagnetic sensors are commonly referred to as ported coaxial cable systems. This type of IDS is activated by a disturbance in the electromagnetic field between two active cables, one a transmitter and the other a receiver of electromagnetic energy.

**Seismic.** Seismic sensors detect ground motion. Their detection range is greater for a moving vehicle than for a moving person. Seismic sensors are best used in remote areas where human or vehicle-generated ground motion is the exception. Seismic sensors have also been used in tunnel detection.

**Acoustic.** Acoustic sensors detect vehicles on the basis of the noise generated by the vehicle. They are not used to detect personnel. An acoustic sensor (microphone) typically is used in conjunction with a ground motion sensor (geophone).

**Magnetic.** Magnetic sensors detect movement of ferrous metal, with detection range depending on the amount of metal: tens of meters for vehicles, a few meters for personnel. Provided their detection ranges coincide, a magnetic sensor can be used to discriminate the source of alarms by another type of IDS. Alarms by both IDSs indicate passage of a vehicle or metal-bearing person through the detection zones; alarms by only the nonmagnetic IDS indicate passage of wildlife or personnel with no/few metal objects.

**Break Wire.** A break-wire sensor must be in contact with the intruder for an alarm to be generated. The intruder (person or vehicle) physically breaks the tripwire, resulting in an alarm.

**Electrostatic Field/Capacitance.** These sensors consist of a vertical arrangement of horizontal wires that are free-standing or mounted to a chain link fence. The wires detect an intruder by sensing the disturbance of the electrostatic field between the wires and the ground. The intruder does not have to contact the wires.

**Closed Circuit Television (CCTV).** Though not as effective as direct observation, CCTV is often used to augment security forces when

Table 18-1. Sensor Selection Tool

Conditions								
Sensor Type	Taut Wire Sensor	1	1	1	1	1	1	1
	Fence-Mounted Sensor	3	1	1	1	2	1	1
	Acoustic Sensor	1	1	1	1	1	1	1
	Near-Infrared Sensor	2	2	2	2	1	2	2
	RADAR	4	3	1	1	1	1	1
	Thermal Imaging / Passive Infrared	5	4	1	1	1	2	3
	Heavy Rain							
	Moderate Rain							
	Light Rain							
	Heavy Snowfall							
	Moderate Snow-							
	Light Snowfall							
	Strong Wind							
	Moderate Wind							

Sensor Type		6	6	1	4	4	1	1	1	1	1	1	1	1	1
Ported Coaxial Cable		6													1
Ground Motion		1	1	1	4	4	1	2	2	2	2	1	1	1	1
Seismic		1	1	1	4	1	1	2	2	2	1	1	1	1	1
Video Motion Detection		5	4	3	6	5	4	2	2	2	3	3	3	3	3
CCTV Cameras		5	4	3	6	5	4	2	2	2	3	3	3	3	3
LIDAR		4	3	1	5	4	1	1	1	1	1	1	1	1	1

The sensor types are prioritized by the highest probability to detect an intrusion for the given atmospheric/weather condition. They are ranked 1-6 with 1-Best to 6-Worst. An example would be if a certain area received moderate snowfall throughout the majority of the year, the Acoustic and Seismic sensors would have the highest probability to detect an intrusion and the fewest false alarms. On the other hand, Thermal Imaging, Video Motion Detection and CCTV's would have the lowest probability of detection and the most false alarms. A combination of sensors should be used as redundant systems to help analyze the specific intrusion situation.

manpower is limited. A CCTV is most effective when it is linked to motion detectors and has a dedicated operator monitoring the system. CCTV cameras should have pan, tilt, and zoom capability to allow the operator to track suspicious activities. When encased in mirrored globes, cameras can be moved to track personnel without their knowledge. Mirrored globes alone can be used to hide false cameras that give the perception that an area is being observed by CCTV.

**Automated Video Surveillance Systems (AVS).** AVS software detects intruders on the basis of their actions and their image and discriminates against other changes in the camera scene by the characteristic features of those changes. Several types of cameras can be used as part of AVS:

- Black/White Camera
- Color Camera
- Day/Night Camera
- Thermal Camera

**Information on Sources of Technology.** New technology solutions are regularly being tested, researched, and produced that have IDS application. The following organizations may be contacted for information on new and fielded technologies:

- DoD Physical Security Equipment Action Group (PSEAG; <https://dodpse.spawar.navy.mil> - portal registration required)
- Defense Advanced Research Projects Agency (DARPA; <http://www.darpa.mil>)
- Department of Homeland Security System Assessment and Validation Emergency Responders (SAVER; <https://saver.fema.gov>)
- Joint IED Defeat Organization (JIEDDO; <https://www.jieddo.dod.mil>)
- G3/5/7 Army Asymmetric Warfare Office (IED Defeat Division/ Asymmetric Warfare Group/ Electronic Warfare Division/ Rapid Equipping Force; <http://www.awg.army.mil/>)
- Army Materiel Command, Research Development and Engineering Command (<http://www.rdecom.army.mil/>)
- Army Test and Evaluation Command (ATEC; <http://www.atec.army.mil>)
- Corps of Engineers Engineer Research and Development Center (ERDC; <http://www.erd.c.usace.army.mil>)
- Product Manager, Force Protection Systems (PM-FPS; <http://www.pm-fps.army.mil>)
- Training and Doctrine Command, Army Capabilities Integration Center (<http://www.arcic.army.mil>)



# Existing Structures

## Introduction

Many times a FOB may make use of existing conventional buildings for housing, office space, exchange and recreation facilities, etc. However, in most cases these buildings do not provide acceptable levels of protection (LOP) from either VBIED blast or overhead protection from RAMs. Use Table 10-2 in Chapter 10 as an aid to decide what level of protection is acceptable.

Retrofitting buildings is generally an expensive and time consuming option. Some important factors for providing personnel protection in existing buildings against the blast from VBIEDs are outlined below.

- If occupying an existing structure with inadequate standoff to prevent exterior walls from failing from the blast load is unavoidable, do not occupy the exterior rooms on the side of the building most likely to be exposed to a VBIED direct blast if a retrofit is not available.
- Windows break at relatively low blast loads causing hazardous window fragments to be thrown into the building. If possible, locate personnel away from windows and doors or remove windows and fill or cover openings with material that is as strong as the surrounding wall and well connected to the wall.
- Any structural upgrades to buildings should use approved procedures or those designed by a structural engineer familiar with blast resistant design. Improvised strengthening measures may cause more harm than good.
- Connections are often the most critical part of blast resistant building upgrades. Therefore, they should receive special attention during construction. In general, the connections fail suddenly and should be stronger than the building components so that they are not the weak link in the overall building strength against blast loads.
- In almost all cases, injuries to building occupants from blast effects are not caused by blast pressures themselves. Rather, the injuries are caused by debris from failed building components and non-structural items inside the building. Therefore, upgrades should prevent building component failures or “catch” failed component debris.
- Interior non-structural items (bookcases, light fixtures, etc.) can also be very hazardous if a building is overpowered by blast loads. Location and weight of these components are very important. The closer to the ground these items are, the less hazardous they are. Anything

above head height is potentially most hazardous. Also, lighter, more crushable components are less hazardous than heavy, rigid components. Hazardous nonstructural components should be removed from exterior walls and rooms or well attached to the building structure if possible.

Table 19-1 (refer to the “Conventional Building Wall with No Retrofit” column) provides an estimate of standoff for different size vehicle bombs provided by conventional-style buildings. If the building utilizes load-bearing wall construction, it should not be used to house assets. For more precise standoff estimates, use a tool developed for such purposes (such as AT Planner or BEEM; See Figure 11-8 in Chapter 11).

### **Exterior Soil-Filled Container Retrofit**

One method for retrofitting the ground floor of a building is to use a soil-filled container wall on the exterior placed close to the building wall to shield it from the blast loads. However, it is very important that the wall is closed at the top and sides to prevent blast from entering through these openings. Figure 19-1 shows the exterior soil bin retrofit concept. Table 19-1 shows the standoff distances for different explosive charge weights for which this retrofit will provide a HIGH level of protection (refer to the “Exterior Soil-Filled Container” column).

A test configuration<sup>1</sup> was constructed in front of an 8-in. thick brick wall typical of Middle-Eastern light construction. It was then exposed to two blasts from 4000 lbs (TNT equivalent) at 145-ft and 121-ft. The soil-filled container wall was not damaged and the brick wall survived both detonations with negligible damage. The problem with this retrofit is that it is only practical for the ground floor walls. However, it also has the advantage that it will protect building occupants from small arms, RPGs and near miss rockets and mortars in addition to the VBIED blast effects.

### **Modular Concrete Wall Exterior Retrofit**

This retrofit is similar in concept to the soil-filled container wall except that it is made of precast modular concrete walls that are supported at the bottom by a footing and at the top by a leg that bears against the floor slab of the building (See Figure 19-2). The advantage of this retrofit is that it can be designed to resist large blast loads. The disadvantage is that the design is specific to the building requiring protection (dimensions, distance from foundation to first floor slab, standoff to the perimeter, etc.) and should be designed by a structural engineer familiar with blast-

<sup>1</sup>. See discussion in Chapter 21.

Table 19-1. Standoff Distances for Existing Structure Retrofits

VBIED Explosive Weight (lbs) ▼	Standoff distance needed for MEDIUM Level of Protection (ft) ►								
	Conventional Building Wall with No Retrofit	Exterior Soil-Filled Container (NOTE 1)	Pressure Sensitive Adhesive (NOTE 1 and 3)	Hi-Capacity Wall Catcher System (NOTE 3)	Geotextile Fabric Catcher System Fabric # (NOTE 2 and 3)				Polymer Retrofit System (NOTE 3)
					1	2	3	4	
50	110			3	15	18	23	26	17
220	181	46	46	6	34	41	56	69	41
500	238	60	60	10	61	71	92	110	62
1,000	300	76	76	13	92	110	151	171	90
4,000	476	121	121	33	215	271	342	400	180
10,000	646	164	164						

NOTES:

- 1. Exterior Soil Filled Container and Pressure Sensitive Adhesive columns are for **HIGH** Level of Protection; all other table columns are for **MEDIUM** Level of Protection.
- 2. See ETL 1110-3-494 for commercial designations of geotextile fabrics.
- 3. Do not use this retrofit for load-bearing wall structures.

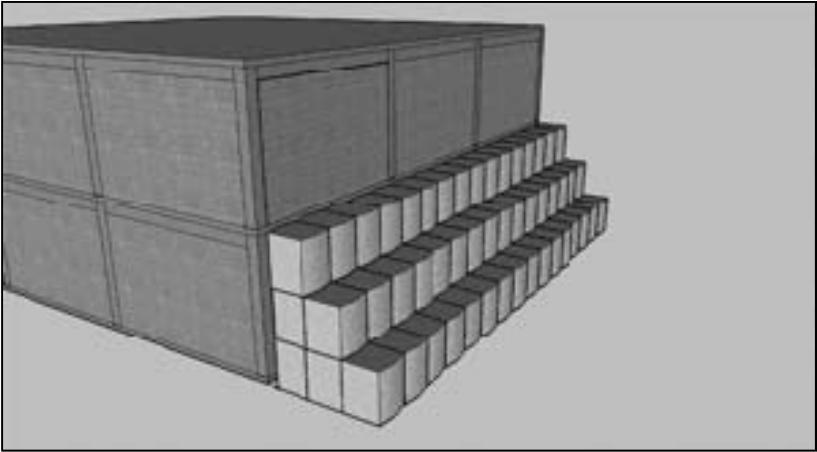


Figure 19-1. Soil-filled Container Exterior Wall Retrofit Concept

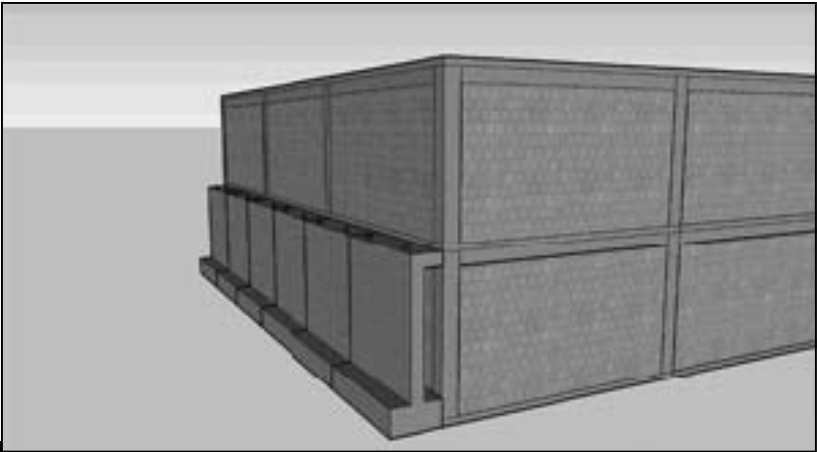


Figure 19-2. Modular Concrete Wall Exterior Retrofit Concept

resistant design. This retrofit will also provide protection from small arms fires and near miss of rockets and mortars. It does not protect from RPGs.

**Pressure Sensitive Adhesive Retrofit**

The pressure sensitive adhesive (PSA) is a material that is similar to a peel and stick wallpaper. It is an elastomeric/aramid fiber laminate with a pressure sensitive adhesive. It is applied to the wall and then anchored to the floor and ceiling slabs with a standard cold formed steel channel and concrete expansion anchors (See Figure 19-3). Table 19-1 shows the standoff distances for different explosive charge weights for which this retrofit will



Figure 19-3. Pressure Sensitive Adhesive Retrofit  
(Left: application to brick wall; Right: anchoring floor to slab)

provide a HIGH level of protection (refer to the “Pressure Sensitive Adhesive” column).

A test configuration<sup>2</sup> of this material was applied to the inside surface of an 8-in. thick brick wall typical of light Middle-Eastern construction. It was then exposed to two blasts from 4000 lbs (TNT equivalent) at 145 feet and 121 feet. The brick wall deflected inward as much as 8 inches but no debris entered the room. In fact the brick remained attached to the adhesive following the test.

### High Capacity Wall Catcher System

This system (see Figure 19-4) is an aggressive retrofit concept that is not designed to strengthen the wall. Instead, the design seeks to prevent injurious wall and window debris from entering the occupied spaces of the building, even for very close-in vehicle bombs. The system is composed of a thin (1/16 in. to 1/8 in.) steel plate attached to the diaphragms of the building with a highly ductile anchorage. A layer of crushable material is placed between the masonry and the plate to minimize the shear load at the support and to mitigate impact loads caused by individual pieces of the building wall. The crushable material may be high-density polyurethane foam or pumpable lightweight perlite concrete. The entire masonry wall (including any windows) is completely covered by the plate.

2. See discussion in Chapter 21.

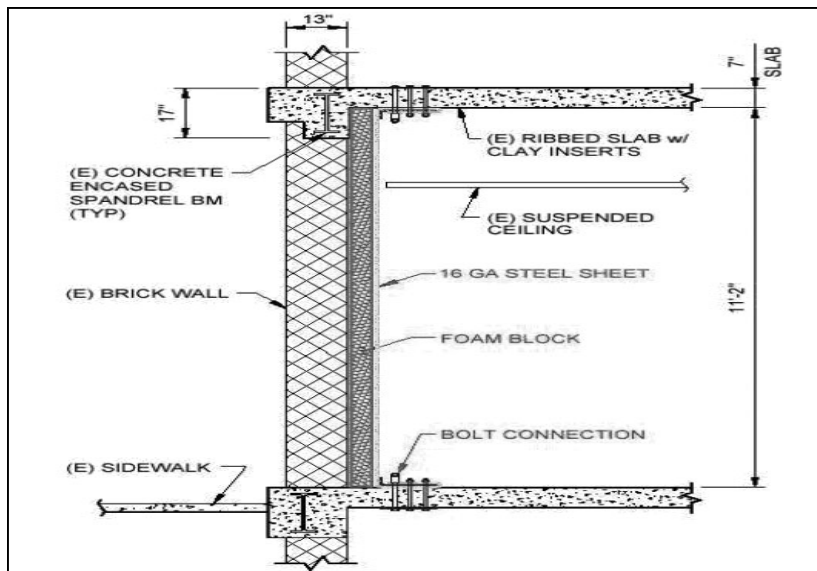


Figure 19-4. High-Capacity Wall Catcher System (Schematic View)

This retrofit is applicable to all non-load bearing wall types, especially for the worst-case threat on the ground floor. Adequate reinforced concrete floor and ceiling slabs are required to develop anchorage requirements for the retrofit. The designer will be responsible to ensure that the anchorage is adequate to mobilize the yield strength of the steel plate in tension membrane section.

Tests conducted with 500 lb. of ANFO at a standoff of 8 ft. showed this retrofit capable of providing a medium level of protection. Application of this data to other explosive weights is given in Table 19-1 (refer to the "Hi-Capacity Wall Catcher System" column).

### Geotextile Fabric Catcher System

A curtain of geotextile fabric (see Figure 19-5) is placed behind the existing masonry wall but not directly attached to it, covering the entire inside face of the wall. In the event of an explosion, the fabric catches the wall debris, preventing it from flying into the protected space and injuring occupants. This retrofit method is effective, relatively inexpensive, uses lightweight materials, and is easy to install.

This retrofit is applicable to unreinforced concrete masonry infill walls. It is not applicable to walls with windows, as the fabric must continuously span from floor to ceiling without interruption. It is not an aesthetically

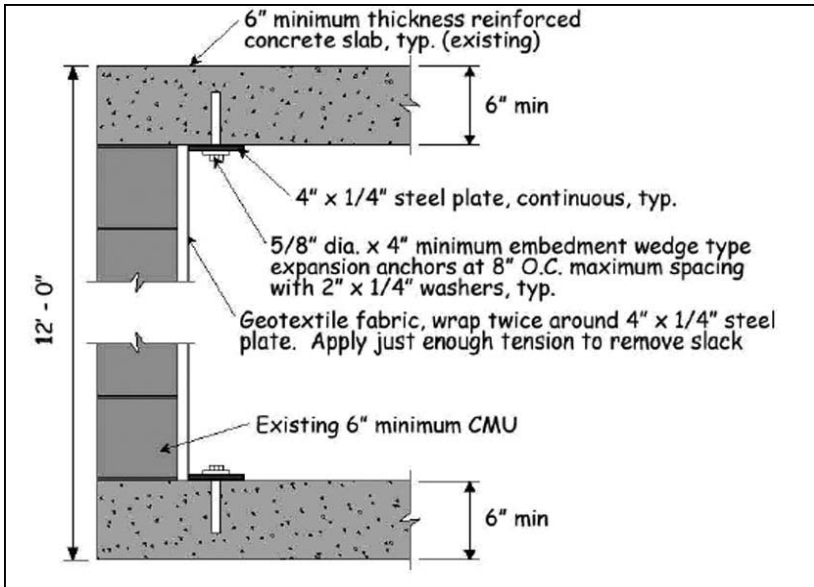


Figure 19-5. Geotextile Fabric Catcher System (Schematic View)

pleasing solution either.

Table 19-1 presents the standoff information for this retrofit. (refer to the "Geotextile Fabric Catcher System" columns) Standoff criteria are provided for four different types of fabric. The criteria were developed using analytical methods and verified by comparison with data from explosive tests. The results of the testing showed significant deformation of the fabric, but no debris entered the interior space. This retrofit provides a MEDIUM level of protection.

### Polymer Retrofit System for Masonry

Unreinforced masonry walls can be coated on the interior with an elastomeric polyurea coating to improve their resistance to air blast. This material is similar to that used for industrial coatings and spray-on liners for truck beds. Although the masonry walls may still shatter in a blast, the polymer material remains intact and contains the debris. This retrofit method is effective, uses lightweight materials, and is relatively inexpensive. There are two methods for applying the polyurea coating. One uses special application equipment with trained personnel to apply a "spray-on" coating to the wall (see Figure 19-6). The other is a "trowel-on" system (see Figure 19-7).



Figure 19-6. Spray-on polymer retrofit system



Figure 19-7. Trowel-on polymer retrofit system

This retrofit is applicable to unreinforced concrete masonry infill walls. It should not be used for load-bearing wall structures. Wall penetrations (for example, doors and windows) are permitted but must be carefully tied into the polymer coating.

Table 19-1 presents the standoff criteria for this retrofit (refer to the "Polymer Retrofit System" column). The criteria were developed by analytical methods and verified by comparison with experimental results. The results are conservative estimates of the retrofit wall response to blast loading. The analysis approach ensures debris will not enter the occupied space, but significant deformation of the wall will take place, providing a MEDIUM Level of Protection.



# Protective Structures

### Introduction

The full spectrum of survivability encompasses planning and locating position sites, designing adequate overhead cover, analyzing terrain conditions and construction materials, selecting excavation methods, and countering the effects of direct and indirect fire weapons. Survivability is also performed as a part of combat engineering and is focused on the hardening of facilities, personnel, equipment, and critical supplies in support of the maneuver commander at the brigade or regimental and lower echelons. It includes camouflage, concealment, and deception (CCD) support to tactical ground maneuver forces. This may include employing barriers, walls, shields, berms, and the construction of fighting positions and/or protective positions. Combat engineers typically provide the “lower end” hardening and CCD support while general engineering support is focused on those aspects that are not involved with close combat. In most cases, survivability support is designed to reduce vulnerability and enhance force protection.

Commanders of all units must know their requirements for protection (See Chapter 10). They must also understand the principles of fighting positions and protective positions, as well as the level of protection needed, given limited engineer assistance. The concepts presented here are illustrative of protective structures in common use. Custom designs are also in use, however they require thorough evaluation by a structural engineer for suitability of use in a tactical or combat environment.

### Bunkers

Bunkers offer excellent protection against both direct fire and indirect fire effects. Bunkers, built either above or below ground, are made of reinforced concrete, revetment material, or timber. If properly constructed with appropriate collective protection equipment, they can provide protection against chemical and biological agents. When designing a bunker, consider its purpose (command post or fighting position) and the degree of protection desired (small arms, mortars, or bombs). Prefabricated bunker assemblies (wall and roof) afford rapid construction and placement flexibility. These bunker designs that have been effective in both weapon effects tests and field evaluations.

**Concrete Bunkers.** An improvised reinforced-concrete bunker (often referred to as a “SCUD bunker”) has been built throughout the Iraq and Afghanistan theatres of operation. The bunker is typically constructed using reinforced concrete “C” sections with Jersey barriers placed across each end. Sandbags are placed around the body of the bunker and in front of the Jersey barriers (See Figure 20-1). They serve to increase fragmentation protection from near-miss indirect fire weapons.



Figure 20-1. Improvised bunker using concrete culvert sections. Sandbags provide increased fragmentation protection from near-miss weapons.

The lack of entrance shielding exposes the inhabitants to lethal fragmentation from incoming rounds detonating between the Jersey barrier and the bunker entrance or at the end of the bunker where there is line-of-sight to the bunker entrance. The “shielded entrance” modular concrete bunker shown in Figure 20-2 was developed to eliminate these concerns. **THIS IS THE RECOMMENDED CONFIGURATION FOR A CONCRETE BUNKER.**

*Performance.* Weapon effects test showed the sandbag/concrete walls provide good protection levels from moderately sized threats. A series of weapon effects tests using 82-mm and 120-mm mortars and 122-mm rockets verified the effectiveness of the shielded entrance modular concrete bunker design in defeating fragmentation and direct hits by those munitions. The modular concrete bunker can also be fully buried, and it can be constructed in multiple configurations.



Figure 20-2. Shielded entrance concrete bunker (shown without soil cover). Steel straps connect the bunker modules together.

*Construction Procedures.* Weapon effects protection is provided by soil cover when the bunker is fully buried, in a cut and cover configuration, or constructed above ground and covered by several layers of sandbags.

- Place 2 to 3 layers of sandbags on the roof to generate full protection from the quick-fused 82-mm and 120-mm mortars. With no sandbags, only a minor spall hazard should be expected for the 82-mm, but fairly significant spall and breaching hazards could be expected for the 120-mm mortar.
- Cover the bunker with approximately 48 in. of sandbags or bury it with approximately 48 in. of soil cover for full protection from the quick-fused 122-mm rocket.
- Place a minimum of 2 layers of sandbags along the bunker walls for full protection from the blast and fragmentation of near-miss (4 ft.) hits of the 82-mm and 120-mm mortars and 122-mm rocket.
- See Figure 20-3 for general dimensions and reinforcing details for the primary sections of the bunker. The recommended concrete compressive strength is 4,000 psi. The sections are connected together with steel straps (shown in Figure 20-2).

*Limitations.* This bunker provides temporary protection, given sufficient warning of incoming threats. Although referred to as a “SCUD bunker,” this bunker will not protect its occupants from near misses of a SCUD missile.

**Soil-Filled Container Bunkers.** Soil-filled containers have many applications. One commonly used application is bunkers for personnel and equipment protection. Constructed properly, these bunkers will protect from direct hits of 82-mm mortar rounds, and the sidewalls of the above-ground bunkers will stop the fragmentation from near-contact burst of up to 120-mm mortar, 122-mm rockets and 155-mm artillery rounds. See Appendix D for soil-filled container applications.

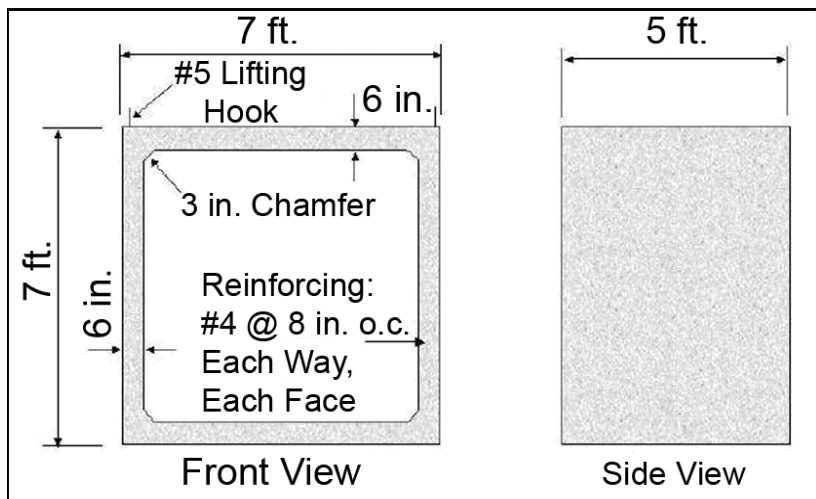


Figure 20-3. Primary module for modular concrete bunker

**Timber Bunkers.** Like the other bunkers already discussed, timber bunkers are either underground, partially underground, or above ground. Numerous designs are presented in FM 5-103, *Survivability*. In all cases, soil cover provides fragmentation and blast protection. The timbers are used to provide support for the soil cover. Table 20-1 provides a quick reference for the allowable span length and spacing of different size timbers that will support various soil depths to provide contact burst protection from 82-, 120-, 122-, and 152-mm rounds.

**NOTE:** The maximum beam spacing listed in Table 20-1 is 18 in. This is to preclude further design for roof material placed over the stringer to hold the earth cover. A maximum of 1 in. wood or plywood should be used over stringers to support the earth cover for 82-mm burst; 2 in. should be used for 120-mm, 122-mm and 152-mm burst. **Table information is based on both Dead Load and Blast Load Effects.** Consult with a security engineer for further clarification.

### Fighting Positions and Observation Posts

In order to protect their personnel in hostile areas, commanders or leaders must fully understand the importance of fighting positions and observation posts, both in the offense and in the defense. Above-ground observation

Table 20-1. Center-to-Center Spacing for Wood-Supporting Soil Cover to Defeat Various Contact Bursts (From FM 5-34)

Nominal Stringer Size (in.)	Depth of Soil, ft. (m)	Span Length, ft. (m)				
		2 (0.6)	4 (1.2)	6 (1.8)	8 (2.4)	10 (3.0)
		Center-to-Center Stringer Spacing, in. (cm)				
		82-mm Contact Burst				
2 x 4	2.0 (0.6)	3 (7.6)	4 (10)	4 (10)	4 (10)	3 (8)
	3.0 (0.9)	18 (46)	12 (30)	8 (20)	5 (13)	3 (8)
	4.0 (1.2)	18 (46)	14 (36)	7 (18)	4 (10)	3 (8)
2 x 6	2.0 (0.6)	4 (10)	7 (18)	8 (20)	8 (20)	6 (15)
	3.0 (0.9)	18 (46)	18 (46)	16 (41)	12 (30)	8 (20)
	4.0 (1.2)	18 (46)	18 (46)	18 (46)	11 (28)	7 (18)
4 x 4	2.0 (0.6)	7 (18)	10 (25)	10 (25)	9 (22)	7 (18)
	3.0 (0.9)	18 (46)	18 (46)	18 (46)	12 (30)	8 (20)
	4.0 (1.2)	18 (46)	18 (46)	18 (46)	10 (25)	7 (18)
4 x 8	1.5 (0.5)	4 (10)	5 (13)	7 (18)	8 (20)	8 (20)
	2.0 (0.6)	14 (36)	18 (46)	18 (46)	18 (46)	18 (46)
	3.0 (0.9)	18 (46)	18 (46)	18 (46)	18 (46)	18 (46)
		120-mm and 122-mm Contact Burst				
4 x 8	4.0 (1.2)	3.5 (9)	4 (10)	5 (13)	5 (13)	6 (15)
	5.0 (1.5)	12 (30)	12 (30)	12 (30)	11 (28)	10 (25)
	6.0 (1.8)	18 (46)	18 (46)	18 (46)	16 (41)	12 (30)
6 x 6	4.0 (1.2)	--	--	5.5 (14)	6 (15)	6 (15)
	5.0 (1.5)	14 (36)	14 (36)	13 (33)	12 (30)	10 (25)
	6.0 (1.8)	18 (46)	18 (46)	18 (46)	16 (41)	12 (30)
6 x 8	4.0 (1.2)	5.5 (14)	6 (15)	8 (20)	9 (23)	10 (25)
	5.0 (1.5)	18 (46)	18 (46)	18 (46)	18 (46)	18 (46)
8 x 8	4.0 (1.2)	7.5 (19)	9 (23)	11 (28)	12 (30)	13 (33)
	5.0 (1.5)	18 (46)	18 (46)	18 (46)	18 (46)	18 (46)
		152-mm Contact Burst				
4 x 8	4.0 (1.2)	--	--	--	--	3.5 (9)
	5.0 (1.5)	6 (15)	6 (15)	7 (18)	7 (18)	7 (18)
	6.0 (1.8)	17 (43)	16 (41)	14 (36)	12 (30)	10 (25)
	7.0 (2.1)	18 (46)	18 (46)	18 (46)	15 (38)	11 (28)
6 x 6	5.0 (1.5)	7 (18)	8 (20)	8 (20)	8 (20)	7 (18)
	6.0 (1.8)	18 (46)	18 (46)	15 (38)	12 (30)	10 (25)
	7.0 (2.1)	18 (46)	18 (46)	18 (46)	15 (38)	11 (28)
6 x 8	4.0 (1.2)	--	--	--	--	6 (15)
	5.0 (1.5)	10 (25)	11 (28)	12 (30)	12 (30)	12 (30)
	6.0 (1.8)	18 (46)	18 (46)	18 (46)	18 (46)	17 (43)
8 x 8	4.0 (1.2)	--	--	--	--	8 (20)
	5.0 (1.5)	14 (36)	14 (36)	16 (41)	17 (43)	16 (41)
	6.0 (1.8)	18 (46)	18 (46)	18 (46)	18 (46)	18 (46)

Table information is based on both Dead Load and Blast Load Effects

See note on Page 11-34 or refer to FM 5-34.

posts provide the best observation and are easier to enter and exit than below-ground shelters. They also require the least amount of labor to construct, but are hard to conceal and require a large amount of cover and revetting material. While it is desirable for a fighting position to give maximum protection to personnel and equipment, primary consideration should always be given to effective weapon use. In offensive operations, weapons are sited wherever natural or existing positions are available, or where weapon emplacement is made with minimal digging (See Figure 20-4).

Many designs use soil-filled containers for construction of fighting positions and observation posts. These positions will allow engagement of an enemy and offer some level of protection from small arms, VBIEDs and near-miss and direct hits of RAMs. These designs have been developed and tested by the U.S. Army Engineer Research and Development Center (ERDC). Test results indicate that the overhead cover provided will protect from direct hits of 81/82-mm mortar rounds and that the sidewalls of the positions will stop the fragmentation from near contact bursts of up to 120-mm mortar, 122-mm rocket and 155-mm artillery rounds. See Appendix D for soil-filled container applications.

## Towers

Design of guard towers and observation posts must begin with a physical site study, including terrain analysis, and an analysis of security requirements. Based on this data, basic design considerations include:



Figure 20-4. A fighting position constructed on a rooftop

- Accommodations for the maximum number of personnel required in the guard tower(s)/observation posts to meet security requirements
- Required number of guard towers/observation posts
- Installation requirements for electronic and communications equipment, including location in the guard tower/observation posts, for optimum use by security personnel
- Heating, ventilation, air conditioning (HVAC), and plumbing requirements
- Appropriate small arms protection for security force personnel based on the anticipated threat
- Provisions to ensure that security personnel under duress are able to transmit signals discretely to other security personnel by electrical, electronic, or oral means
- Installation of a searchlight on the center of the tower roof that can be rotated manually by the tower occupant

As a minimum, gun ports should be designed to ensure that the perimeter and the entire clear zone can be brought under fire. Another design consideration is the compatibility of gun ports to type of weapons and attachments to be used (for example, night vision scopes).

The location and height of the guard tower/overwatch that best suits a particular FOB should be based on, to a great extent, the nature of the facility, the terrain to be under observation, the physical environment, and the functions that the tower will serve. Place towers/overwatch inside the perimeter of the FOB with at least a 30 ft (9.1m) inner clear zone. Guard tower/overwatch positions must be located so that the entire inner and outer clear zones and fence line can be observed.

**Sandia National Laboratories Design.** Sandia National Laboratories has designed a guard tower/overwatch position that consists of pre-cast concrete, double-tee beams placed vertically to form the walls of the tower and a pre-cast concrete cab placed atop the structure to house the guard quarters and surveillance equipment (See Figure 20-5). The completely enclosed space formed in the interior of the double-tee shell provides protection from attack and from extremes in weather conditions. Due to the possibility these towers will be constructed in diverse locations of the world, the design considered a 150 mph (241.4 km/hr) wind and zone 3 seismic loading. The tower should be supported on a spread footing with a maximum allowable bearing of 2,300 psf (11,230.9 kg/sq m). It should be noted that some areas may require specialized foundations, such as piles, caissons, etc. Walls a minimum of 4 in. (101.6 mm) thick provide excellent resistance to small arms projectiles because double-tee concrete has a 28 day compressive strength of 5,000 psi (3,515,500 kg/sq m). This also provides significant ballistic properties.

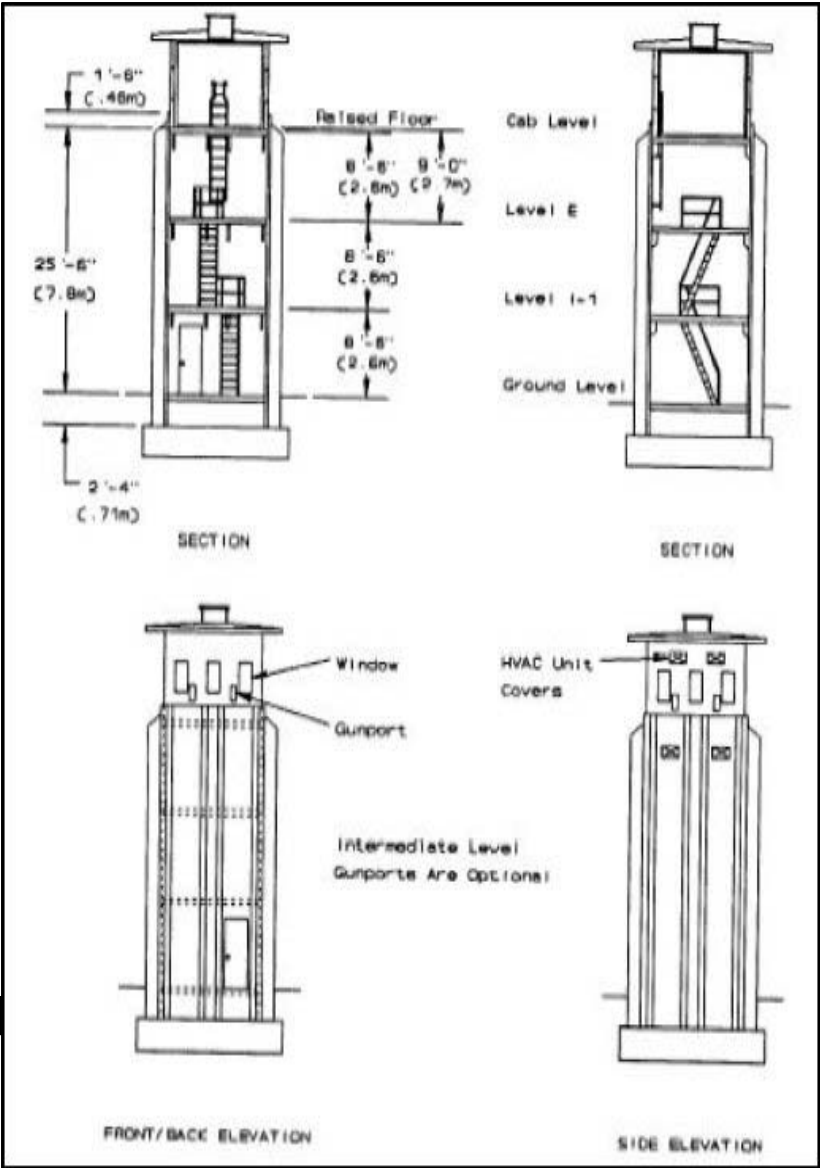


Figure 20-5. Sandia Laboratories Guard Tower Design  
(From MIL-HDBK-1013/10)

**Pre-cast Concrete Pipe Guard Tower.** This type of tower is constructed of eight precast elements (See Figure 20-6). Welds placed on plates embedded in each segment connect the elements. The tower contains an internal bunker just below the cab. The construction sequence is: (1) Place



the rectangular footing on the ground; (2) Place the bottom pipe section on the base; (3) Place the next pipe section the same way; (4) Place a floor section on the pipe section; (5) Place the next pipe section; (6) Place a floor section on the pipe section; (7) Place the cab section; and (8) Place the roof section.

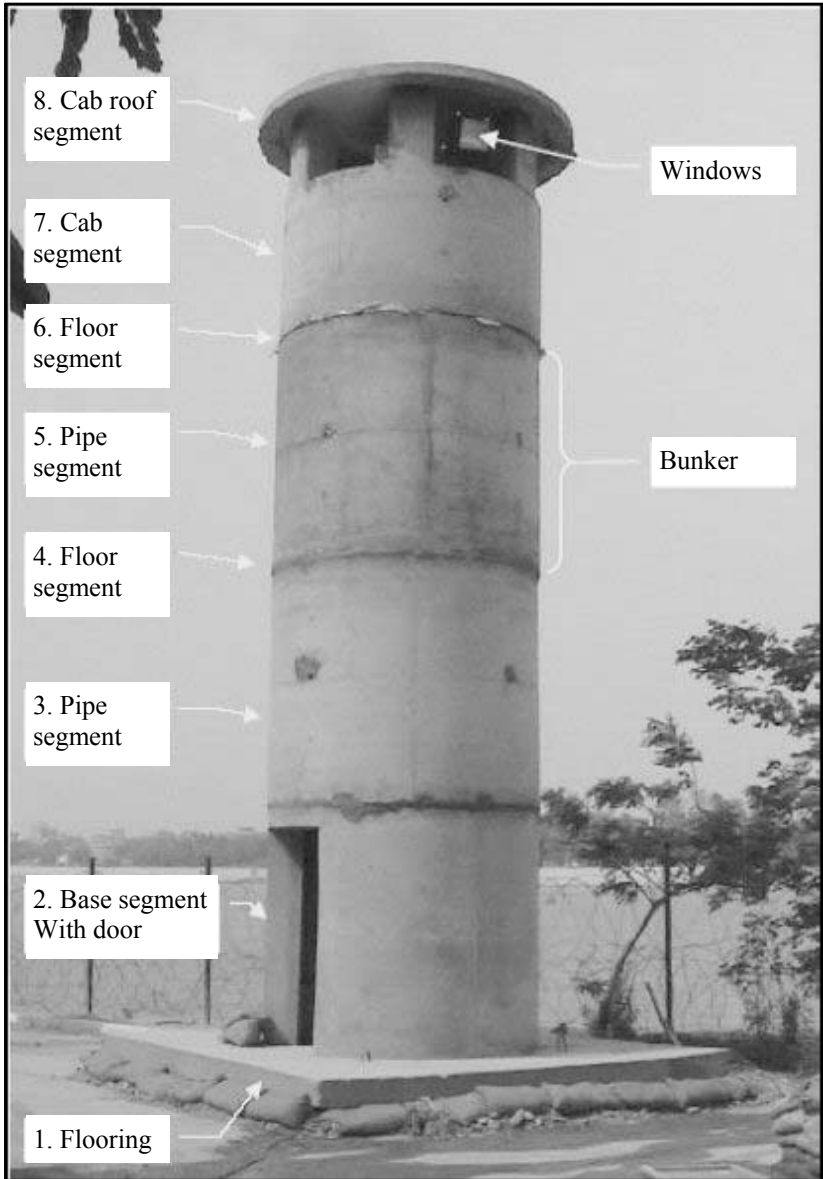


Figure 20-6. Precast Concrete Pipe Guard Tower Design

**Freight Container Guard Tower.** This guard tower design by the U.S. Navy consists of up to five stacked steel containers, where each container is approximately 8 ft. x 8.5 ft. x 20 ft. (2.4 m x 2.6 m x 6.1 m), weighing 5,000 lb (2,268 kg) empty (See Figure 20-7). The bottom container is attached to large cast-in-place concrete footings with anchor bolts and all other containers are bolted to the container below, as required to resist all conventional design loads. The top container is empty and acts as a pre-detonation screen against a direct mortar or artillery hit. A shielding layer is placed at the floor of the top container to resist fragments from detonated weapons at the container roof. Sandbags, E-glass, or similar fragment resistant material is placed along the inside face of the container walls at all inhabited levels to protect against direct and indirect fire threats as required. Ballistic resistant glazing can also be used over all windows. Contact Naval Facilities Engineer Command for details.

**Portable Guard Tower.** The Portable Guard Tower (See Figure 20-8) is a complete unit which includes one guard tower, one standard freight container (CONEX Box), one pallet (75 coils or 3750 ft) of 18" Helix Coil, and a wire installation kit. The wire installation kit includes a fence driver, 25 5-foot stakes, and 25 7-foot stakes. Options available include either concertina wire or hook barbed detainer wire.

The guard tower itself is manufactured with four separate wall units that allow for quick and easy assembly on top of the CONEX Box. Once placed on the CONEX Box the guard tower will be approximately 12 feet in the air, giving the guards a greater view of the perimeter or area of threat. Once in position, the walls are filled from the top using sand as ballast. The sand filled walls provide the guards inside with 360 degrees of protection from 9mm, 5.56 mm, and 7.62 mm threats. 12" dumps are provided for easy removal of the ballast allowing the guard tower to be repositioned as needed.

The overhead cover is 3/4" plywood on which lights, sensors, and antennae can be installed if desired. Access to the cover can be reached through a hatch type door that is pre-installed for convenience. This guard tower eliminates the time and the mess associated with using sandbags. This product is a recoverable asset that can be broken down and deployed inside the CONEX Box.

All parts and tools needed for assembly are included in the kit bag. Stakes are also provided for the Concertina Wire installation. The standard colors for the Portable Guard Tower are olive drab or desert tan. The tower is available for purchase through GSA (<http://www.gsaadvantage.gov>; Item GS-07F-9503S; current price \$11,572.09).

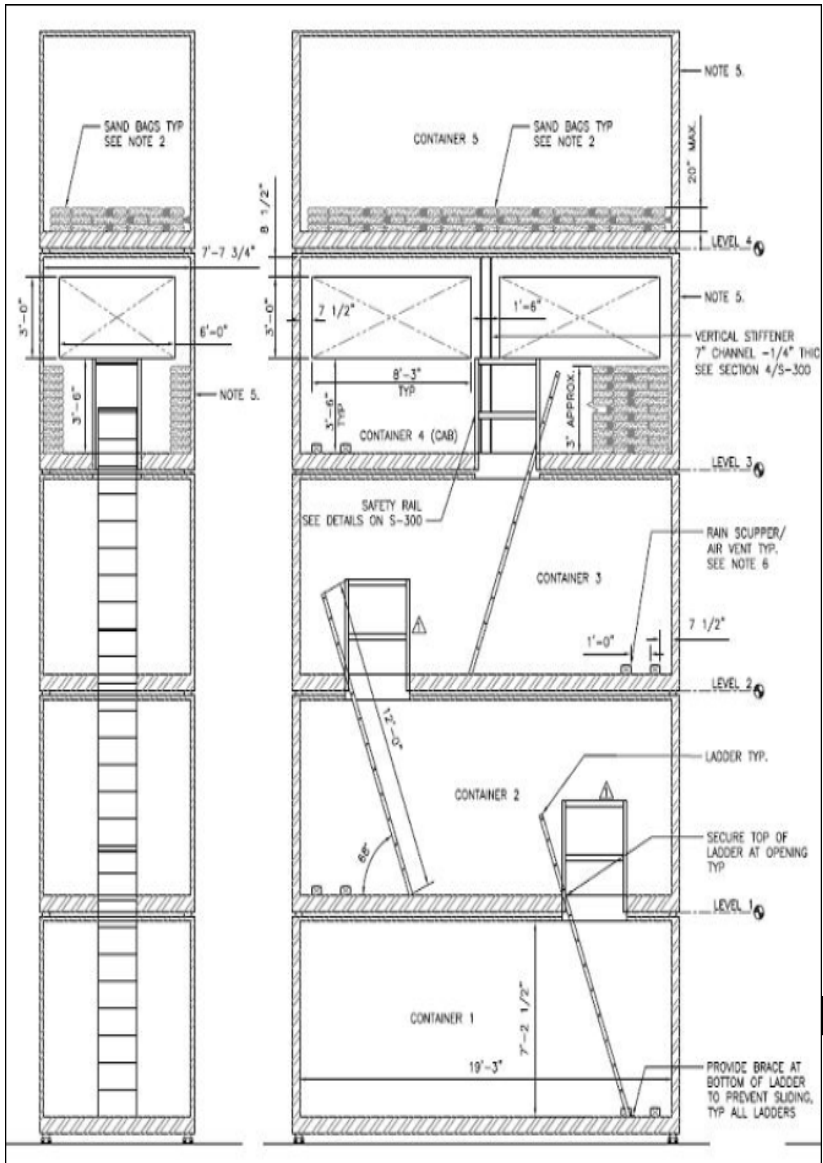


Figure 20-7. Freight Container Guard Tower Design

**Camp Bondsteel Kosovo Design.** A design used extensively during the Kosovo campaign is shown in Figure 20-9. This design utilizes 3/4 inch plywood and lumber posts and braces. This guard tower requires interior sand bags or other fragment resistant material to resist small arms and indirect fire threats. The U.S. Army Corps of Engineers Protective Design Center has information on the design and construction of this tower.

Detailed drawings for these designs are scheduled to be released electronically with a new UFC tentatively titled “Design of Deployed Operational Bases to Mitigate Terrorist Attacks.” More information on UFC’s is available at <https://pdc.usace.army.mil/library/ufc/>.



Figure 20-8. Portable Guard Tower

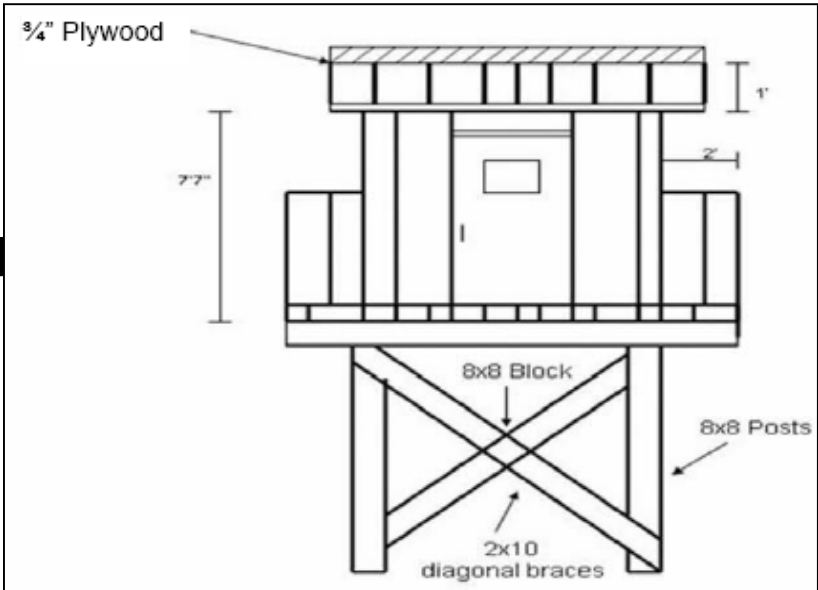


Figure 20-9. Camp Bondsteel Kosovo Guard Tower Design

# Joint Combat Outposts

## Introduction

The first rule of counterinsurgency (COIN) operations is to establish the force's presence in the area of operations (AO).<sup>1</sup> COIN doctrine is being executed in Iraq and Afghanistan by moving personnel from larger, more secure, forward operating bases and establishing Joint Combat Outposts (JCOPs)<sup>2</sup> at critical areas in close contact with the local population. This creates relationships designed to improve security, establish government control, and gain the support of the population. However, moving from the larger, more secure FOBs increases force protection concerns and risks that had previously been reduced. This chapter provides tactics, techniques, and procedures to mitigate risk situations created when occupying the smaller JCOPs with fewer personnel and less established defensive fortifications.

## Threats and Risks

The overall threat is an insurgent using a weapon against allied or coalition forces on or near a JCOP. Figure 21-1 illustrates the most severe attack of a dual VBIED on the outpost. The results from the first VBIED will be a crater that the second VBIED must drive through or around in this double VBIED attack scenario. The speeding VBIEDs may be supported by small-arms fire and rocket-propelled grenades as shown.

A risk assessment combines threat severity and probability estimates in a risk assessment matrix. For example, with a double-VBIED attack using thousands of pounds of TNT-equivalent explosives along with small arms fire, the severity may be judged to be "Catastrophic" with a "Likely" probability of attack. The intersection of the "Catastrophic" row and "Likely" column on the matrix shows the risk level as "E" (Extremely High—IB; See Figure 23-2). Using the same methodology, the risk assessments for improvised rocket assisted mortar (IRAMs) and all other threats are "High—IC" and "Medium—IIIC" respectively. The actual risks will vary from location to location. The force protection officer should keep these results to guide the next set of decisions regarding controls to limit risk.

1. See Army Field Manual [FM] 3-24/Marine Corps Warfighting Publication [MCWP] 3-33.5, *Counterinsurgency*, p. A-4.  
2. Army FM 3-90, *Tactics*, defines a combat outpost as a reinforced observation post (OP) capable of conducting limited combat operations. This generally accepted definition will apply to the discussion of JCOPs throughout this chapter.

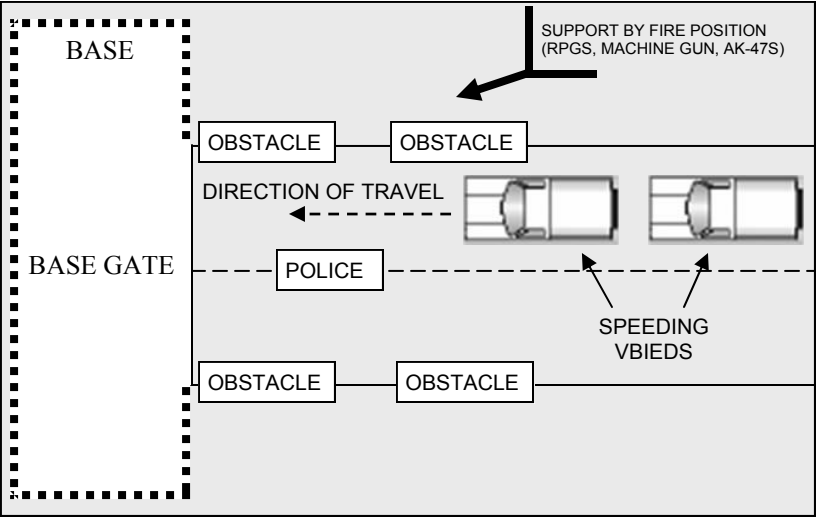


Figure 21-1. Complex VBIED Attack (from *TRADOC DCSINT Handbook No. 3*)

Severity ▼		Probability ►				
		Frequent	Likely	Occasional	Seldom	Unlikely
		A	B	C	D	E
Catastrophic	I	E	E <sup>1</sup>	H <sup>2</sup>	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M <sup>3</sup>	L	L
Negligible	IV	M	L	L	L	L
(1) Double VBIED Attack; (2) IRAM Attack; (3) All Other Threats						

Figure 21-2. Risk Assessment Matrix for a JCOP

### Layout and Design

During the JCOP layout and design stage, methods for integrating perimeter security, standoff, protective construction, entry control points, vehicle barriers, and security lighting to diminish potential threat to personnel and critical assets should be addressed. Figure 21-3 shows a conceptual JCOP layout.

One of the key aspects of this planning is deciding what level of protection (LOP; See Table 10-2 in Chapter 10 for a discussion of Levels of Protection) is warranted or desired for JCOP Personnel. The key issue regarding

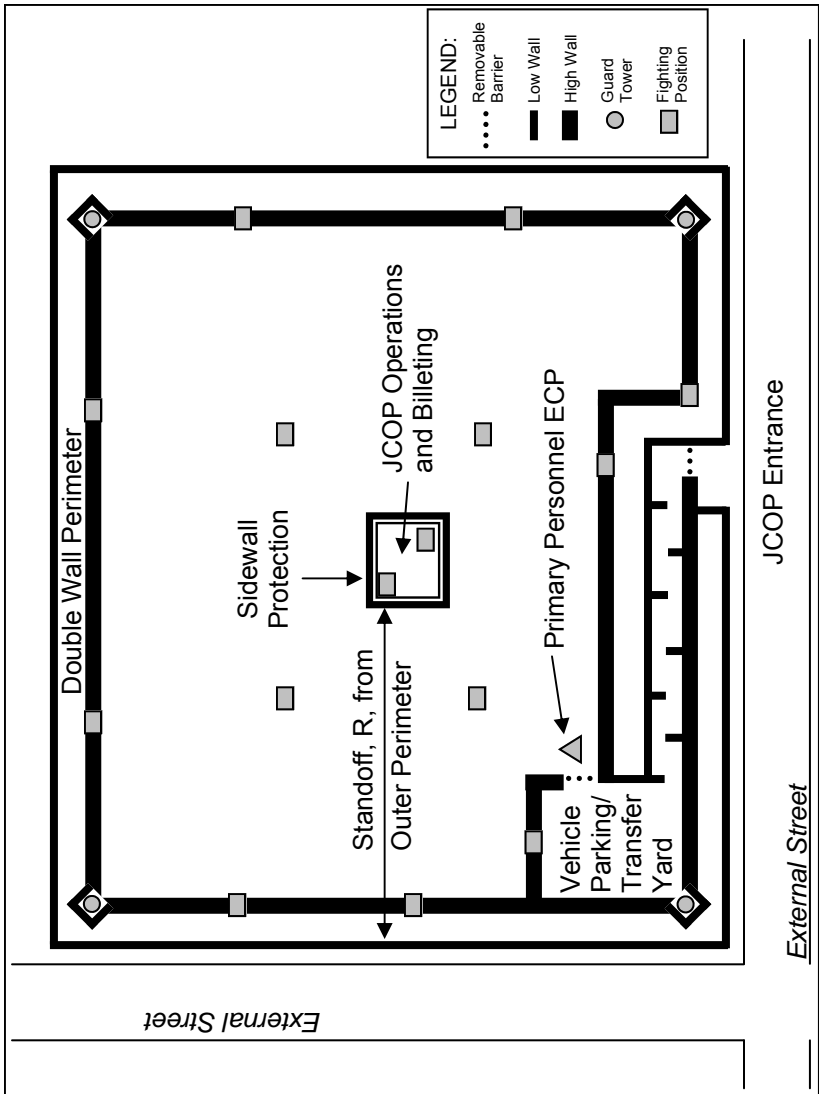


Figure 21-3. Conceptual Layout of a JCOP

LOP is that more resources (standoff, construction effort, time, personnel, etc.) are needed for higher LOPs. Consideration of measures that provide the desired level of protection during the site selection stage may preclude the need for applying more stringent protection measures to the JCOP at a later time. The following paragraphs highlight site selection considerations for protecting a JCOP from VBIEDs and direct fire weapons.

**Parking and Roadways.** Detonation of VIBEDs can occur without warning on nearby roadways and parking areas. For a JCOP, do not allow vehicles inside the primary compound. Instead, set up a parking area and transfer point in a protected area near the perimeter. Locate vehicle entrances so there is no straight-line entrance into the compound. Direct pedestrian and vehicle routes of travel for local residents away from the JCOP. Unauthorized and unofficial traffic should also be routed away from the JCOP.

**Terrain Features.** Although less likely and more obvious than attacks along roadways, attacks can occur over open terrain. Choose a site with natural and manmade terrain features that can prevent a vehicle attack over open terrain at the perimeter (such as a lake or a deep drainage ditch on one side). A site with terrain features that provide clear observation and fields of fire (such as a large open field on one side) will allow easy detection, assessment, and engagement of any approaching vehicle.

While open fields allow for clear observation and fields of fire, open fields have many civilian uses that will be taken away if used for a JCOP. If local leaders are not involved in the decision process this may increase the chances of alienating the local population. This may increase the chances of the JCOP being attacked because its location has upset the populace and given them a reason to help adversaries. Placing a JCOP away from a population center may also make it easier for an adversary to attack it without risking injury to civilians (which could become an information operations disaster for them). Another issue with placing a JCOP away from population centers is that civilians may be more exposed to enemy surveillance when travelling to the JCOP.

**Standoff.** If attacks can occur at locations along the perimeter, provide as much standoff as possible from the perimeter to structures occupied by JCOP personnel. Design a site that will provide defense in depth, one that requires an adversary to negotiate a series of varied and often alternating obstacle/barrier layers, interspersed with varying distances of open ground.

**Perimeter Walls.** Select a site that allows for the construction of the recommended perimeter wall; consider a flat area near the perimeter that will provide a good foundation for wall placement and construction. Use a double perimeter wall system to prevent a double VBIED attack from gaining entry into the compound (See Figure 21-4). This is a combination low wall and high wall system to provide obscuration and direct fire protection. Recent explosive tests have shown that a low outer wall with a high inner wall is the preferred configuration. Use only soil-filled containers for the perimeter walls since concrete walls become large debris pro-





Figure 21-4. Double-wall perimeter system concept

jectiles up to several hundred feet. For an existing site this may involve backing existing concrete walls or removing concrete walls and replacing them with soil-filled containers.

**Potential Enemy Vantage Points.** Select a site to limit, or preferably block, an attack by direct line-of-sight weapons from potential vantage points. Use natural or manmade obstructions, such as trees, perimeter walls, obscuration netting, land forms, or buildings to obscure sight paths. Choose a site at a high point that forces aggressors to fire up toward the JCOP. Avoid locations that have higher surrounding terrain or buildings that allow line-of-sight into the JCOP. Use obscuration netting to limit visibility into and around buildings.

**Use of Existing Buildings.** If existing buildings are needed for operations and billeting, it is very important to obtain an engineering assessment of the type and quality of construction used. Avoid sites having load-bearing wall buildings. Depending on the number of stories and the construction details, this type of building can collapse catastrophically if one or more of the walls fail due to the blast. It may be better to use tents rather than occupy a building of this type.

**Restricting Vehicle Attack Speed.** For a given site, analyze the possible attack routes to determine the worst case (the one with the maximum possible attack velocity and angle). In order to identify the worst-case attack scenario, make a sketch of the site and the surrounding topography, buildings and streets (See Figure 21-5). For each segment of the site boundary, identify the longest, straightest, most level path that an attack vehicle could use. Different arrangements of site boundaries, surrounding topography, buildings, and pathways result in different attack paths. Any surface on which a vehicle can be driven can be used in an attack (street, lawn, or sidewalk). A path must be at least 8 feet wide to be used in an attack, and may be wider for large trucks. A path must have no radius of curvature less than 22.5 feet to be used in an attack.

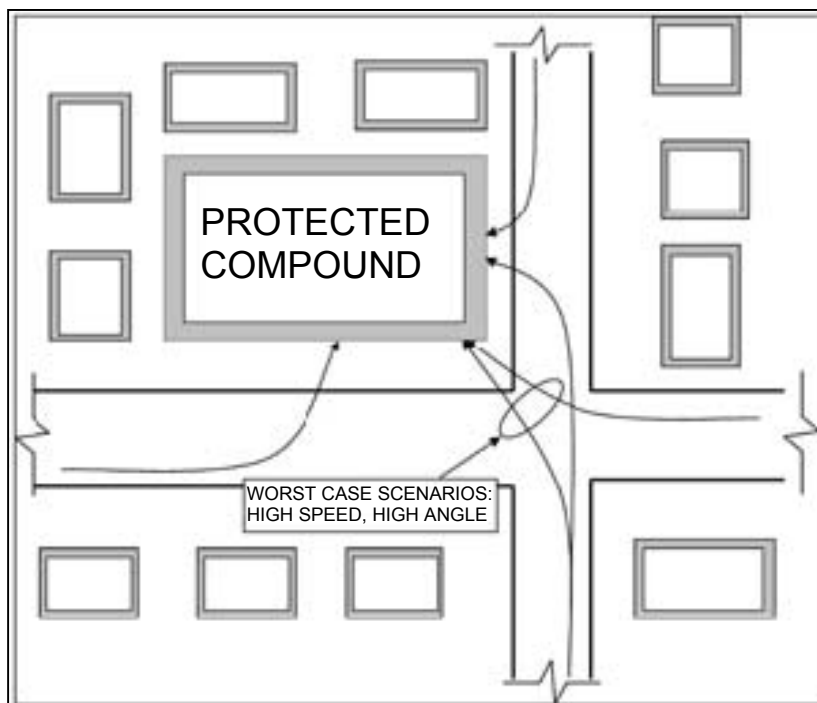


Figure 21-5. Example sketch of a JCOP attack scenario

**Cultural Considerations.** Other reasons for carefully considering JCOP placements involve sensitivities and concerns of the local populace. The potential for ill-considered JCOPs to substantially disrupt the local populace's daily lives and produce other unintentionally negative effects is significant. JCOPs must be set up so that they do not project an image of undue permanency or a posture suggesting a long-term occupation. Similarly, logistics postures that project an image of unduly luxurious living conditions while host nation civilians suffer should be avoided.

While the JCOP should be viewed as a temporary position for US forces, it may become a permanent location for host nation security forces. If the location decision is made with local authorities and host nation security forces consultation, the JCOP may be used long after US forces have left.

### Perimeter Security

The goal of perimeter security is to safeguard the JCOP mission by protecting personnel and property. This is accomplished through prevention, detection, and response to enemy-threat tactics (to include the double VBIED attack), attacks using direct fire weapons such as small arms and RPGs, and PBIED attacks. The perimeter zone is not only the actual pe-

rimeter of the JCOP but can also include an area outside the perimeter from which the site would be vulnerable to a VBIED attack as well as direct fire and standoff weapons. The properly designed perimeter should provide an integrated, layered, defense-in-depth.

**Standoff.** The best technique to reduce the risks and effects of an attack, especially one involving explosives (such as VBIEDs and PBIEDs) is to keep the attack as far away from the JCOP as possible. Injury to personnel from the primary blast and blast damage to buildings decreases significantly with standoff distance. If feasible, the area outside the perimeter should be controlled to prevent potential threat vehicles from approaching the JCOP closer than the needed standoff. To provide standoff for PBIEDs, no unauthorized personnel should be allowed inside the perimeter.

**Access Control.** Each JCOP must clearly define access control measures required to ensure only authorized personnel gain entry to the JCOP. Access control procedures should be designed to delay attackers by increasing the amount of time needed to gain access to the JCOP and allow security personnel to sound alarms and take immediate protective actions to address the threat. The recommended type of access for a JCOP in a high threat environment is one that limits all personnel access to only mission-essential personnel. Likewise, it is recommended that vehicle access be limited to only mission-essential vehicles; with all vehicles remaining outside the interior of the JCOP in a vehicle parking/transfer yard.

**Security Lighting.** Security lighting requirements for the JCOP will vary based on light discipline restrictions and availability of lighting systems. Regardless the type of lighting used (continuous, standby, emergency or motion-activated lighting), security lighting should serve as a deterrent and aid in threat detection, assessment and response.

**Guard Towers/ Overwatch/ Fighting Positions.** Position guard towers and fighting positions so they have a clear line of sight to engage attackers and ensure they have proper weapons and protection. Combinations of elevated towers and hardened fighting positions are recommended around the perimeter of the JCOP. All of these positions are intended to enhance security by providing identification, assessment and engagement of potential threats.

**Intrusion Detection and Surveillance (IDS) Systems.** IDS systems, if used, can enhance the ability of JCOP security force personnel to detect and defeat intruders. IDS systems are also an excellent force multiplier, allowing for a more economical and efficient use of security force personnel. The use of IDS systems for a JCOP will be dependent upon availabil-

ity of systems and the ability of JCOP personnel to install, operate and maintain the systems. The requirement for IDS must be identified during the JCOP site selection and design process.

**Internal Security.** The initial focus of security forces at a JCOP should be on establishing or reassessing force protection measures at the perimeter of the base. Once these measures are adequate, attention should be directed to internal security procedures. Internal security consists of those measures used to protect personnel or assets located on the interior of the JCOP. Regardless of the type of measure implemented, internal security procedures should be constantly assessed to ensure changes in the threat are incorporated into the JCOP security posture.

### **Perimeter Barriers**

Barriers are an integral part of the JCOP perimeter security system and serve to facilitate control of pedestrians and vehicles. Physical barriers used in the JCOP perimeter security system should control traffic on both perpendicular and parallel roadways surrounding the JCOP, create the primary double perimeter wall system (including the exterior and interior walls for the entry control point (ECP) and vehicle parking areas), provide vehicle and traffic control measures at the ECP, provide a removable anti-vehicular barrier for the entrance to the ECP and the primary personnel ECP, and provide antipersonnel barriers along the perimeter and at the ECP/primary personnel ECP.

**Traffic Control Barriers.** These barriers are used for controlling traffic on roadways surrounding the JCOP. They should have the following capabilities.

- Slow vehicles to 30 mph or less along roadways perpendicular to the JCOP perimeter where a high speed attack could occur. Such barriers should be used in a serpentine layout. Typical barriers for this use include cabled jersey barriers and soil filled containers.
- Close roads and perpendicular high speed avenues of approach, block off-road approaches and potential approaches over median strips or traffic islands. Stop or at a minimum slow the potential attack vehicle from its estimated impact speed to 30 mph before it impacts the outer perimeter wall. Examples include soil filled containers, ditches, berms, cabled jersey barriers and field expedient rubble.

**Double Wall Barriers.** These barriers comprise the primary double perimeter wall system, including the exterior and interior walls for the entry control point (ECP) and vehicle parking areas). They should have the capability of stopping moving vehicle bomb threats in a two stage attack;

capable of stopping a second VBIED after detonation of a first VBIED. In addition they should be able to stop most of the fragments from the VBIEDs and should not create a significant secondary debris hazard.

Use soil-filled container systems for the perimeter walls to minimize the debris hazard. Explosive blasts adjacent to concrete walls create large pieces of debris and fragments that can travel long distances. Remove concrete walls from an existing site and replace them with soil-filled containers or back existing concrete walls with them.

A combination low barrier on the outer perimeter wall and a high barrier on the inner perimeter wall is effective in most situations. This combination allows for visibility and observation of engagement zones and fields of fire from guard towers and fighting positions. Use low barriers for the outer perimeter wall that are capable of stopping a 30 mph attack. Soil-filled containers or anti-vehicle ditches are preferred since they do not create debris hazard. However, double jersey barriers with soil between them are an acceptable alternative. The soil will help mitigate the velocity of concrete debris. Place the outer barriers on a good soil foundation rather than on a concrete or thick asphalt road surface. A soil foundation will create less debris. In addition, a deeper crater will be formed in soil and could function as an anti-vehicle barrier for a second VBIED attack (See Figure 21-6).



Figure 21-6. Crater formed after detonation of a 4,000 lb. TNT equivalent charge

**Barriers at the ECP.** The barrier walls at the entrance to the ECP should be capable of stopping a 30 mph attack from the first vehicle. Barriers should be used to form a serpentine approach to control the speed of entering vehicles to 10 mph or less. For the serpentine approach, use soil filled containers, cabled jersey barriers, cabled concrete blocks, bollards or heavy vehicles.

**Removable anti-vehicle barriers at ECP entrances.** These barriers should be capable of being moved to provide access for JCOP vehicles and, when needed, emergency vehicles. They should be capable of being removed in a timely fashion. Removable bollards are a good solution. Heavy vehicles in all sizes and configurations should be considered as expedient barriers. Large construction-type vehicles or armored vehicles (including destroyed and captured enemy vehicles) can be very effective or as barriers for the serpentine in ECPs. Crash beam gates or cabled gates can be used if the ECP entrance is designed so that approaching vehicles must slow to 10 mph or less to enter.

**Antipersonnel barriers.** These barriers should be used to deter and delay attackers on foot from gaining entry to the JCOP. Antipersonnel barriers should be used along the outer and inner perimeter walls and at the entrance to and around the ECP. Install triple-strand concertina, razor wire, etc., along the top and outer base of the outer perimeter wall to prevent attackers from using the low wall as cover/protection during an attack. Antipersonnel barriers should also be installed as a topping for the inner perimeter wall as an anti-climb measure.

A removable antipersonnel barrier should be used in conjunction with the removable anti-vehicle barrier at the ECP entrance and the primary personnel ECP. A staked strand of concertina or razor wire will deter unauthorized personnel from entering the ECPs. At sections of the perimeter where drainage culverts, sewers, and utility openings traverse under or through the perimeter wall, special measures (such as welded wire grids) may need to be installed to reduce the opening sizes to less than 96 square inches with the smallest dimension being less than 6 inches.

### **Entry Control Points**

The JCOP entry control point (ECP) will normally be much smaller in scale than for a large FOB. Despite the smaller scale the ECP must still provide the same functions in order to facilitate access control and enhance the layered defense-in-depth concept. The entrance to the ECP should only be manned when vehicles/personnel must enter or exit the ECP. This can be accomplished through the use of a combination of removable anti-vehicle and antipersonnel barriers (See Figure 21-7).

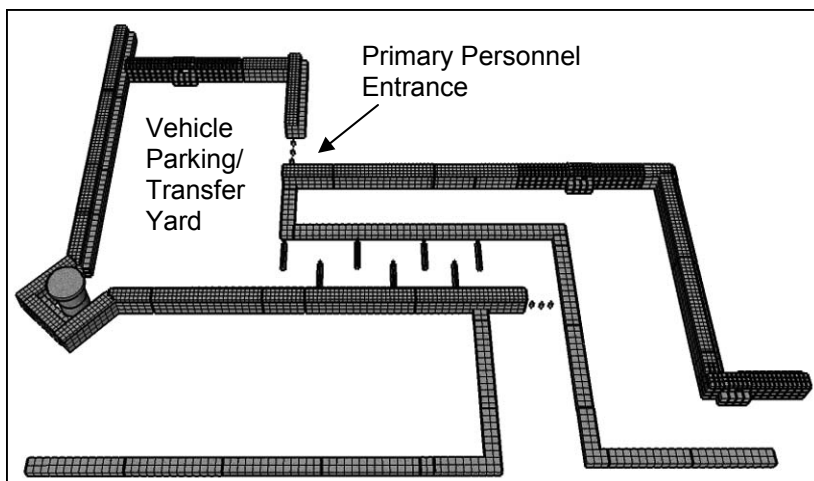


Figure 21-7. JCOP Entry Control Point Concept

The ECP entrance should be designed to stop a 30 mph vehicle attack. In order to reduce the speed of incoming vehicles; the recommended method is to design the ECP entrance so that entering vehicles must negotiate a 90 degree turn from the external roadway, a turn that forces entering vehicles to slow down to 10 mph or less. Additionally, the entry should be constructed as a single lane that requires entering vehicles to slow down to negotiate. Use adequate vehicle speed management/reduction measures consisting of anti-vehicular barriers in a serpentine layout to lower the speed of vehicles to 10 mph or less (Refer to Chapter 13 for speed management techniques).

The JCOP ECP provides the first opportunity for early warning to identify potential threat personnel/vehicles. In order to allow time for assessing and reacting to a threat; the ECP and serpentine layout should be extended to a length that allows adequate time for security personnel to assess/engage a threat. The JCOP ECP should also provide adequate stacking distance for vehicles waiting for entry. It should also allow for verification of authorized access of personnel and vehicles; and allow access to only authorized personnel and vehicles through the use of removable anti-personnel and anti-vehicle barriers (Refer to Chapter 12). Screening from observation and line-of-sight denies an adversary easy targets or collection of information for an attack. Conversely, continuous monitoring and observation by security force personnel allows the entire ECP to be covered by fires from guard towers/overwatch (Refer to Chapter 13).

The entrance to the JCOP ECP should be considered an approach and access control zone. The entire ECP should be considered a response and

safety zone. When selecting the site for a JCOP ECP the following concepts should be considered:

- Capability of the surrounding road network to tie-in to the ECP, including its capacity to handle vehicles waiting to enter the ECP
- Space to allow unauthorized vehicles that attempt to enter the ECP to be redirected
- Capability to reduce, minimize and control perpendicular and straight-line high speed avenues of approach
- Capability to maximize standoff requirements
- Space for creating an adequate serpentine access lane through the ECP
- Space for creating a vehicle parking/transfer yard
- Capability of guard towers/overwatch to continuously observe and cover the ECP with fires
- Capability to incorporate natural barriers, if available

**Vehicle Parking/Transfer Yard.** The recommended access control measure for vehicles is for all vehicles to remain in a vehicle parking/transfer yard located between the outer perimeter wall and the inner perimeter wall (Refer to Figure 21-7). A vehicle parking/transfer yard can allow for JCOP personnel to maintain positive control of their vehicles at all times while keeping the potential threat of VBIEDs outside the interior of the JCOP. Like perimeter barriers and the ECPs, the vehicle parking/transfer yard should be continuously monitored and kept under observation by security force personnel. The design of the vehicle parking/transfer yard should allow for the entire area to be covered by fires from guard towers/overwatch.

A properly designed vehicle parking/transfer yard should provide protection for vehicles and for personnel as they exit their vehicle and enter into the interior of the JCOP through the primary personnel ECP. Examples of measures used to protect personnel and vehicles include the use of taller barriers for the outer wall of the perimeter surrounding the vehicle parking/transfer yard or the use of obscuration and screening materials. Like the ECP, the vehicle parking/transfer yard should be shielded from observation to prevent attackers from identifying targets and patterns of predictability.

**Vehicle Search Area.** If needed, the vehicle parking/transfer yard can be used as a search area for vehicles that must enter into the interior of the JCOP; it is recommended that each vehicle (100%) undergo a thorough search for explosives/IEDs before entering the interior of the JCOP. If this is required, then specific policies and procedures should be established for each JCOP that detail vehicle search procedures/requirements. The design-



nated search area should be a separate and distinct area of the vehicle parking/transfer yard and at a distance that provides acceptable standoff. The area should be capable of handling larger vehicles and should include blast mitigation measures (berms or soil-filled bins/walls) that can protect JCOP personnel should a bomb-laden vehicle explode while being searched. The search area should also include obscuration and screening measures that obstruct observation of the search area from outside the JCOP.

**Primary Personnel ECP.** The primary personnel ECP should be a combination of a personnel gate and the final denial barrier for the JCOP. Located adjacent the vehicle parking/transfer yard (Refer to Figure 21-7), the primary personnel ECP should be capable of denying access to both vehicles and personnel. As a personnel gate, the ECP should be designed to permit only one person to approach and enter at any time and designed with limited obstructions to ensure that security personnel can maintain visual contact with personnel as they approach the ECP. Examples of materials to use to limit personnel access include removable antipersonnel barriers such as single strands of concertina or razor wire or a single swing chain link gate.

As a final denial barrier, the primary personnel ECP should be designed to protect against a ramming VBIED attack. Examples of materials to use can be found in the earlier discussion on anti-vehicular barriers. Additional anti-vehicular barriers can be installed behind the ECP to provide defense-in-depth against a VBIED attack. If the decision is made that vehicles must enter into the interior of the JCOP then removable anti-vehicular barriers (see earlier discussion) should be used. A fighting position should also be constructed at the primary personnel ECP, one that can be used by security force personnel to cover security force members that are conducting access control operations or moving antipersonnel/anti-vehicular barriers and to repel an attack.

## Construction Sequence

Personnel and assets should be provided an appropriate level of protection for each of the threat tactics identified for the JCOP. These include small arms, RPGs, Rockets, Mortars, PBIEDs and VBIEDs. There are numerous construction concepts for achieving protection against these tactics. The best concept must be determined on a case-by-case basis using information on available concepts presented in this handbook. Multiple concepts can be used against some tactics to increase the protection level, particularly within an integrated, layered, defense-in-depth plan. Some concepts provide protection against multiple tactics.

The ultimate goal is to construct a perimeter system and internal components that will provide protection from a complex attack using dual VBIEDs, PBIEDs, direct fire and indirect fire weapons. The most significant of these and the one that has the greatest impact on the design of protective elements is the dual VBIED. A design that protects from this threat will generally provide significant baseline protection from the other threats. *NOTE: These wall designs are based on a 4000 lb VBIED. They will work for smaller threats but may not provide the same level of protection for larger threats.*

**Step 1. Construct the Inner High Perimeter Wall.** The recommended wall configuration for a 4000 lb VBIED threat is to have a 3 ft.-3 in. high exterior low wall with a 12 ft. high wall located 35-40 ft. behind it. The exterior low wall defines the perimeter, is capable of stopping a 15,000 lb vehicle at 30 mph, and does not create a significant debris hazard. The inner high wall stops a second vehicle, stops most of the vehicle fragments and does not create hazardous debris. After construction (even without the outer low wall) the high wall will help conceal and shield JCOP activities, provide ballistic protection from small arms and RPGs, protect against PBIEDs and reduce blast and fragment effects from single VBIED attacks. It will also provide fragment protection for mortars and rockets that land outside the perimeter.

Two high wall designs can be used. The first is for the case where a new perimeter wall is being constructed. It consists of set of soil-filled containers that is nominally 12 ft. high and 6- 10 ft. thick (See Figure 21-8).<sup>3</sup> The second is for retrofitting an existing concrete wall to reduce the potential debris hazard. A recommended design using soil-filled containers behind a 10 ft. high concrete wall is shown in Figure 21-8. Place a triple-strand concertina or razor wire antipersonnel barrier along the top of the wall.

**Step 2. Construct the perimeter fighting positions and locations for guard towers.** Fighting positions should be located at several locations along the high perimeter wall. Two options for an “in-wall” position are shown in Figure 21-9. The first is easier to construct while the second provides for more coverage when engaging an enemy. These positions should be planned for and built during initial construction of the perimeter wall rather than trying to modify the wall later. The overhead cover shown

3. Concrete walls do not provide the same fragmentation protection as soil-filled containers. However keep in mind the minor military construction threshold is \$750,000. A T-wall/soil container hybrid wall may provide a structurally sound perimeter without violating minor military construction thresholds. From a cost perspective soil-filled containers are considered “construction” while concrete T-walls are considered “unit property” because they are relocatable and can be used for other purposes. Refer to DA Pamphlet 420-11, *Project Definition and Work Classification*.

will protect from direct hits from small mortars. However, be sure to use the size and spacing of the lumber shown (12-ft. long 4x4's spaced 9-in. on center with  $\frac{3}{4}$ -in. treated or marine grade plywood nailed to the top surface).

Guard towers/posts should be located at each corner so that they have good visibility of the exterior of the perimeter in two directions. Several designs can be used. Figure 21-10 shows one constructed of soil-filled containers and modeled after the large observation post in Annex D. The pre-cast concrete pipe tower concept is discussed in more detail in Chapter 20.

### Step 3. Construct fighting/personnel bunkers inside the perimeter.

Ground level fighting positions and personnel bunkers should be constructed at key locations on the interior of the JCOP to provide fallback locations and for temporary protection if given sufficient warning of a VBIED attack or rocket or mortar attack. See Chapter 20 and Annex D for concepts and construction details.

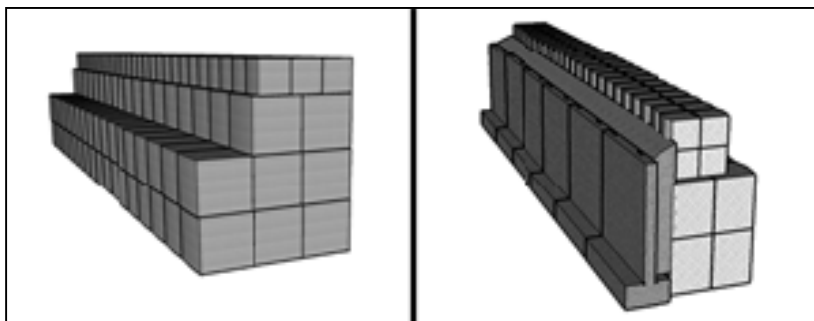


Figure 21-8. Inner Perimeter Wall Construction Concepts  
(Left: Wire and fabric containers; Right: Concrete wall retrofit)

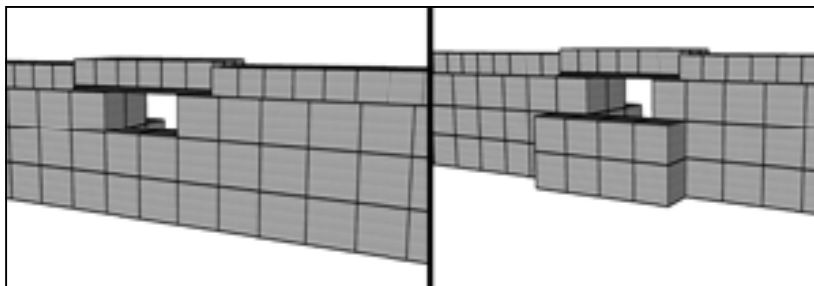


Figure 21-9. Perimeter Fighting Position Concepts  
(Left: Option 1; Right: Option 2)

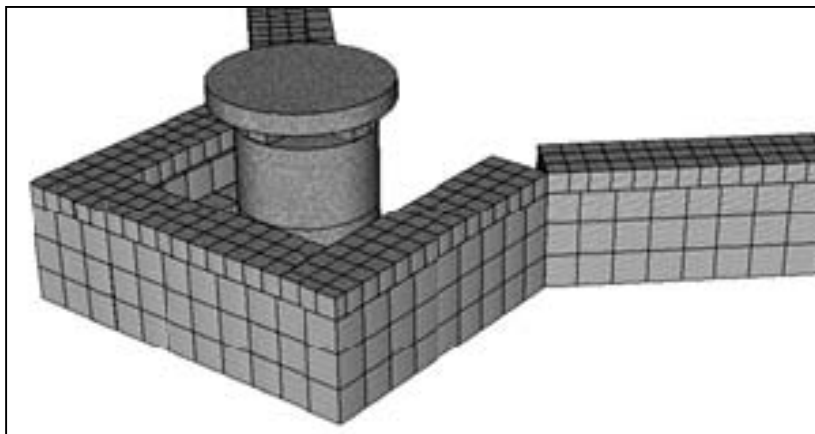


Figure 21-10. Corner construction concept for use with tower.

**Step 4. If sufficient standoff is not available, retrofit or harden existing buildings to increase blast resistance.** Apply protective construction/design measures during the occupation of the JCOP. This includes structural hardening of walls, roofs, floors, and windows to reduce the vulnerability of these structures, thereby making them less inviting targets. At a minimum, structures in which personnel sleep, work, or eat should be hardened as soon as possible. Regardless the type of hardening techniques used large numbers of personnel should not be placed in one structure.

If the existing level of protection in an existing structure is determined to be unacceptable, it may be necessary to retrofit existing buildings to increase their level of protection. However, retrofitting is generally an expensive and time-consuming option, so other courses of action, such as relocating assets, should be explored first. Before proceeding with any retrofits, consult with structural engineers to obtain detailed designs.

**Step 5. Construct observation/fighting positions on roof of buildings.** Depending on the type of structure, fighting positions may be located inside or on the roof of the building (See Figure 21-11). Many roofs are flat and some have parapet walls. Sandbags can be used to provide/increase protection. Be sure to have the floor and roof structure evaluated by an engineer before adding any substantial loads (such as soil filled revetments over 2 feet high).

**Step 6. Construct the outer low outer wall of the perimeter wall system.** These can consist of ditches or low height soil-filled containers. The recommended ditch design is given in Chapter 8. The recommended minimum thickness soil bin shown in Figure 21-12 is at least 3-ft 3-in. high and 6-ft. 6-in. thick.



Figure 21-11. Fighting position constructed on building roof.

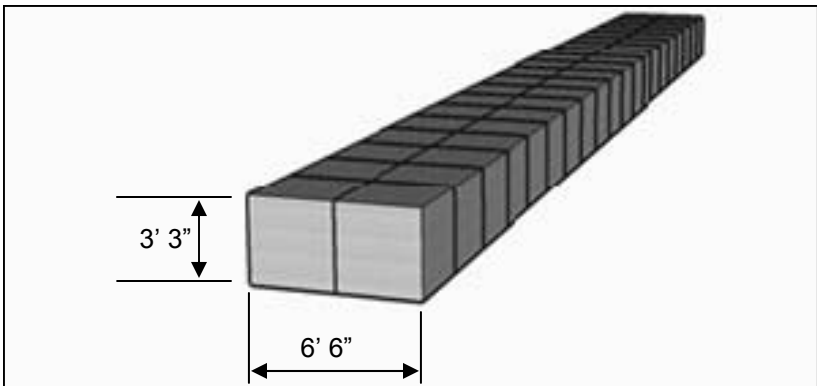


Figure 21-12. Outer Perimeter Wall Construction Concept

This low wall design could also be constructed using soil-filled metal containers (See Appendix D for information on metal soil bin sizes). Since the outer low wall could provide cover for an attacker, place a triple-strand concertina or razor wire antipersonnel barrier along the outer side and top of the wall.

**Step 7. Construct the entry point, vehicle parking/transfer yard and personnel entry.** Barriers at the ECP include a removable barrier at the entrance intended to deny entry by unauthorized vehicles and low barriers that are used to develop the serpentine approach along the entrance. The entrance barrier can be a drop-arm barrier or removable bollards. Since the entrance to the ECP requires a right angle turn, the serpentine approach past the entrance gate need only control vehicles traveling at 10 mph. Therefore the barriers along this approach can be single Jersey barriers or low soil-filled containers.

The barrier between the vehicle parking area and the main JCOP should be similar to the barriers at the entrance to the ECP. This barrier will remain in place except to allow access by emergency vehicles or other special circumstances. The antipersonnel barrier at the ECP vehicle entrance and the primary personnel entrance can be either a single staked strand of concertina or razor wire or a single swing chain link gate (See Chapter 12 for additional details).

**Step 8. Emplace traffic control barriers on surrounding roadways.**

These work in conjunction with the perimeter wall system in providing protection against a VBIED attack. These barriers can be used in the surrounding area outside the JCOP to detour traffic or control approach speeds. Barrier types include soil bins similar to those used for the outer perimeter wall, ditches, berms, and cabled Jersey barriers. Additional details on these types of barriers can be found in Chapter 12 and Annex D

**Step 9. Provide full-height sidewall protection for near miss rocket and mortar threats** (Primarily for tents and other lightweight structures). See Chapter 14 for additional details.

**Step 10. Compartmentalize large area, high occupancy facilities.**

Compartmentalization is intended primarily to limit injuries and fatalities from direct hits of rockets and mortars on large lightweight structures such as tents and metal buildings. For this threat against a reinforced concrete frame building, compartments may not be needed since the incoming rounds would likely detonate on the roof of the building. However, they would perform the same function in any structure faced with a PBIED.

**Step 11. Provide overhead cover incorporating pre-detonation and shielding layers** (Primarily for tents and other lightweight high-occupancy structures).

Overhead protection is intended primarily to limit injuries and fatalities from direct hits of rockets and mortars. For this threat against a reinforced concrete frame building, only a pre-detonation layer would be needed since the roof slab would stop most fragmentation. If the top floor of the building is not occupied, no additional overhead protection would be needed since the roof would detonate the incoming round and the next floor slab would stop the fragments.

**Step 12. Provide bunkers for critical equipment.** If there is a more likely attack direction, placing critical equipment on the opposite side of the JCOP building may help shield it from some of the blast and fragmentation effects.

## Performance Issues

The JCOP double wall configuration shown in Figure 21-3 was tested<sup>4</sup> against the effects of two successive 4000 lb (TNT equivalent) VBIEDs in dump trucks. Several perimeter wall designs were constructed and evaluated for their performance in maintaining a capability for stopping the second dump truck, protecting the JCOP interior from dump truck fragments and not creating hazardous wall debris.

The high wall design shown in Figure 21-8 is a retrofit for existing modular concrete wall perimeters. It significantly reduced the debris from these walls. Figure 21-13 shows the limited debris behind the wall; most was sand used to fill the soil bins.

The high wall design shown in Figure 21-8 uses soil-filled wire and fabric containers. It stopped the fragments from the vehicle and did not create any hazardous debris. It also survived at the edge of the blast crater (see Figure 21-14) maintaining its capability for stopping a second vehicle attempting to go around the crater.

The low wall design shown in Figure 21-12 uses soil-filled wire and fabric containers. It survived at the edge of the crater (see Figure 21-14) and maintained its capability for stopping a second vehicle attempting to go around the crater.

The configuration for the second detonation was a test of the inner soil-filled container wall (Shown in Figure 21-12) damaged from a previous explosion. This wall successfully stopped the hazardous fragments from the engine and frame and maintained its capability for stopping any addition vehicles trying to gain entry to the JCOP interior (See Figure 21-15).



Figure 21-13. Post explosion photo of debris behind concrete retrofit wall

4. Army Test and Evaluation Command and the Engineer Research and Development Center conducted tests at Eglin AFB on 28-30 July 2008.



Figure 21-14. Post-explosion photos.  
(Above: High soil bin wall; Below: Low soil bin wall)



Figure 21-15. Second explosion test of inner wall (Left: Before; Right: After)



## Appendix A

# Abbreviations and Acronyms

The following numbers, when preceded by the appropriate echelon (C = Coalition Staff; J = Joint Staff; G = General Staff; S = Battalion or Brigade Staff) refer to formal staff sections of a command:

-1	Manpower and Personnel
-2	Intelligence
-3	Operations
-4	Logistics
-5	Plans
-6	Communications and Computer Systems
-7	Engineering
-8	Force Structure, Resource, and Assessment
-9	Civil-Military Operations

AC	Alternating Current
ADC	Area Damage Control
AF	Air Force
AFDD	Air Force Doctrine Document
AFH	Air Force Handbook
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFPD	Air Force Policy Directive
AFTTP	Air Force Tactics, Techniques, and Procedures
ALO	Air Liaison Officer
AO	Area of Operation
AOC	Area Operations Center
AOR	Area of Responsibility
APOD	Aerial Port of Debarkation
AR	Army Regulation
ASAS	All-Source Analysis Software
ASG	Area Support Group
ASOC	Air Support Operations Center
AT	Antiterrorism
ATEP	Antiterrorism Enterprise Portal
ATO	Antiterrorism Officer
ATSC	Army Training Support Center
AVS	Automated Video Surveillance
AWS	Alert Warning System

BCOC	Base Cluster Operations Center
BDOC	Base Defense Operations Center
BICADS	Building Injury Calculator And Database S
BOS	Base Operating Support
C2	Command and Control
CALL	Center for Army Lessons Learned
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognizability
CBR	Chemical, Biological, and Radiological
CBRN	Chemical, Biological, Radiological, and Nuclear
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives
CbT-RIF	Combating Terrorism Readiness Initiative Fund
CCD	Camouflage, Concealment, and Deception
CCDR	Combatant Commander
CCIF	Combatant Commander's Initiative Fund
CCIR	Commanders Critical Information Requirement
CCTV	Closed Circuit Television
CD	Compact Disc
CERP	Commander's Emergency Response Program
CFLCC	Combined Force Land Component Command
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJCSM	Chairman, Joint Chiefs of Staff Manual
CJTF	Combined Joint Task Force
CM	Consequence Management
(or cm)	Centimeter (unit of measurement)
CMU	Concrete Masonry Unit
COA	Course of Action
COCOM	Combatant Command
COIN	Counterinsurgency
COM	Chief of Mission
COMSEC	Communications Security
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
CRREL	Cold Regions Research and Engineering Lab
CVAMP	Core Vulnerability Assessment Management Program

DA	Department of the Army
DA PAM	Department of the Army Pamphlet
DARPA	Defense Advanced Research Projects Agency
DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DoD	Department of Defense
DON	Department of the Navy
DONCIP	Department of the Navy Critical Infrastructure Protection
DPW	Director of Public Works
DSN	Defense Switched Network
DTRA	Defense Threat Reduction Agency
ECP	Entry Control Point
ECR	Effective Casualty Radius
EDD	Explosive Detector Dog
EOD	Explosive Ordnance Disposal
EOF	Escalation of Force
EPW	Enemy Prisoner of War
ERDC	U.S. Army Engineer Research and Development Center
ESS	Electronic Surveillance System
FC (or fc)	Foot-Candles (unit of measurement)
FHP	Force Health Protection
FM	Field Manual
FOB	Forward Operations Base
FP	Force Protection
FPCON	Force Protection Condition
FPL	Final Protective Line
FPTAS	Flight Path Threat Analysis Simulation
FPWG	Force Protection Working Group
FRAGO	Fragmentary Order
FSCoord	Fire Support Coordinator
FT (or ft)	Feet (unit of measurement)
GCC	Geographic Combatant Commander
GPS	Global Positioning System
GPTO	General Purpose Tape Obstacle

GSA	General Services Administration
GWOT	Global War on Terror
HAZMAT	Hazardous Material
HMMWV	High-Mobility Multipurpose Wheeled Vehicle
HN	Host Nation
HPAC	Hazard Prediction and Assessment Capability
HPS	High Pressure Sodium
HQ	Headquarters
HSS	Health Service Support
HUMINT	Human Intelligence
HVAC	Heating, Ventilation, and Air Conditioning
HVT	High Value Target
IAW	In Accordance With
IBE	Installed Building Equipment
ICP	Incident Command Post
ID	Identification
IDS	Intrusion Detection System
IED	Improvised Explosive Devices
IN (or in)	Inch (unit of measurement)
INFOSEC	Information Security
IR	Incident Response
IRAM	Improvised Rocket Assisted Mortar
ISO	International Standards Organization
JAT Guide	Joint Antiterrorism Program Manager's Guide
JCEOI	Joint Communications Electronic Operating Instructions
JCOP	Joint Combat Outpost
JCS	Joint Chiefs of Staff
JFC	Joint Force Commander
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFOB	Joint Forward Operations Base
JIEDDO	Joint Improvised Explosive Device Defeat Organization
JMC	Joint Movement Center
JOC	Joint Operations Center
JOPP	Joint Operation Planning Process

JP	Joint Publication
JSA	Joint Security Area
JSC	Joint Security Coordinator
JSCC	Joint Security Coordination Center
JSD	Joint Security Directorate
JSIVA	Joint Service Integrated Vulnerability Assessment
JSS	Joint Security Station
JTF	Joint Task Force

KG (or kg)      Kilogram (unit of measurement)

LB (or lb)	Pound (unit of measurement)
LN	Local National
LOC	Lines Of Communications
LOP	Levels Of Protection
LVB	Large Vehicle Bomb

M (or m)	Meter (unit of measurement)
MANPADS	Man-Portable Air Defense System
MASCAL	Mass Casualty
MCAP	Mine Clearing/Armor Protection
MCO	Marine Corps Order
MCRP	Marine Corps Reference Publication
MEDEVAC	Medical Evacuation
METL	Mission Essential Task Lists
METT-T	Mission, Enemy, Terrain and Weather, Troops Available and Time
METT-TC	Mission, Enemy, Terrain and Weather, Troops Available, Time, and Civil Considerations
MEVA	Mission Essential Vulnerable Asset
MM (or mm)	Millimeter (unit of measurement)
MP	Military Police
MPS	Modular Protective System
MSHARPP	Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
MVACIS	Mobile Vehicle and Cargo Inspection System
MWD	Military Working Dog
MWR	Moral, Welfare, and Recreation

NIPRNET	Non-Classified Internet Protocol Router Network
NSN	National Stock Number
NTTP	Navy Tactics, Techniques, and Procedures
O&M	Operations and Maintenance
OIF	Operation Iraqi Freedom
OP	Observation Post
OPCON	Operational Control
OPLAN	Operations Plan
OPNAVINIST	Chief of Naval Operations Instruction
OPORD	Operations Order
OPSEC	Operations Security
ORM	Operational Risk Management
PBIED	Personnel-Borne Improvised Explosive Device
PDC	Protective Design Center
PDF	Principal Direction of Fire
POL	Petroleum, Oils, and Lubricants
PPE	Personal Protective Equipment
PSA	Pressure Sensitive Adhesive
PSEAG	(DoD) Physical Security Equipment Action Group
PVAB	Portable Vehicle Arresting Barrier
PVNTMED	Preventive Medicine Program
QRF	Quick Reaction Force
QRT	Quick Reaction Test
RAC	Risk Assessment Code
RAM	Rockets, Artillery, and Mortars; Random Antiterrorism Measures
RAMP	Return fire, Anticipate attack, Measure, and Protect
RAOC	Rear Area Operations Center
ROE	Rules Of Engagement
ROWPU	Reverse Osmosis Water Purification Unit
RPG	Rocket Propelled Grenade
RRR	Reduce, Recycle, Reuse

RSOI	Reception, Staging, Onward movement, and Integration
RV	Recreational Vehicle
SA	Situational Awareness
SAM	Surface to Air Missile
SCBA	Self-Contained Breathing Apparatus
SF	Security Force
SIPRNET	Secret Internet Protocol Router Network
SLAM	
SLUDGEM	Salivation, Lacrimation, Urination, Defecation, Gastro-intestinal Distress, Emesis, Miosis
SOC	Special Operations Command
SOP	Standard Operating Procedure; Standing Operating Procedure
SPL	Sound Pressure Level
SPOD	Sea Port of Debarkation
STDTT	Security Technology Decision Tree Tool
STX	Situational Training Exercise
SUV	Sport Utility Vehicle
SWEAT	Sewer, Water, Electricity, Academics, Trash
SWEAT-MSO	Sewer, Water, Electricity, Academics, Trash, Medical, Safety, and Other considerations
TC	Training Circular
T&E	Traversing and Elevation
TACON	Tactical Control
TCF	Tactical Combat Force
TCMS	Theater Construction Management System
TCP	Traffic Control Points
TM	Technical Manual
TOC	Tactical Operations Center
TRADOC	(Army) Training and Doctrine Command
TTP	Tactics, Techniques, and Procedures
UFC	Unified Facilities Criteria
UGS	Unattended Ground Sensors
UPS	Uninterrupted Power Supply
US, U.S.	United States

USACE	US Army Corps of Engineers
USAF	US Air Force
USCENTCOM	US Central Command (also referred to as CENTCOM)
USTRANSCOM	US Transportation Command
UXO	Unexploded Ordinance

VBIED	Vehicle-Borne Improvised Explosive Devices
VLAD	Vehicle Light Arresting Device

WMD	Weapons of Mass Destruction
WVAT	Weather Vulnerability Assessment Tool





## Appendix B

# Force Protection Conditions

Force Protection Conditions (FPCONs) describe the progressive level of countermeasures in response to a terrorist threat to US military facilities and personnel as directed by DOD Directive 2000.12, *DOD Antiterrorism (AT) Program*. These security measures are approved by the Joint Chiefs of Staff and are designed to facilitate inter-Service coordination and support of US military AT activities. They are outlined in DOD O-2000.12-H, *DOD Antiterrorism Handbook*, Appendix 3, DOD FPCON System.<sup>1</sup> When installations adapt these measures for their site-specific circumstances, they should account for, as a minimum, combatant commander/Service requirements, local laws, and status of forces agreements. According to DOD Instruction 2000.16, *DOD Antiterrorism Standards*, FPCON measures are FOR OFFICIAL USE ONLY. An AT plan with a complete listing of site-specific AT measures, linked to an FPCON, shall be classified, as a minimum, CONFIDENTIAL. When separated from the AT plan, specific measures and FPCON measures remain FOR OFFICIAL USE ONLY.<sup>2</sup>

The FPCON system is the principal means through which a military commander or DOD civilian exercising equivalent authority applies an operational decision on how to best guard against the threat. These guidelines assist commanders in reducing the effect of terrorist and other security threats to DOD units and activities.

Creating additional duties and/or watches and heightening security enhance the command's personnel awareness and alert posture. These measures display the command's resolve to prepare for and counter the terrorist threat. These actions convey to anyone observing the command's activities that it is prepared and an undesirable target, and that the terrorist(s) should look elsewhere for a vulnerable target.

The DOD system is generally not applicable to DOD elements for which the Chief of Mission (COM) has security responsibility, and may have limited application to DOD elements that are tenants on installations and facilities not controlled by US military commanders or DOD civilian exercising equivalent authority. Still, commanders of US elements on non-US

---

1. Current FPCON supporting measures as of 2 October 2006 are listed in Enclosure 4 of DoD Instruction 2000.16.

2. See paragraph E3.22.3.2, DoD Instruction 2000.16, p. 27.

installations can execute many FPCON measures that do not involve installation level actions, at least to a limited degree. The terminology, definitions, and specific recommended security measures are designed to facilitate inter-Service coordination and support for the combating terrorism efforts of the DOD components.

There are five FPCONs. Supporting measures for each condition are listed in Appendix 3 of DOD O-2000.12-H. The circumstances that apply and the purposes of each protective posture are as follows:

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

**FPCON ALPHA** applies when there is an increased general threat of possible terrorist activity against personnel or facilities, the nature and extent are unpredictable. ALPHA measures must be capable of being maintained indefinitely.

**FPCON BRAVO** applies when an increased or more predictable threat of terrorist activity exists. Sustaining BRAVO measures for a prolonged period may affect operational capability and relations with local authorities.

**FPCON CHARLIE** 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.

**FPCON DELTA** applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location or person is imminent. Normally, this FPCON is declared as a localized condition. FPCON DELTA measures are not intended to be sustained for substantial periods.

Geographic combatant commanders shall ensure that FPCONs are uniformly implemented and disseminated within their AOR. All military commanders and DOD civilians exercising equivalent authority are responsible for ensuring that their subordinates fully understand FPCON declaration procedures and FPCON measures. While there is no direct correlation between threat reporting and FPCONs, such information assists commanders in making prudent FPCON declarations. Existence of threat reporting in and of itself should not be the only factor used in determining FPCONs. FPCON declaration should be based on multiple factors that may include, but are not limited to, threat, target vulnerability, criticality

of assets, security resource availability, operational and physiological impact, damage control, recovery procedures, international relations, and planned US Government actions that could trigger a terrorist response.

The FPCON system allows all military commanders and DOD civilians exercising equivalent authority the flexibility and adaptability to develop and implement AT measures that are more stringent than those mandated by higher authorities whenever FPCONs are invoked. Each set of FPCON measures is the minimum that must be implemented when a change in local threat warrants a change in FPCON or when higher authority directs an increase in FPCON. Authorities directing implementation may augment their FPCON by adding measures from higher FPCONs as necessary.

Military commanders or DOD civilians exercising equivalent authority may implement additional FPCON measures from higher FPCONs on their own authority, develop additional measures specifically tailored for site-specific security concerns, or declare a higher FPCON for their operational area/installation.

Subordinate military commanders or DOD civilians exercising equivalent authority at any level may not lower an FPCON or implement measures that are less rigorous than those appropriate for the declared FPCON. Waivers for not complying with prescribed FPCON measures may be obtained by following the procedures in Appendix H of Joint Publication 3-07.2, *Antiterrorism*.

It is essential for military commanders and DOD civilians exercising equivalent authority to implement formal analytical processes that result in a set of operational area or locality-specific terrorist threat indicators and warnings for use when transitioning from lower to higher FPCONs. Threat credibility, and if known, duration, operational environment (both host nation and DOD), asset criticality, mission impact and measures in place that contribute to mitigating the current threat are but a few of the important elements commanders should consider when calibrating FPCON postures. Such processes and measures should be harmonized to the maximum degree possible, taking fully into account differences in threat, vulnerability, criticality, and risk of resources requiring protection.

Military commanders, DOD civilians exercising equivalent authority, and their staffs shall examine the threat, physical security, terrorist attack consequences, and mission vulnerabilities in the context of specific DOD activities and the declared FPCON. When factors are combined and the collective terrorist threat exceeds the ability of the current physical security system (barriers, surveillance and detection systems, security personnel,

and dedicated response forces) to provide the level of asset protection required, then implementation of higher FPCONs or additional measures is appropriate.

Once an FPCON is declared, all listed security measures are implemented immediately unless waived by competent authority as described above. The declared FPCON should also be supplemented by a system of RAMs in order to complicate a terrorist group's operational planning and targeting. Specific measures for each FPCON are listed in DOD O-2000.12-H, Appendix 3. Several factors influence specific countermeasures:

1. Ability to maintain highest state of operational readiness.
2. Measures to improve physical security through the use of duty and guard force personnel limit access to the exposed perimeter areas and interior of the unit/facility by hostile persons, and barriers to physically protect the unit/facility.
3. Availability of effective command, control, and communication systems with emphasis on supporting duty/watch officers, security personnel, and key personnel.
4. An AT awareness program for all personnel.
5. Protection of high-risk assets and personnel.
6. Measures necessary to limit activities, and visitor/social engagements.

FPCON NORMAL and all FPCON levels should include site specific measures a facility commander deems necessary when establishing a baseline posture.

Implementation of FPCONs does not come without adverse effects on day-to-day operations; the additional costs can be measured and described both quantitatively and qualitatively. The DOD FPCON system acknowledges cost as a significant factor bearing on the selection and maintenance of FPCONs. FPCONs ALPHA and BRAVO include measures that can be sustained for extended periods, consistent with the terrorist threat.

## **Appendix C**

# **Materiel Support**

### **Introduction**

This appendix contains listings and pictures of construction and equipment products available from the Defense Logistics Agency (DLA) to assist in planning for protective construction and security missions. TTPs for use of the materials presented here are detailed elsewhere in the JFOB Handbook. Contents of this appendix include fielded systems with National Stock Numbers (NSNs) and systems that were obtained through DoD Operational Needs Statements. These materials are being used in training at the Combined Training Centers. Additional material and technologies listed in this book that are not in the DLA system will have contact information listed with them to assist planners. Stock numbers, cost data, and product availability are valid as of December 2008. This appendix is not exhaustive, as other related items may be available through supply channels. This data is subject to change. Contact DLA ([www.dla.mil](http://www.dla.mil)) for additional information.

## Annex C-1

## Soil-Filled Containers

Soil-filled containers have many applications. Kit dimensions and NSN data for the most common wire and fabric containers are shown in Table C-1. Kit dimensions and NSN data for the most common metal containers are shown in Table C-2. Refer to Appendix D for construction guidelines and additional applications for these containers.

**Perimeter Wall Dimension Calculations.** Figure C-1 illustrates an occupied structure in the center of a proposed perimeter. Simple equations are used to calculate the interior wall length (IWL) and the outer wall length (OWL) when the approximate building dimensions are known. The following variables are used in the perimeter calculations:

- $L_1$  and  $L_2$  – Approximate lengths of two sides of the billeting
- $R_{inner}$  – Standoff should be greater than or equal to 115 feet from the face of the occupied structure

Table C-1. Wire and Fabric Container Kit Dimensions

Height (ft)	Width (ft)	Length (ft)	NSN 5680-99-	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
4.5	3.5	32.0	Beige color: 835-7866 Green color: 001-9396	\$27.67	\$885.34
2.0	2.0	4.0	Beige color: 968-1764 Green color: 001-9397	\$16.33	\$65.30
3.25	3.25	32.0	Beige color: 001-9392 Green color: 001-9398	\$21.03	\$673.08
3.25	5.0	32.0	Beige color: 001-9393 Green color: 001-9399	\$31.41	\$1,005.08
2.0	2.0	10.0	Beige color: 001-9394 Green color: 001-9400	\$13.42	\$134.24
7.25	7.0	90.0	Beige color: 169-0183 Green color: 126-3716	\$53.12	\$4,780.45
4.5	4.0	32.0	Beige color: 335-4902 Green color: 517-3281	\$28.06	\$898.04
3.25	2.5	30.0	Beige color: 563-5949 Green color: 052-0506	\$20.26	\$607.76
7.0	5.0	95.0	Beige color: 391-0852 Green color: 770-0326	\$52.63	\$4,999.96

1. Approximate cost for each linear foot, based on kit cost and length

2. NSN cost data as of 1 December 2008 and subject to change

Contact Defense Logistics Agency ([www.dla.mil](http://www.dla.mil)) for further information.

- **R<sub>Outer</sub>** – Standoff should be greater than or equal to 150 feet from the face of the occupied structure
- **IWL<sub>1</sub>** – Interior Wall Length running parallel to length **L<sub>1</sub>**
- **IWL<sub>2</sub>** – Interior Wall Length running parallel to length **L<sub>2</sub>**
- **OWL<sub>1</sub>** – Outer Wall Length running parallel to length **L<sub>1</sub>**
- **OWL<sub>2</sub>** – Outer Wall Length running parallel to length **L<sub>2</sub>**

Table C-2. Metal Container Kit Dimensions

Height (ft)	Width (ft)	Length (ft)	NSN	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
6	3	104	5450-01-554-1249	\$60.65	\$6,307.94
6	4	96	5450-01-554-1238	\$92.42	\$8,872.42
6	5	88	5450-01-554-1240	\$77.98	\$6,862.09
8	5	64	5450-01-554-1253	\$103.97	\$6,654.31
10	5	48	5450-01-554-1256	\$129.96	\$6,238.13
6	6	80	5450-01-554-1267	\$86.64	\$6,931.39
8	6	64	5450-01-554-1303	\$115.53	\$7,393.68
10	6	48	5450-01-554-1309	\$144.40	\$6,931.39
12	6	48	5450-01-554-1315	\$173.29	\$8,317.89
6	7	72	5450-01-554-1331	\$95.31	\$6,862.40
8	7	48	5450-01-554-1336	\$127.08	\$6,099.79
10	7	32	5450-01-554-1341	\$192.12	\$6,147.84
12	7	32	5450-01-554-1351	\$190.61	\$6,099.66
16	7	24	5450-01-554-1358	\$254.15	\$6,099.66
6	8	72	5450-01-554-1377	\$103.97	\$7,486.10
8	8	48	5450-01-554-1382	\$138.63	\$6,654.31
10	8	40	5450-01-554-1392	\$173.29	\$6,931.58
12	8	32	5450-01-554-1398	\$207.94	\$6,654.15
16	8	24	5450-01-554-1401	\$277.26	\$6,654.12
10	4	48	5450-01-537-7061	\$159.80	\$7,670.25
8	4	64	5450-01-535-7952	\$123.23	\$7,886.59
6	2	104	5450-01-535-7955	\$68.85	\$7,160.58

1. Approximate cost for each linear foot, based on kit cost and length
2. NSN cost data as of 1 December 2008 and subject to change  
Contact Defense Logistics Agency ([www.dla.mil](http://www.dla.mil)) for further information

To calculate the length of perimeter wall follow these steps:

1. Measure the lengths of two adjacent walls of the occupied building ( $L_1$  and  $L_2$ ).
2. The total Outer Wall Length can be calculated by adding 800 feet to  $L_1$  and  $L_2$ . **The total OUTER WALL perimeter length needed =  $L_1 + L_2 + 800$ .**
3. The total Inner Wall Length can be calculated by adding 635 feet to  $L_1$  and  $L_2$ . **The total INNER WALL perimeter length needed =  $L_1 + L_2 + 615$ .**

These totals can be used in procuring the approximate amount of materials needed to defend a JCOP or other structure requiring standoff protection. The distances in the calculations are used to attain standoff for maximum protection from a VBIED attack. Refer to Chapter 11 for standoff guidelines.

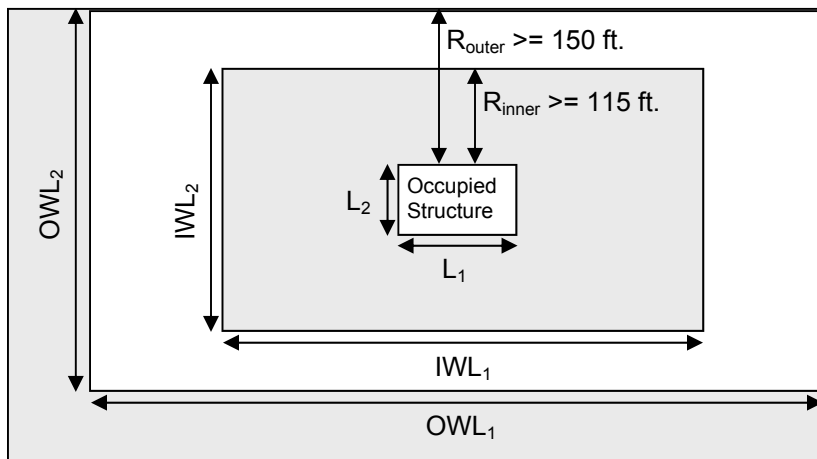


Figure C-1. Perimeter Wall Length Calculations ( $L_1$ = length 1 of structure;  $L_2$ = length 2 of structure;  $R_{inner}$ = standoff from structure face to inner perimeter wall;  $R_{outer}$ = standoff from structure face to outer perimeter wall)

**Soil-Filled Wire and Fabric Container Perimeter Wall.** This wall (See Figure C-2) is 3.5 ft thick at bottom (2 ft thick at top) x 6.5 ft tall. No additional wall stiffeners are required to prevent toppling from close-in detonations. This is a result of the thicker wall base created by the 4.5 ft x 3.5 ft x 32 ft units. Material requirements are shown in Table C-3.

**Low Soil-Filled Wire and Fabric Perimeter Wall.** This low height wall (See Figure C-3) is constructed using two rows, one unit high of 3.25 ft x 3.25 ft x 32 ft containers. Each 32 ft unit requires approximately 16 cubic yards of infill material. Material requirements are shown in Table C-4.





Figure C-2. Example of a perimeter wall using soil-filled wire and fabric containers

Table C-3. Wire/Fabric Container Perimeter Wall Requirements

Height (ft)	Width (ft)	Length (ft)	NSN 5680-99-	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
4.5	3.5	32.0	Beige color: 835-7866 Green color: 001-9396	\$27.67	\$885.34
2.0	2.0	4.0	Beige color: 968-1764 Green color: 001-9397	\$16.33	\$65.30
<b>Materials Required:</b> One 3.25 ft x 3.25 ft x 32 ft unit; Eight 2 ft x 2 ft x 4 ft units, and approximately 32 cubic yards of infill material for each 32 linear feet of perimeter wall.					
1. Approximate cost for each linear foot, based on kit cost and length 2. NSN cost data as of 1 December 2008 and subject to change Contact Defense Logistics Agency ( <a href="http://www.dla.mil">www.dla.mil</a> ) for further information.					

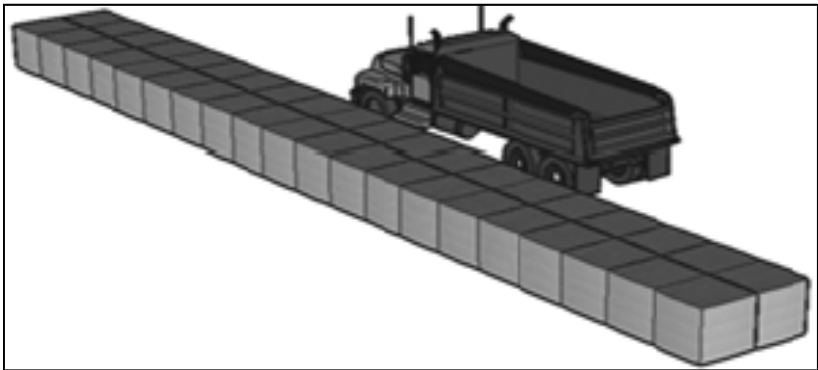


Figure C-3. Low soil-filled wire and fabric container perimeter wall concept

Table C-4. Wire/Fabric Container Low Wall Requirements

Height (ft)	Width (ft)	Length (ft)	NSN 5680-99-	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
3.25	3.25	32.0	Beige color: 001-9392 Green color: 001-9398	\$21.03	\$673.08
<b>Materials Required:</b> Two units and approximately 32 cubic yards of infill material for each 32 linear feet of perimeter wall.					
1. Approximate cost for each linear foot, based on kit cost and length 2. NSN cost data as of 1 December 2008 and subject to change Contact Defense Logistics Agency ( <a href="http://www.dla.mil">www.dla.mil</a> ) for further information.					

**High Soil-Filled Wire and Fabric Perimeter Wall.** This high height wall (See Figure C-4) is constructed using two rows, three units high of 3.25 ft x 3.25 ft x 32 ft containers; plus one row, two units high of 2 ft x 2 ft x 4 ft containers. Each 32 ft unit requires approximately 143 cubic yards of infill material. Material requirements are shown in Table C-5.

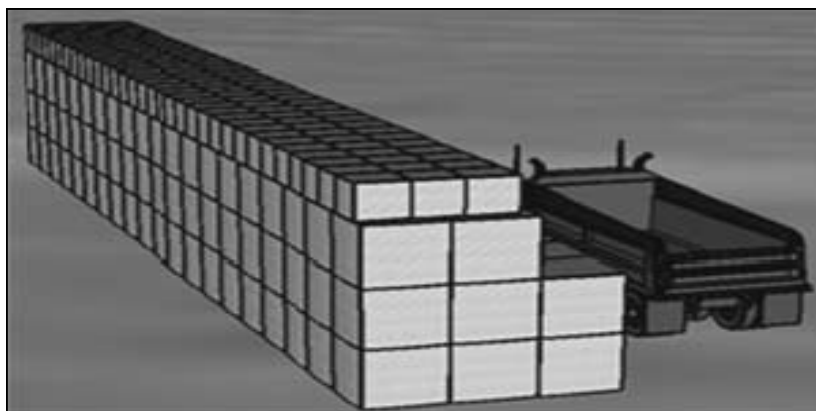


Figure C-4. High soil-filled wire and fabric container perimeter wall concept

Table C-5. Wire/Fabric Container High Wall Requirements

Height (ft)	Width (ft)	Length (ft)	NSN 5680-99-	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
2.0	2.0	4.0	Beige color: 968-1764 Green color: 001-9397	\$16.33	\$65.30
3.25	3.25	32.0	Beige color: 001-9392 Green color: 001-9398	\$21.03	\$673.08
<b>Materials Required:</b> Twenty-four 2 ft x 2 ft x 4 ft units; Eight 3.25 ft x 3.25 ft x 32 ft units and approximately 143 cubic yards of infill material for each 32 linear feet of perimeter wall.					
1. Approximate cost for each linear foot, based on kit cost and length 2. NSN cost data as of 1 December 2008 and subject to change Contact Defense Logistics Agency ( <a href="http://www.dla.mil">www.dla.mil</a> ) for further information.					

**Soil-Filled Metal Container Perimeter Wall.** U.S Army Engineer Research and Development Center (ERDC) in response to a request from US Central Command (CENTCOM) was tasked to develop an alternative to soil-filled geotextile revetments. This request was based on longevity issues related to the soil-filled geotextile revetments exposed to severe environmental conditions. The design was based on the existing Air Force Technology on corrugated metal revetments, Type B-1. The new (ERDC) design takes into account reduced footprint to meet base camp logistical requirements and weapons threats seen in theater.

**Low Soil-Filled Metal Container Perimeter Wall.** This low wall (See Figure C-5) is constructed using one 7 ft by 3 ft by 32 ft container. Each 32 ft unit requires approximately 224 cubic yards of infill material. Materiel requirements are shown in Table C-6.

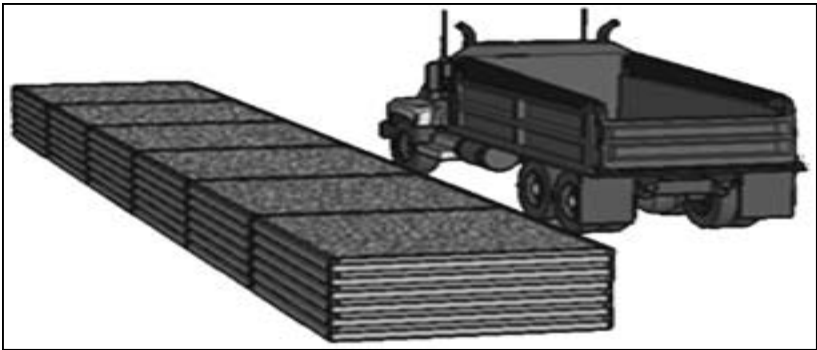


Figure C-5. Low soil-filled metal container perimeter wall concept

**High Soil-Filled Metal Container Perimeter Wall.** This high wall (See Figure C-6) is constructed using four 7 ft by 3 ft by 32 ft containers. Each 32 ft unit requires approximately 896 cubic yards of infill material. Materiel requirements are shown in Table C-6.

Table C-6. Metal Container Perimeter Wall Requirements

Height (ft)	Width (ft)	Length (ft)	NSN	Cost/Linear Foot <sup>1</sup>	Cost/Kit <sup>2</sup>
12	7	32	5450-01-554-1351	\$190.61	\$6,099.66

This kit will construct ONE wall 7 ft wide, 12 ft high, 32 ft in length. Each container course is 3 ft high. By using only one container course, this kit can provide a 3-ft high wall approximately 128 ft in length.

1. Approximate cost for each linear foot, based on kit cost and length
  2. NSN cost data as of 1 December 2008 and subject to change
- Additional sizes available. Contact Defense Logistics Agency ([www.dla.mil](http://www.dla.mil)) for further information

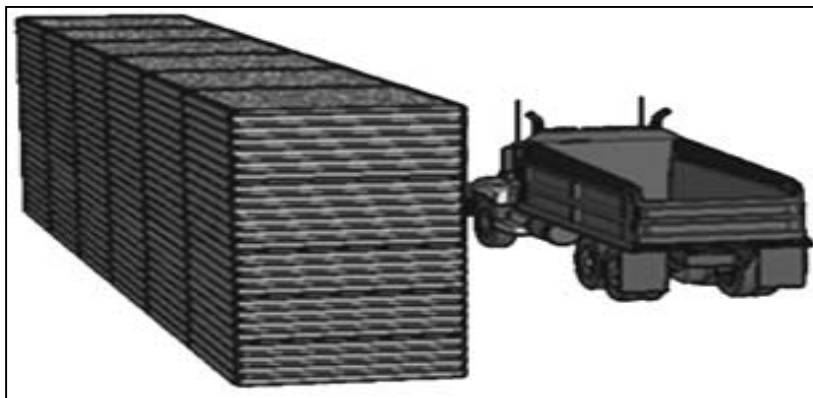


Figure C-6. High soil-filled metal container perimeter wall concept

## Annex C-2

### Fencing Materials

Fences can be used to define a perimeter and deny personnel entry to a FOB or restricted area. Fence materials are shown in the following pages. Refer to Chapter 11 for additional details. Table C-7 details materials common to all barb wire fences.

**Wire Reinforced Long Barb Tape.** Barbed tape (See Figure C-7) is used for warehousing, manufacturing, parking lots, storage, confinement and detention, and other low-level security applications. Materials are listed in Table C-8 lists materials for Helical Single Coil Barbed tape. Table C-9 lists materials for Concertina Single Coil Barbed Tape.

**Concertina Barbed Tape (Non-Reinforced Long Barb).** Non-reinforced concertina tape (See Figure C-7) is used for confinement applications, nuclear generating plants, petroleum and chemical storage, refineries, sensitive areas at airports, nuclear weapon storage, and other security applications. Table C-10 lists materials for Non-Reinforced Concertina Barbed Tape.

**Barb Wire.** Lightweight barb wire (See Figure C-8) is preferred over heavyweight barb wire. Lightweight wire costs less, costs less to transport, and has a higher strength. Table C-11 lists materials for barb wire.

**Chain Link Fence.** Chain link fences (See Figure C-9) can provide a moderate level of security. Their installation requires considerable planning and preparation compared to concertina fences. Table C-12 lists materials for chain link fences.

Table C-7. Concertina Fence Materials

Description	NSN
Post, Fence, Metal Steel 24 in. (size 5)	5660-00-270-1588
Post, Fence, Metal Steel 32 in. (size 4)	5660-00-270-1589
Post, Fence, Metal Steel 60 in. (size 3)	5660-00-270-1587
Post, Fence, Metal Steel 72 in. (size 2)	5660-00-270-1510
Post, Fence, Metal Steel 96 in. (size 1)	5660-00-262-9914
Barbed, Tape, Concertina (1 roll=50' erected length)	5660-00-921-5516
Fence Post Driver Hammer	5660-01-248-2466
Barb Gloves	8415-00-926-1674

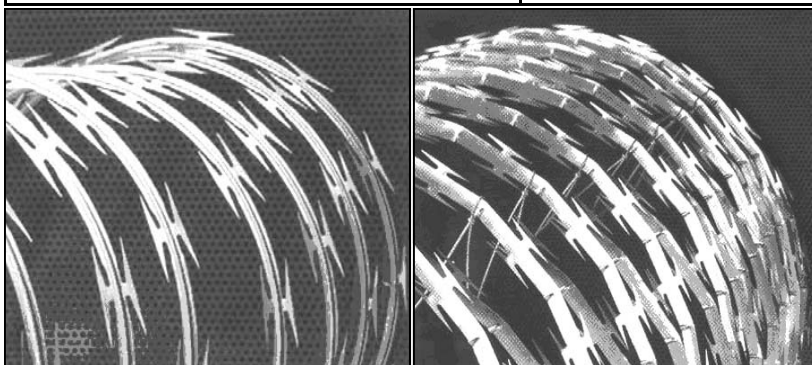


Figure C-7. Barbed Tape (Left: Reinforced; Right: Non-reinforced)

Table C-8. Helical Single Coil Barbed Tape

NSN	Dia.	Strip Matl	Core Wire	Yield	Pkg
5660-01-457-9757	18"	SS	GA	50 ft	5/box
5660-01-495-6123	18"	GA	GA	50 ft	5/box
5660-01-457-9828	18"	SS	SS	50 ft	5/box
5660-01-457-9842	24"	SS	GA	50 ft	5/box
5660-01-495-6277	24"	GA	GA	50 ft	5/box
5660-01-457-9843	24"	SS	SS	50 ft	5/box
SS = Stainless Steel GA = Galvanized Aluminum					

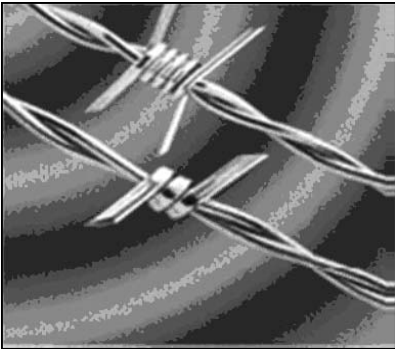


Figure C-8. Barb Wire

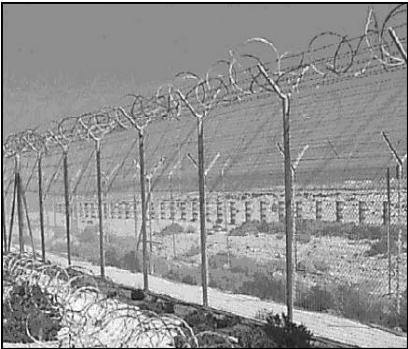


Figure C-9. Chain Link Fence

Table C-9. Concertina Single Coil Barbed Tape

NSN 5660-01-	Dia	Coil Loops	Strip Mail	Core Wire	Clips	Coil Spacing	Yield	Pkg
457-9847	18"	31	SS	GA	3	32"	15'	4/Box
495-6178	18"	31	GA	GA	3	12"	15'	4/Box
457-9849	18"	31	SS	SS	3	12"	15'	4/Box
457-9850	24"	31	GA	GA	3	16"	20'	5/Box
495-6284	24"	31	GA	GA	3	16"	20'	5/Box
457-9852	24"	31	SS	SS	3	16"	20'	5/Box
495-9534	30"	51	SS	SS	5	12"	52'	4/Box
495-9566	30"	51	SS	GA	5	12"	25'	4/Box

SS = Stainless Steel  
GA= Galvanized Aluminum

Table C-10. Non-Reinforced Concertina Single Coil Barbed Tape

NSN 5660-01-	Dia	Coil Loops	Strip Mail	Coil Spacing	Yield	Pkg	ATSM F1910 Item #
495-6363	30"	101	SS	12"	50'	7/Box	#25

SS = Stainless Steel

Table C-11. Barb Wire

	NSN	
	5660-00-224-8663 (4 Barb)	5660-01-309-4223 (4 Barb)
Description	Heavyweight Barb Wire	Lightweight Barb Wire
Steel	Low Carbon	High Tensile
Size	12.5 Gauge	15.5 Gauge
Length	1,320 Feet	1,320 Feet
Weight per Roll	90 lbs	42 lbs
Roll per Pallet	18 Rolls	36 Rolls
Containers	20 Foot Container, based on 10 Pallets; 180 Rolls	20 Foot Container, based on 10 Pallets; 360 Rolls

Table C-12. Chain Link Fence

Description	NSN
Chain Link Fabric Fencing Wire - 8 ft high by 50 foot roll - 2 inch mesh - 9 gauge - 1.2 oz zinc coating	5660-00-720-4527
Post --- 2.375 inch OD---10 feet long---3.65# per foot---thickness .154---galvanized steel pipe	5660-01-247-5681
Top Rail pipe --- 21 feet long---1.66 inch OD-- galvanized steel pipe---0.111 wall thickness	5660-00-969-5285
Tension Bar---94 inches long --- .188 inch thick --- .75 inches wide ---galvanized steel bar	5660-00-408-8821
Tension Band--- Galvanized steel straps---.75 inches wide x 12 gauge thick---used with tension bar	5660-00-467-3276
Arm Extension---single arm at 45 degrees---fits on top of 2.375 post---accepts 3 strands of barbed wire	5660-00-408-8743
Rail End --- steel or cast iron with Galvanized finish--- attaches to 1.666 top rail	5660-01-038-1458
Tie Wire -- 9 gauge --- 6.5 inches long --used to attach fencing fabric to posts	5660-01-063-4873
Brace band-- galvanized .75 inch, 12 gauge used to secure top rail end to post	5660-01-021-6356

**Hatbox Rapid Dispensing and Recovery Unit.** The Hatbox Rapid Deployment Unit (See Figure C-10) is designed for military and police use in varying climates and terrain conditions. This unit is rapidly dispensed and quickly recovered for repeated reuse. Developed for interior and exterior applications, this unit is deployed in hallways, stairwells, entrances and exit areas, etc. Table C-13 lists materials for the Hatbox Rapid Deployment Unit.

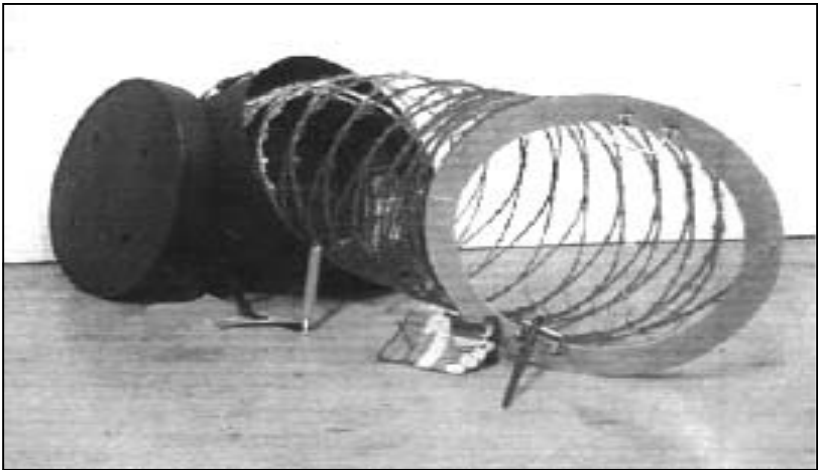


Figure C-10. Hatbox Rapid Dispensing and Recovery Unit


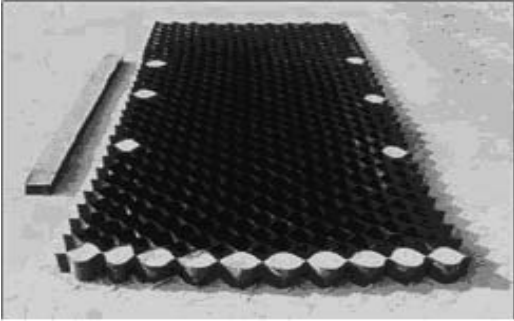
Table C-13. Hatbox Single Coil Concertina Rapid Deployment Unit

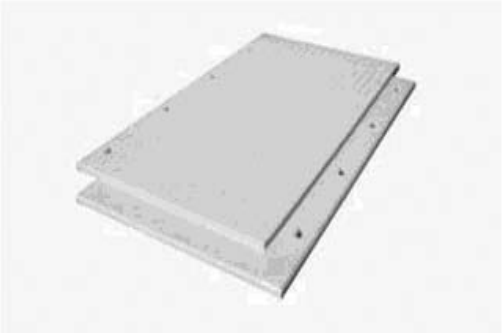
NSN	Dia	Coil Loops	Strip Mail	Cable	Welds	Yield	Pkg
5660-01-495-6421	30"	101	SS	1	5	50'	One/ Concertina
SS = Stainless Steel							



Annex C-3

Ground Stabilization Products

Item Description	NSN
<p data-bbox="355 259 527 285">AM2 Landing Mat</p>  <p data-bbox="153 529 708 649">This is a medium-duty, aluminum, landing mat capable of supporting both fighter and cargo aircraft operations. The USAF, USN, and USMC use this mat for expedient airfield construction. This mat should be placed in a brickwork pattern to offset joints. Specifications:</p> <ul style="list-style-type: none"> <li data-bbox="336 651 546 675">16 Panels (2 ft x 12 ft)</li> <li data-bbox="346 677 536 701">4 Panels (2 ft x 6 ft)</li> <li data-bbox="331 703 551 727">Pallet Weight: 2,880 lb</li> <li data-bbox="346 729 536 753">Pallet Area: 432 ft<sup>2</sup></li> </ul>	<p data-bbox="761 259 940 285">5680-01-176-9076</p>
<p data-bbox="225 766 657 815">Geocell Cellular Confinement System (Sands and Soils with CBR Greater than 4%)</p>  <p data-bbox="153 1156 723 1302">Geocell is a three dimensional honeycomb-like structure that stabilizes fill material by confinement. This product has been evaluated extensively for use in sands and other soils. The Geocell collapses into lightweight, compact bundles for easy transport and is expanded during installation. Specifications:</p> <ul style="list-style-type: none"> <li data-bbox="246 1328 636 1352">Collapsed Panel Size: 4 in. x 8 in. x 11 ft</li> <li data-bbox="246 1354 636 1378">Expanded Panel Size: 8 in. x 8 ft x 20 ft</li> <li data-bbox="253 1380 629 1404">Expanded Panel Area: 160 square feet</li> <li data-bbox="342 1406 540 1430">Weight: 113 lb each</li> </ul> <p data-bbox="178 1432 704 1474">Typical pallet holds 10 each, for a total weight including wood pallet: 1165 lb.</p>	<p data-bbox="761 766 940 815">5680-01-198-7955 (Closed Cell)</p> <p data-bbox="761 841 940 889">5680-01-501-1032 (Perforated Cell)</p>

Item Description	NSN
<p style="text-align: center;"><b>Dura-Base Mat</b></p> <p>The DURA-BASE Interlocking Mat System is made of High Density Polyethylene (HDPE) and has a service life expectancy of 15 years. The system is used in commercial oil fields and can be used for building roads over very soft soils (CBR &lt; 1%). Two layers of mat are required for road construction over very soft soils.</p>  <p>(For wet or soft soils with CBR Less than 4%, a geotextile (NSN: 5675-01-471-2674) should be placed between these systems and the natural sub-grade soil to reduce mudflow and the degradation of the system. Specifications:</p> <p style="text-align: center;">Panel Size: 4.5 in. x 8 ft x 14 ft  Half Panel: 4.5 in. x 8 ft x 7.5 ft  Full Panel Weight: 1,050 lb.  Full Panel 8-ft x 14-ft  Half Panel 8-ft x 7.5-ft</p> <p style="text-align: center;"><b>Related Materials:</b></p> <p>Locking Pin ..... 5675-01-476-7336  Cover Pin ..... 5675-01-476-7338  Spike ..... 5675-01-476-7339  Tool Kit ..... 5675-01-476-7345</p>	<p>5675-01-471-2683 (Full Panel)</p> <p>5675-01-476-7335 (Half Panel)</p>
<p style="text-align: center;"><b>Operational Foldable Fiberglass Mat (FFM)</b></p> <p>Specifications:</p> <p style="text-align: center;">2 Panels (54 ft x 30 ft)  2 Joining panels (24 ft x 2 ft)  2 Joining panels (30 ft x 2 ft)  Pallet Area: 3,240 ft<sup>2</sup>  Nominal Mat Thickness: 0.20 in.  Weight: 3000 lb.</p>	<p>5680-01-368-9032</p>
<p style="text-align: center;"><b>Training Foldable Fiberglass Mat (FFM)</b></p> <p>Specifications:</p> <p style="text-align: center;">2 panels (30 ft x 54 ft)  2 Joining panels (30 ft x 2 ft)  2 joining panels (24 ft x 2 ft).</p>	<p>5680-01-354-8331</p>

Item Description	NSN
<p data-bbox="303 154 556 175">Ace Glass Reinforced Mat</p> <p data-bbox="153 203 700 345">The fiberglass reinforced mat (FRM) system is a strong, lightweight system capable of being carried by two men. The mat consists of a polyester resin reinforced with 4 plies of woven fiberglass. The mat is connected together using 6 aluminum connector pins to form various configurations.</p>  <p data-bbox="153 716 703 907">The Army Corps of Engineers has approved this multi-purpose mat system for helipads, with the following exceptions. The CH-47 is the maximum size rotary aircraft approved. It is also critical that the ground soil be at least CBR 4 or greater and the perimeter of the helipad anchored every 6 feet. It may also be necessary to use geotextile, NSN 5675-01-471-2674 for certain applications. Specifications:</p> <p data-bbox="244 933 613 1029"> Panel Size: 6ft-8in x 6ft-8in panels  Usable Surface Area: 36 sq. ft. / panel  Panel Thickness: 0.35 in.  Weight: 115 lb/panel </p> <p data-bbox="153 1057 471 1127">This NSN includes:  6 Pin Connectors  1 Duck Bill Ground Anchor.</p> <p data-bbox="153 1154 685 1273"><b>(Wet or Soft Soils with CBR Less than 4%): *A Geotextile (NSN: 5675-01-471-2674) should be placed between these systems and the natural sub-grade soil to reduce mudflow and the degradation of the system.</b></p>	<p data-bbox="749 154 928 175">5675-01-476-8989</p>

Annex C-4


Lighting Products

Item Description	NSN
Portable Lighting	
Light, Chemiluminescent, Green	6260-01-074-4229
Light, Chemiluminescent, Red	6260-01-178-5559
Light, Chemiluminescent, Blue	6260-01-178-5560
Light, Chemiluminescent, Infrared	6260-01-195-9752
Light, Chemiluminescent, Yellow	6260-01-196-0136
Light, Chemiluminescent, White	6260-01-218-5146
Light, Chemiluminescent, Green	6260-01-247-0362
Vehicle Light Fixtures	
Spotlight	6220-00-756-5764
Headlight	6220-01-193-1970
Floodlight, Electric	6220-01-306-8203
Electrical Portable, Hand Lighting Equipment	
Flashlight, Olive Drab	6230-00-264-8261
Electric Lantern, 6VDC	6230-00-500-0523
Electrical Lighting	
Tow Light Assembly	6220-01-217-8316
Floodlight Assembly	6230-01-158-8019
Lamp Incandescent	6240-00-019-3093
Lamp Incandescent, Waterproof	6240-00-966-3831
Mantle Illuminating	6260-00-270-4060

Annex C-5

Construction Materials

Item Description	NSN
Lumber/Plywood	
1x4x16, Common	5510-01-433-1145
1x8x16, Common	5510-01-433-1183
2x6x16, #2	5510-01-433-1371
2x12x16, #2	5510-01-433-3930
1x10x16, #2 Common	5510-01-433-1199
2x4x16, #2 Common	5510-01-433-1244
¾" AC Plywood	5530-00-129-7833
¾" CDX Plywood	5530-00-618-8073
½" CDX Plywood	5530-00-618-6958
½" AC Plywood	5530-00-129-7777
5/8" CC Plywood	5530-00-128-5147
1" AC Plywood	5530-00-129-7889
¾" BB CF Plywood	5530-00-128-5134
Sandbags	
Sandbag – Green, Poly	8105-00-142-9345
Sandbag – Green, Acrylic	8105-00-935-7101
Sandbag – Sand, Cloth	8105-00-782-2709
Sandbag – Sand, Poly	8105-01-336-6163
Sandbag – Sand, Acrylic	8105-01-331-3704
E-Glass	
E-Glass, Ballistic Grade 4 ft x 8 ft	9340-01-533-3758
Drums and Cans	
Drum, shipping & storage, 55 gallon, steel closed head	8110-00-292-9783
Drum, shipping & storage, 55 gallon, steel open head	8110-00-030-7780
Drum, steel, ship & storage, 85 gallon, steel	8110-01-101-4055

Item Description	NSN
<b>Advanced Composite Building Panel System</b>	
Advanced composite building panel system suitable for major load-bearing structural applications. The modular construction system consists of a small number of interlocking fiber reinforced polymer structural components. Main building panel is 3" thick and 24" wide. Panels can be connected using toggles.	5510-01-433-1145
8 foot long panel	5675-01-500-2729
10 foot long panel	5675-01-500-2761
12 foot long panel	5675-01-500-2803
14 foot long panel	5675-01-500-2808
<b>Rubberized Roof</b>	
Rubberized roof – non-reinforced EPDM membrane for roofs of earth-filled barriers. Useful for roofs of observation posts. 20' x 100' sections. Thickness: 0.045".	5660-01-504-5373
<b>Sandbag Filling Machines</b>	
Manual, gravity fed machines:	
Two Hopper	3895-01-460-3910
Three Hopper	3895-01-470-5748
Five Hopper	3895-01-470-5751
Automatic, gas powered machines:	
Model MB-3	3895-01-460-4545
Model ASB-3	3895-01-470-5752
Trailer, Model C-2T	3895-01-460-4548
	
Sandbag Filling Machine	

## Annex C-6

### Other Supporting Technologies

Additional technologies have been developed to drastically improve the effectiveness of analysis, terrain visualization, and vehicle search in support of base defense operations. This annex describes technologies that support base defense and those that support entry control point (ECP) operations. Refer to Chapter 9 for access control TTPs.

**Marine AT/FP Kit.** This kit (See Figure C-10) is one of five that the Marines have pre-configured based on mission requirements and resources. The current set is designed for one ECP and four Expeditionary Packs. This kit is not a stand alone escalation of force (EOF) kit, but when complimented by other Class IV items; can provide the user with almost all of the measures needed. Major shortfalls of this kit as it pertains to EOF are the visual and audible signals (flares, sirens, laser designator, bullhorns, etc). Allocation is a minimum of one for each FOB. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

**REF Escalation of Force Kit.** Each escalation of force (EOF) kit (See Figure C-12) consists of 2 Convoy Kits and 2 TCP Kits. These individual kits contain the items listed in Table C-14. The EOF Convoy Kit contains

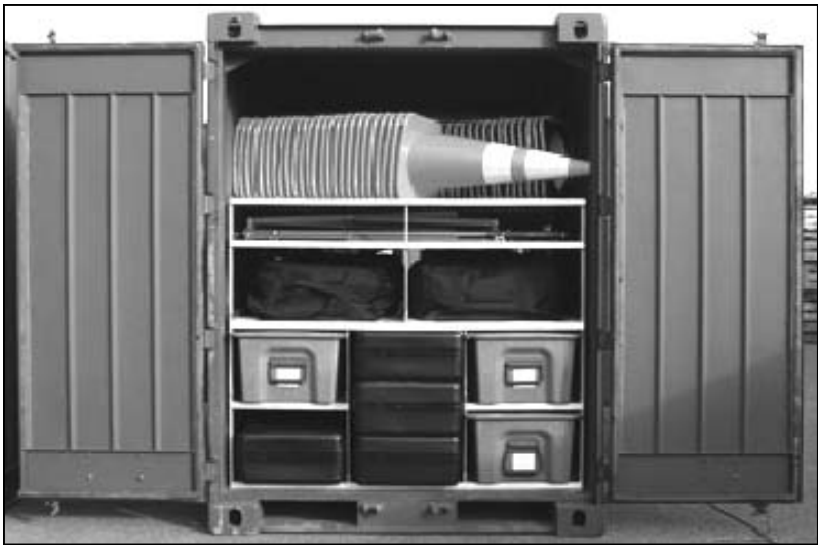


Figure C-11. Marine AT/FP Kit.

the tools needed in appropriate quantities to outfit a 4(+) vehicle convoy. Concept of operation for EOF kits calls for a 3 to 1 ratio of Convoy to TCP kits for a 4(+) Vehicle Convoy. Training is provided during the RSOI phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.



Figure C-12. REF Escalation of Force Kit

Table C-14. REF Escalation of Force Kit Contents

Item	Convoy Kit	TCP Kit
Sirens	2 ea	
Translators	1 ea	
Green Lasers	4 ea	1 ea
Traffic Signs		2 ea
Cones / Power Flares		6 ea
Spike Strips		1 ea
Speed Bumps		2 ea
Weapon Mounted Flashlights	4 ea	
Spotlights	2 ea	
GTA Cards	8 ea	8 ea
Traffic Paddles		2 ea
Fido	1 ea per 10 Convoy Kits	



**Vehicle Light Arresting Device.** The Vehicle Light Arresting Device (VLAD; See Figure C-13) is a lightweight vehicle capture system designed to be deployed by a single person across a road to stop a vehicle. It is a fishnet style design built from extremely strong Spectra Fibers with small spikes across the leading edge of the net. When run over by a car, the spikes embed themselves in the tires of the car. The VLAD also “ties up” the vehicles running gear preventing it from freeing itself after stopping.

The VLAD comes packed in a backpack-style carrying case. Allocation is one for each deliberate checkpoint. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

**Portable Vehicle Arresting Barrier.** The Portable Vehicle Arresting Barrier (PVAB; See Figure C-14) is a non-lethal wheeled vehicle capture and immobilization system that spans a roadway being secured to prevent unauthorized vehicles from entering and exiting a designated area, while allowing authorized vehicles egress without damage to either vehicle or the PVAB. Allocation is one for each deliberate checkpoint. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

**Hasty Check Point Kit.** This kit (See Figure C-15) consists of phraselators, VLADs, spike strips, traffic cones, hand-wand metal detectors, search



Figure C-13. Vehicle Light Arresting Device



Figure C-14. Portable Vehicle Arresting Barrier



Figure C-15. Hasty Check Point Kit

mirrors, check point signs, and additional Class IV items. Visual and audible signals (bullhorn, sirens, spot lights) are not included. Allocation is one for each traffic control point or hasty check point. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

**ECP/Deliberate Check Point Kit.** This kit (See Figure C-16) provides an illuminated search area. The kit contains a light set (6 lights with tripods), generator, voice response translator; hand held lights and wands, hand held metal detector, search mirrors, check point signs, and additional Class IV items. Visual and audible signals are not included. Allocation is one for each hasty or deliberate checkpoint. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

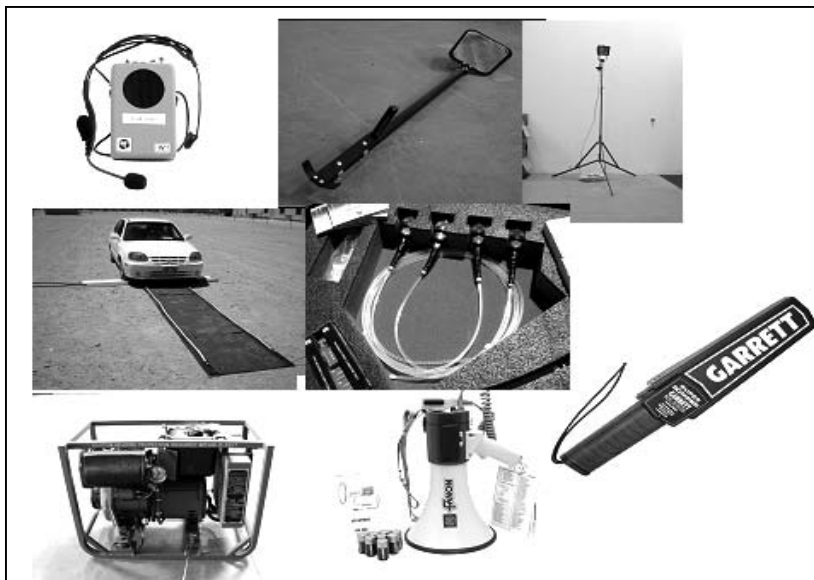


Figure C-16. ECP/Deliberate Check Point Kit

**Expeditionary Pack.** This kit (See Figure C-17) is contained in a weatherproof storage container and contains a SLAM Illuminated Mirror with 8NX Flashlight; SAM Non-Illuminated Mirror; 2 Telescoping Search Mirrors, a lighting pack, a Lumenyte pack, a SnakeEye pack and SnakeEye support pack, an explosive trace detector Kit. Other materials include LCVSK Quick Reference Cards (both laminated and compact disc), DOD/TSWG Vehicle Check List, USMC FMFRP 7-37 Vehicle Bomb Search Tech Data Sheet, USN & USMC Antiterrorism/Force Protection Document Guide, and Material Safety Data Sheets (MSDS) for the Expray reagents.

Allocation is one for each ECP or Tactical Control Point (TCP). Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center. Contact the Naval Facilities Engineering Service Center for more information.



Figure C-17. Expeditionary Pack

**Remote Access Kit.** This kit (See Figure C-18) contains 3.5mm Kevlar line (a 50m reel and a 100m reel), a pulling handle, Karabiners (both Screw Gate and Integral Pulley), screw eye self taps, large and small pitons, hooks (single-tang, double-tang, and 25mm), self-opening snatch block, self-locking grips, shock cords, spring loaded clamp, and wire slings. Units request kits and training as a part of their training support package and are trained during RSOI. Units then have the opportunity to engage training explosive devices and materials during the STX and continuous operations phases of the rotation.



Figure C-18. Remote Access Kit

**Search-Explosives Detection Kit.** This kit (See Figure C-19) contains an explosive detection kit, a hand-held metal detector, an expendable lit mirror, small- and large-mirror extendable poles, mine probe, distance finder, non-magnetic fork and trowel, pruning saw, scrub cutter, two small

torches, laser pointer , bore scope, seventeen-piece bit set, and cordless drill. Units request kits and training as a part of their training support package and are trained during RSOI. Units then have the opportunity to engage training explosive devices and materials during the STX and continuous operations phases of the rotation.



**FOR OFFICIAL USE ONLY**

cle, personnel or package inspections and perimeter patrols. Objects can be detected by the heat signature or shadow they cast to see foreign material hidden inside tires, fuel tanks or body panels. Weapons and vest bombs concealed under clothing can also be detected at up to 50 ft or more. The camera cannot see through insulation or highly polished surfaces such as glass. Effective range is in excess of 100 yards depending on the application.

The camera kit consists of the Scout II Thermo Vision Camera, lens cap, protective jacket, batteries and charger, transformer for battery charger, AC power cable, 12VDC adapter, RCA cable, and a rigid sun visor. Allocation is one for each ECP or checkpoint. Contact the Naval Facilities Engineering Service Center for more information.

**Vehicle Search Kit.** This kit (See Figure C-21) provides an illuminated search area and contains Lumenyte light tubes, a speed bump, search area mats, a light source, search mirrors, hand lights and wands, and sure-fire lights. Allocation is one for each ECP or checkpoint. Contact the Naval Facilities Engineering Service Center for more information

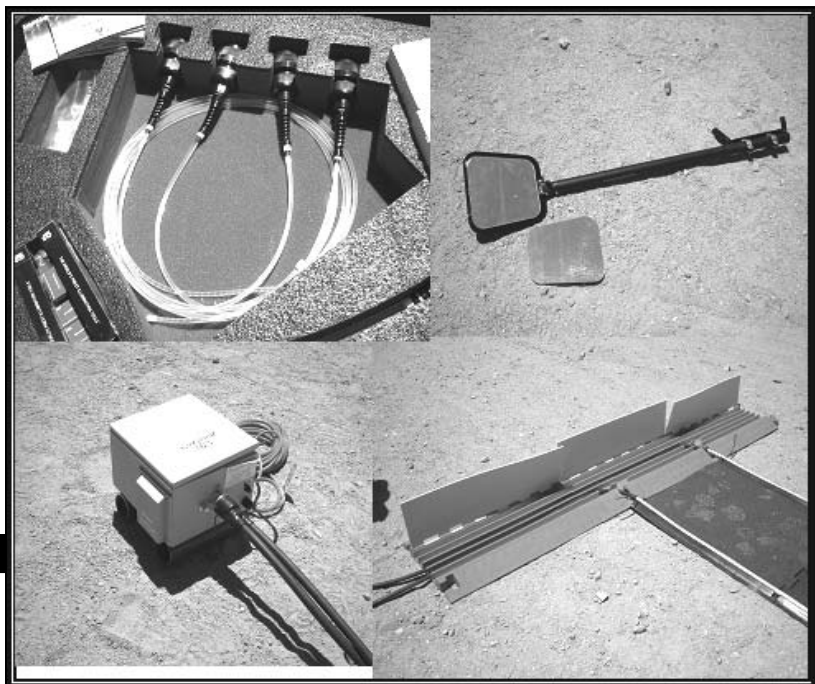


Figure C-21. Vehicle Search Kit

**Tactical Unmanned Aircraft System.** The tactical unmanned aircraft system (UAS; See Figure C-22) is capable of over 15 hours of continuous operation. It operates at a cruising speed of 50 knots and an altitude of 5,000 feet and weighs approximately 18 kg (40 lbs). The UAS flies a pre-programmed route via multiple waypoints, but can be dynamically tasked during a mission based on the changing situation. Allocation of one tactical UAS is normally assigned to a base defense sense and warn package in the baseline configuration and can be either integrated as a part of the Common Operating Picture or as a stand alone system. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.



Figure C-22. Tactical Unmanned Aircraft System

**Battle Staff Analysis Software.** All Source Analysis System (ASAS) should have Analyst Notebook software loaded (Army Corps of Engineers uses Version 6.00.55). For Crystal Reports Version 10 Professional, the Brigade MUST purchase software if the unit intends to use this system outside of NTC facilitated training. Computer MUST have FalconView software loaded for program to function. Allocation is one for each battle staff or BDOC. Training is provided during the RSOI Phase of operations at the Combined Training Centers and is specifically trained at the National Training Center.

**Resources (For Additional Information)**

The **Naval Facilities Engineering Command / Engineering Service Center** (NAVFAC ESC) is an Echelon III organization that provides specialized facilities engineering, technology, and facilities expertise. Their products and services are centralized for economy and efficiency, or require Navy-wide execution to the Navy, Marine Corps, and Department of Defense (DoD). They are the primary points of contact for the Expeditionary Pack (See Page C-23), the Search-Thermo Vision Camera (See Page C-25), and the Vehicle Search Kit (See Page C-25). Their website is [https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC\\_WW\\_PP/NAVFAC\\_NFESC\\_PP](https://portal.navfac.navy.mil/portal/page/portal/NAVFAC/NAVFAC_WW_PP/NAVFAC_NFESC_PP). They can also be reached at the address below:

Naval Facilities Engineering Service Center  
Explosive Detection Equipment Program  
1100 23rd Ave. – Code ESC-66  
Port Hueneme, CA 93043-4370  
805-982-3556 / DSN 551-3556

The **USACE Reachback Operations Center** (UROC) provides a reach-back engineering capability that allows DoD personnel deployed worldwide to talk directly with experts in the United States when a problem in the field needs quick resolution. Deployed personnel can be linked to subject-matter experts within the Corps of Engineers, private industry, and academia to obtain information and analysis of problems that would be difficult to achieve with the limited expertise or computational capabilities available in the field. For further information on the UROC, contact the USACE ERDC at 601-634-2735/3485; DSN 312-446-2735/3485; e-mail: [uroc@usace.army.mil](mailto:uroc@usace.army.mil) (secure e-mail: [rfi@usace.army.mil](mailto:rfi@usace.army.mil)). Their website is <https://reachback.usace.army.mil> (secure website is <http://reachback.usace.army.mil>).



## Appendix D

# Soil-Filled Container Applications

### Introduction

In recent years, the use of soil-filled containers by military forces world-wide has increased greatly. These containers have many applications, including rapid construction of barriers, walls, bunkers, protective and fighting positions. Typical structures consist of a series of large, linked, self supporting cells or bins. There are two general types of soil-filled containers in use: wire/fabric and metal containers.

**Wire and fabric containers.** Each bin consists of collapsible wire mesh lined with a geotextile fabric. The bins are connected at the corners with spiral wire hinges that allow the wall sections to be expanded from a compact, folded storage configuration. Each kit consists of bins, connecting pins, and plastic ties. The bins come in a variety of sizes. The advantage of using this container is that the cells are collapsed during transport. They are then expanded and filled at their destination. This allows the walls to be transported at only 5 percent of their as-constructed volume. They are very light and can be assembled very rapidly.

**Metal containers.** Each bin consists of corrugated metal panels. These panels are shipped flat and unassembled. They are then assembled and filled to construct an appropriate protective structure. Each kit consists of four panel types (side, end, cross, and brace), connecting pins, flaring tools, and corner containment materials (wire mesh and poly film). Metal containers come in sizes designed to hold from 47 to 76 cubic yards of soil. One advantage for using metal containers is the increased life span when subjected to long-term environmental effects. They are, however, heavier than the wire and fabric containers.

This appendix discusses applications of soil-filled containers. Although the term soil-filled is used throughout the appendix, these structures can utilize different infill materials, including sand, loam, clay, or other suitable materials. Strengths and weaknesses of these material is also discussed. Where applicable, bills-of-material and construction techniques for the various structures are provided for reference.

### General Construction Techniques

Many soil-filled container structure designs have been developed by the Engineer Research and Development Center (ERDC) which contain spe-

cific layout configurations and utilize multiple unit types. If it is necessary to construct a structure for which a specific design is not available, the appropriate combination of container units must be determined for the given application. However, in either situation, the basic construction guidelines depicted here should be utilized.

Soil-filled containers are manufactured in several different basic units, distinguished by material, color, dimensions (height, width, length) and the number of bays contained within the units. Wire and fabric container units are presently manufactured in green, desert tan, and gray colors. The dyes used to pigment the fabrics affect resistance to ultraviolet (UV) light degradation, and according to current data the gray color fabric deteriorates the fastest. Based upon this susceptibility to UV deterioration, the gray colored fabric is not recommended for use. Metal containers are not subject to UV light degradation.

**Site Preparation and Foundation Construction.** The performance of soil-filled container structures, as with any conventional structure, is highly dependent upon proper site selection and preparation. Soil-filled container structures rely heavily upon the strength of near-surface soil material for overall structural stability. The condition of these near surface materials can be deteriorated by elevated moisture levels, soil erosion, freeze/thaw cycles, decay of organic matter, compression of weak soils, etc. Therefore, the site evaluation process should include consideration of site drainage patterns and existing soil conditions for the purpose of identifying a well drained, stable site. Refer to Chapter 11 of FM 5-34, *Engineer Field Data*, for procedures to assist in soil evaluation.

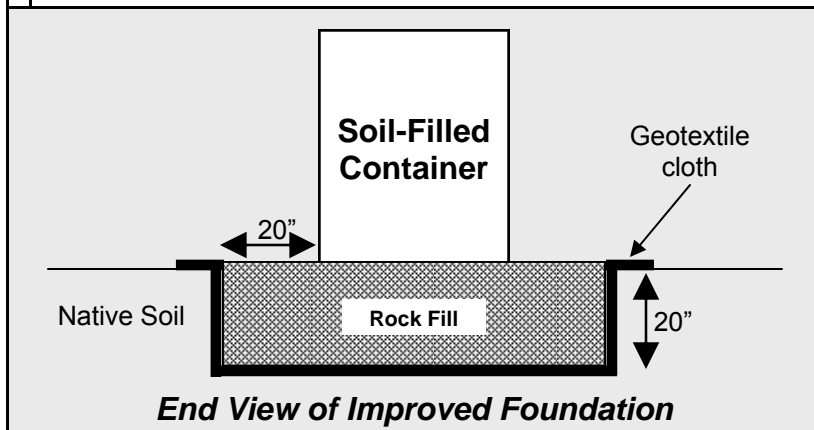
Soil-filled container structures should be constructed on a relatively flat, level foundation. The foundation must exhibit sufficient strength and stability to support the structure over its intended life. If construction will not take place on an improved surface (such as concrete, asphalt, or stabilized soil) the foundation area must be improved (See *Site Preparation and Foundation Construction Considerations*).

## Wire and Fabric Containers

**Layout and Connection.** Wire and fabric container units are available in a variety of sizes. The most common sizes are depicted in Figure D-1. These containers are transported in a compressed “accordion” style, and are expanded on-site for construction (See Figure D-2). When laying out units, position them so that the plastic wire ties attached to the units are located at the top. This will allow for connection to additional layers of container units during the construction process.

## Site Preparation and Foundation Construction Considerations

	Blade area to level foundation site and remove organic material and loose surface soils.
	Test exposed foundation material to ensure a stable foundation will be provided. FM 5-34, Figure 11-1 provides guidelines for procedures which can be utilized to test foundation soils.
	<p>If exposed foundation material will not provide a stable foundation, or if the life of the structure is expected to be greater than 6 months, construct an improved foundation to prevent future settlement and shifting.</p> <ul style="list-style-type: none"> <li>To construct an improved foundation, excavate a trench 20 in. deep beneath all structure walls. The width of the trench should extend 20 in. beyond each edge of the wall.</li> <li>After excavation, line the trench with a geotextile cloth (minimum weight 200 g/m<sup>2</sup>) and backfill the trench with a well compacted layer of coarse-graded fill material or crushed rock.</li> <li>Prior to construction of structure, test improved foundation to ensure the desired level of foundation strength and stability has been achieved.</li> </ul>



In most applications, it will be necessary to utilize multiple wire and fabric container units to achieve the desired dimension and shape for the structure. When utilizing multiple units in a single layer of construction, each unit should be secured to adjacent units to provide continuity throughout the structure.

Wire and fabric container units are generally connected together by utilizing two mechanisms provided as a part of the container system (See Figure D-3). These container units are manufactured with coil hinges located at articulation points. To connect units together, the coil hinges located at

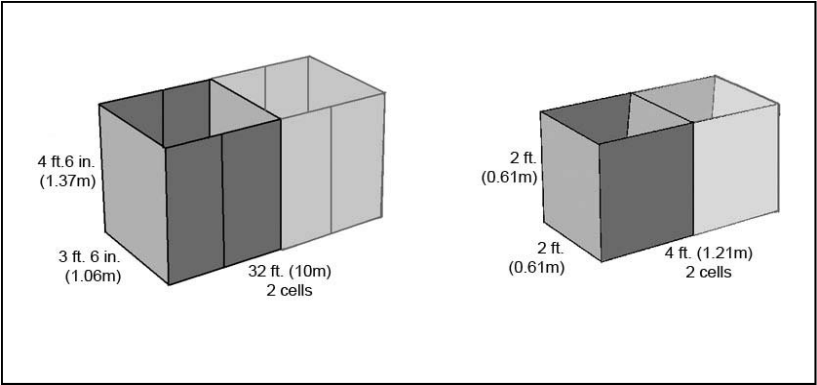


Figure D-1. Typical wire and fabric container dimensions

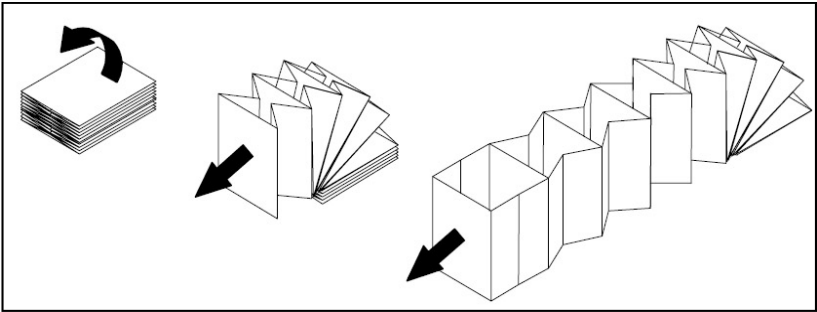


Figure D-2. Wire and fabric container expansion

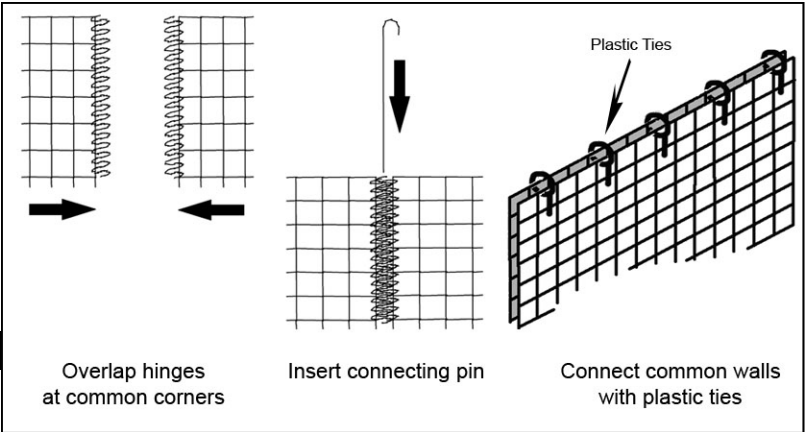


Figure D-3. Wire and fabric container connection technique

the common corners between the two units are overlapped, and a provided connecting pin is inserted into the overlapped hinges, thereby tying the corners together. Container units are also manufactured with pre-positioned plastic ties located at the tops of the units. When connecting two units together, the plastic ties located along the common wall between the units should be utilized to connect the tops of the two adjacent walls.

Container units can be connected end-to-end to obtain the necessary length for the structure. Units are connected end-to-end by connecting the coil hinges at the ends of the units to be joined, and connecting the common wall with the plastic ties.

Container units can be connected end-to-side to form corners and tees as necessary. Units are connected end-to-side by connecting the coil hinges at the common corners between the units, and connecting the common wall with plastic ties.

In addition to forming corners in an end-to-side fashion, in certain cases corners may be formed by manipulating a single container unit. To create a corner from a single unit, the unit must contain coil hinges at the center of each bay sidewall. To form a corner (See Figure D-4), begin by locating two adjacent bays where the corner is to be formed. Push the coil hinges at the center of each bay's sidewall inward, and bring all three coil hinges located at the corners of the bays together. While bringing the three corner hinges together, rotate the end of the unit to form the corner. After bringing the coil hinges together, connect the coil hinges together with a standard coil hinge connection pin.

Depending upon the height or desired wall thickness of the structure, it may be necessary to place two units together in a side-to-side fashion. When placing units side-to-side, the coil hinges at the common corners of the units should be connected with standard coil hinge connections. In addition, to prevent infill material from being deposited between the units (which may affect the overall stability of the structure), the plastic ties should be utilized to connect the common walls along the full length of the units.

**Modifications.** Based upon the dimension and layout of many structures constructed with soil-filled containers, it is necessary to utilize non-standard unit lengths as a part of construction. Consequently, container units may be modified by breaking single units into smaller, multiple units. Units can be separated into smaller units by unscrewing the coil hinges at the center of a single bay's sidewalls. After unscrewing the coil hinges, cut the geotextile liner, fold the loose ends in, and secure with the

removed coil hinges. Note that some units are manufactured with pre-made disconnection points to ease modification. These disconnection points consist of a connection pin inserted into overlapped coil hinges. Units are thus modified by removing the connection pins and separating the units (See Figure D-5).

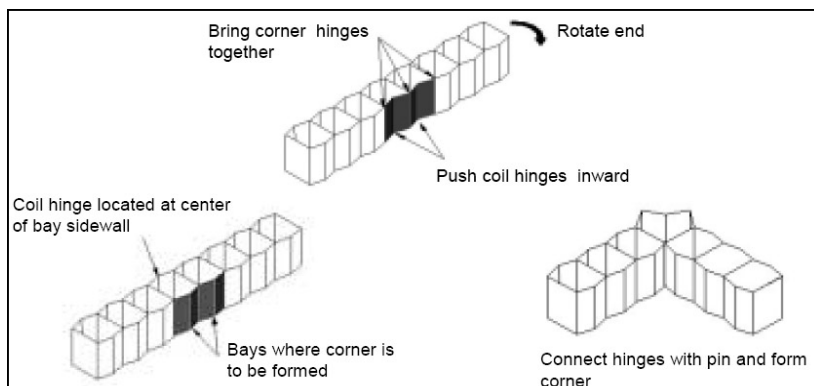


Figure D-4. Wire and fabric container corner formation technique

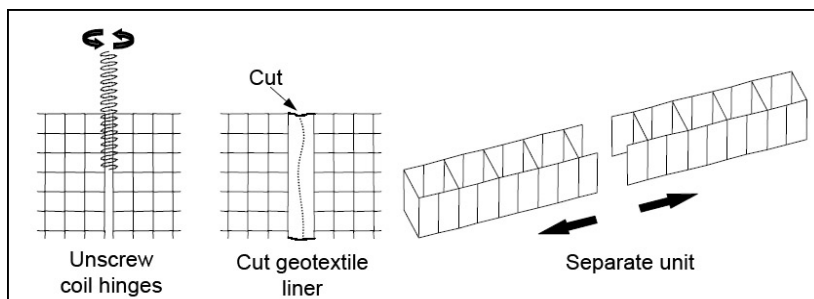


Figure D-5. Wire and fabric container modification technique

**Infill Placement.** A basic principle behind the usage of wire and fabric containers is the user's capability to easily create a lightweight "framework" for a given structure, and then fill the framework with infill material to impart structural strength and integrity. Considering that these container structures therefore rely solely upon the "fill walls" for their strength and stability, the proper placement of infill is critical to the performance of the structure. In all cases possible, the following guidelines to infill placement should be adhered to.

Prior to filling, connect all units in a single layer together and adjust to the desired layout. Attaching empty units to filled units is difficult. In general, filling of a wire and fabric container layer should begin by first filling corner bays, and then every 8th to 12th bay thereafter, with one foot of

compacted fill placed in two 6 inch lifts. This will allow the layer to be “anchored” during remaining filling activities. After anchoring the wall, filling the remaining bays should progress such that the infill material is uniformly placed throughout the container layer (specifically, do not completely fill one bay while the adjacent bay is completely empty).

Wire and fabric container walls obtain their load carrying capacity and stability by “bulging” along the sides during the filling process and allowing the wire/fabric structure to deform to its “maximum state”. By allowing the bays to reach maximum deformation during filling, the infill material becomes confined within the widest, shortest volume of space available. This significantly reduces the potential for future structure movement and failure. “Bulging” also improves structure performance by increasing the width of the container walls, thereby creating a more stable structure.

Restraint mechanisms – such as wires and bracing – must not be used to prevent “bulging” of the container. As infill is placed within the bays, the fill material exerts lateral pressures on the walls in an attempt to “push” the walls outward. This outward pressure induces stress concentrations in restraint mechanisms which can lead to failure of the restraint. Upon restraint failure, the container walls move outward to reach the maximum deformed state described above, and the infill material moves outward with the wall. As the infill material moves outward to occupy the void space created by the moving wall, the fill material also moves downward. This outward/downward infill movement will induce wall settlement, wall and load shifting, and potentially an overall failure of the structure.

To accommodate the deformation process previously described, the center coil hinges on each side of every bay must be pulled out approximately 4 in. during initial filling. If coil hinges are not present, simply pull the sides of each bay outward to create a slightly curved side wall for each bay. This will assist the bay in deforming as necessary during the filling process.

After adjusting the base, fill the bay with infill material (See Figure D-6). Unless otherwise specified, infill should be placed in lifts no greater than 9 in. thickness and must be adequately compacted. Adequate compaction can be obtained through foot compaction. During compaction, care must be taken to ensure that all infill material is compacted along the walls and in the corners. Proper compaction of infill material is critical to prevent future settlement of container walls.

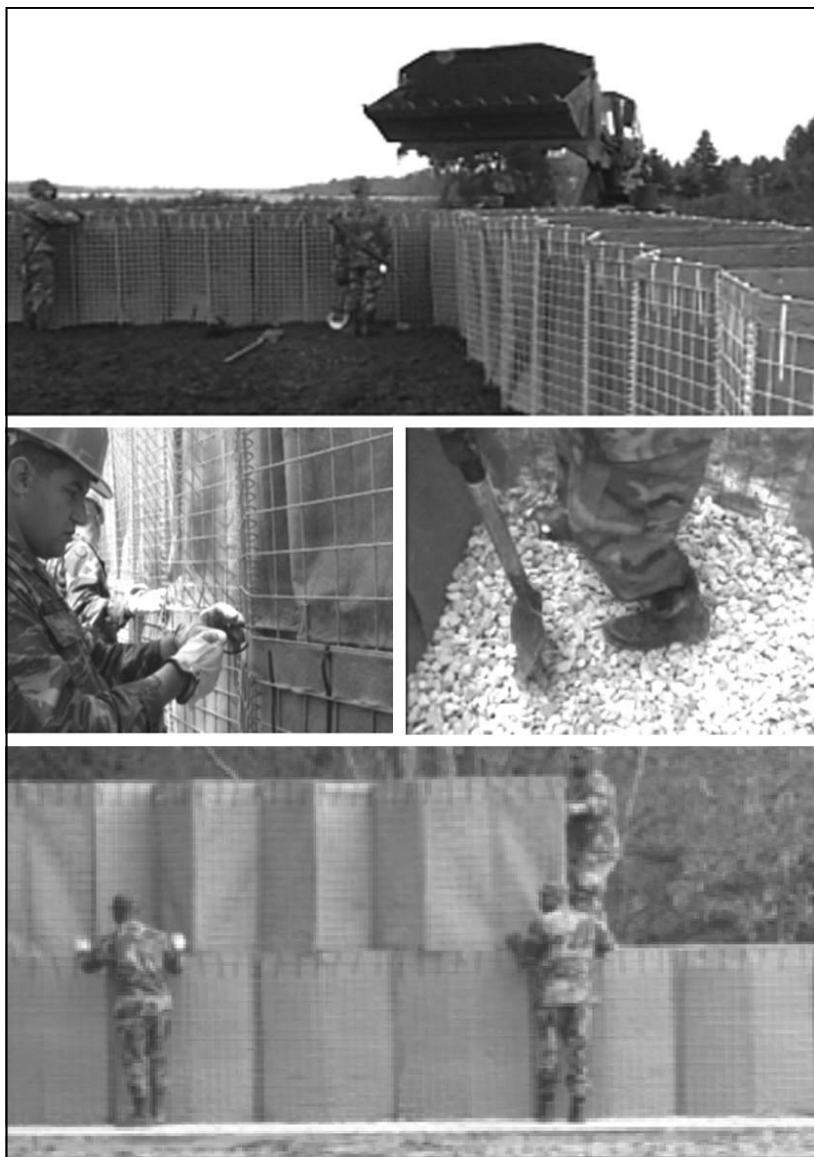


Figure D-6. Wire and fabric container infill procedure (clockwise from top: place and fill first layer; compact fill into sides and corner; place second layer; connect layers together with plastic ties)

If a second level of units is to be placed on top of the first, halt filling the first layer approximately 4 in. from the top of the unit. Place the second layer on top of the first. The second layer must be positioned to ensure that it is correctly aligned with the first layer. To achieve this alignment,



place the second layer such that the bay corners of the second layer are located directly above the corners of the first. This will allow the walls of the second layer to sit directly on top of the walls of the first layer, and thereby help prevent infill leakage and enhance structural stability. After correctly positioning the second layer, seal the wall junctions with the geotextile flaps located at the bottom of the second layer, and connect the layers together with the pre-positioned plastic ties. Continue to fill the second layer in the same manner as the first layer.

**Durability.** Considering that wire and fabric container structures will typically be placed in an exterior environment, give consideration to addressing environmental impacts on the intended life of the structure. A primary environmental factor affecting the long term performance of the containers is UV light degradation. As the result of exposure to sunlight, the fabric liner may deteriorate over a period of time, thereby releasing the infill contained within the units. During the manufacturing process, fabrics are colored with dyes which can affect UV resistance. Based upon current information, the expected life of the available fabric colors are: Gray – 1 to 2 years; Green – greater than 6 years; Tan – no data available

In extremely windy environments, it is possible that some fill materials may be scoured away by wind action. This type of scour activity can negatively affect the structure if it is allowed to undermine soil surfaces which support roof structures, or scour the roof cover to such an extent that adequate cover is no longer provided. In these conditions, measures such as capping the exposed fill material with sand bags can mitigate the wind action. However, take care ensure that the use of capping materials does not create an inadequate bearing surface for roofs or other structures which may bear upon container walls.

In regions which receive high levels of rainfall, moisture infiltration may affect the durability of soil-filled container structures. Excessive moisture infiltration into the “soil walls” of the structure may induce infill settlement and /or weaken the load carrying capacity of the wall. Additionally, excessive exposure to moist conditions may promote fabric liner decay. Therefore, in environments where high levels of moisture are expected, the user may elect to place a waterproofing mechanism (such as a paint or membrane) over exposed surfaces to mitigate water infiltration. If a waterproof mechanism is used, provide some form of drainage for any water that may still infiltrate the walls. In addition, take care not to affect the load carrying functions of the structure, or to negatively impact any concealment objectives.

## Metal Containers

Metal containers (also referred to as metal revetments) can be utilized for supplemental sidewall protect or in the construction of protective positions (See Figure D-7). The containers are shipped flat in an unassembled state. They are assembled on-site and filled with infill material in order to construct the desired protective structure. Each kit will consist of four (4) panel types (side, end, cross, and brace), connecting pins, flaring tools, and corner containment materials (wire mesh and poly film).

Metal container side panels are typically 8 feet in length. End and cross panels are typically 2-, 4-, or 6-feet in length. Brace panels are typically 4 feet in length. The panel heights vary depending on the thickness of the material: 16-gauge metal is 2 feet high; 18 gauge metal is 3 feet high.

As with the wire and fabric containers, the performance and lifespan of the containers depends on proper site selection and preparation. A well prepared foundation is vital for the performance and durability of the revetment. It is essential that ground surface be level and well compacted prior to metal container assembly.

**Layout and Construction.** All metal panels must be placed with their short leg down. This orientation will place panel notches at the top (See Figure D-8). Side panels should be placed so that the large corrugations face outward. If both 16 gauge (2 ft. high) and 18 gauge (3 ft. high) materials are being used, ensure that the 16 gauge materials make up the bottom course(s) of the container.

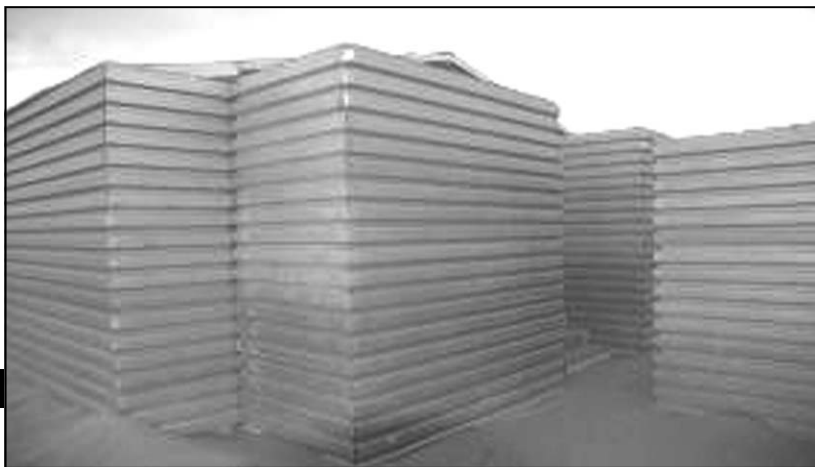


Figure D-7. Typical metal containers

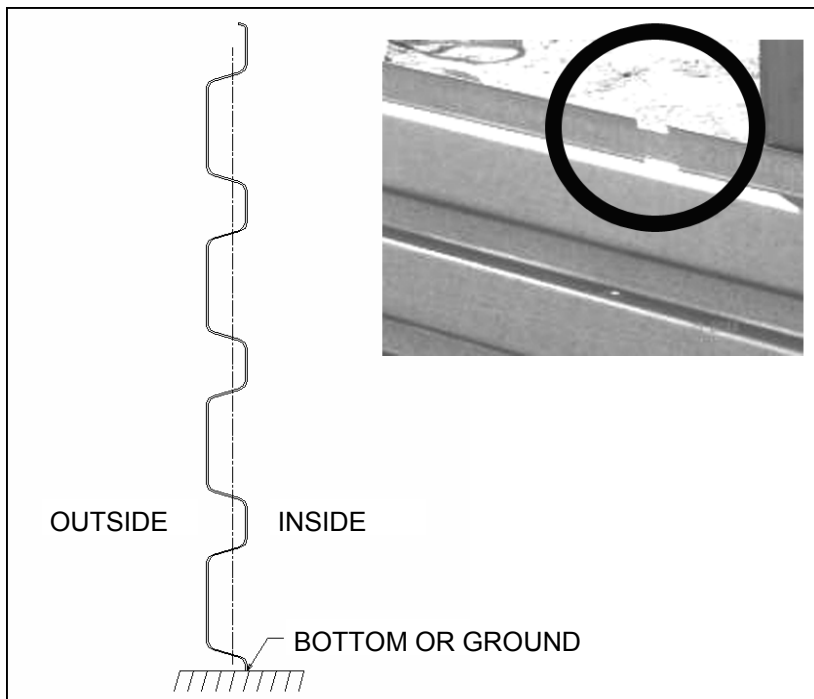


Figure D-8. Panel orientation. Panel notch at top shown in inset

All panels except side panels must have their ends flared prior to installation. Flaring may be accomplished by either the flaring tool itself, flaring tool and hammer, or with a pair of pliers (See Figure D-9). In order to prevent injury, the use of work gloves is highly recommended.

After surface and foundation preparation, assembling a metal container generally consists of five basic steps.

**Step 1.** Assemble end and side panels. Assembly should begin from left to right. Insure the small leg of the panel faces down.. Pin the side panel to the end panel with the connecting pin provided (See Figures D-10 and D-11).

**Step 2.** Add end and brace panels. The small corrugations of end panels should face each other – this allows proper alignment of brace panels.

**Step 3.** Add side and cross panels (See Figure D-10). All cross panels should face in the same direction.. Side panels should be installed

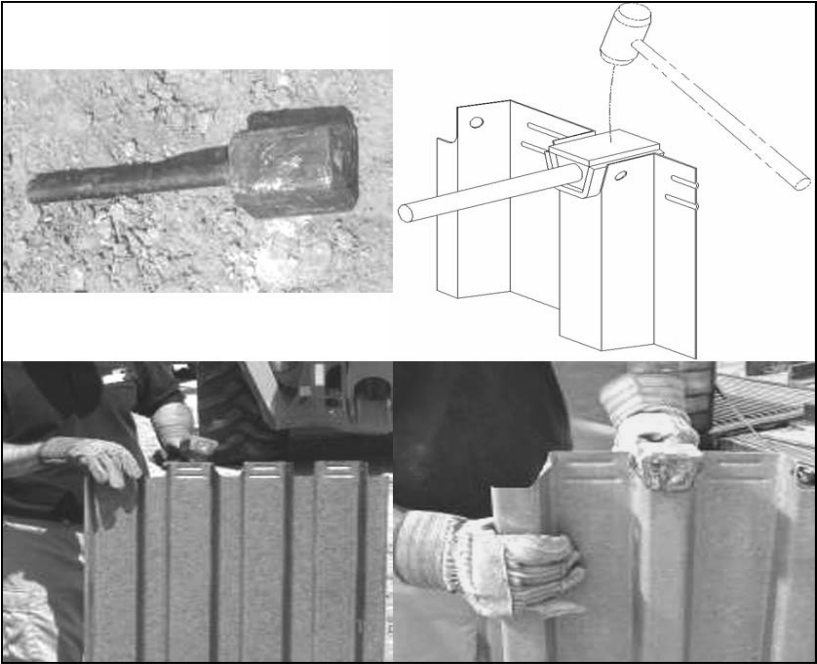


Figure D-9. Methods for flaring panels (clockwise from top: flaring tool with Hammer; flaring tool only; pliers);

from left to right to allow proper overlap. Repeat as needed to obtain the required length.

**Step 4.** Attach side panels on opposite side. Side panels should be installed from left to right to allow proper overlap.

**Step 5.** Install wire mesh and poly film to help eliminate leakage of infill material. Place poly film and wire mesh in corners. Once in place, add the appropriate infill material (See Figure D-11). Repeat these steps as needed to obtain the required height.

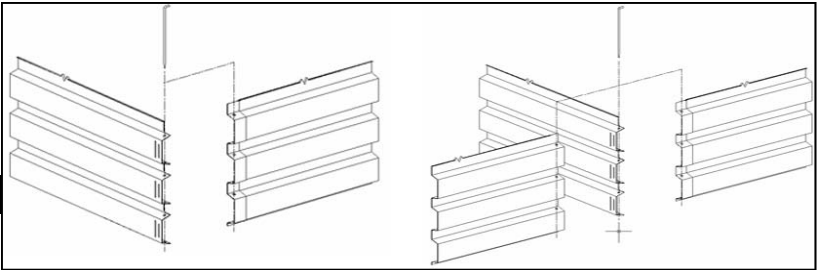


Figure D-10. Panel connection technique (left: end and side panels; right: side and cross panels)



Figure D-11. Metal container infill procedure (clockwise from top left: assemble end and side panels; add cross panels; add brace panels; add poly film and wire mesh; add infill material)

## Hardened Fighting and Observation Positions

The following annexes show several designs using soil-filled containers for construction of fighting positions and observation posts. These positions will allow engagement of an enemy and offer some level of protection from small arms, VBIEDs and near-miss and direct hits of RAMs. These positions can be used around the FOB perimeter to enhance security and at ECPs for overwatch positions. These designs have been developed and tested by the U.S. Army Engineer Research and Development Center (ERDC). Test results indicate that the overhead cover provided will protect from direct hits of 81/82-mm mortar rounds and that the sidewalls of the positions will stop the fragmentation from near contact bursts of up to 120-mm mortar, 122-mm rocket and 155-mm artillery rounds.

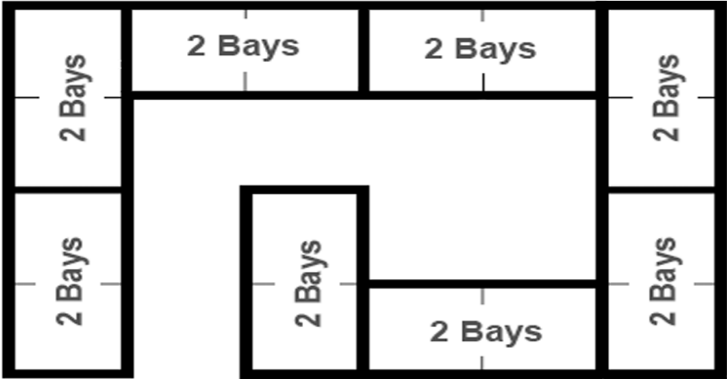
To assist in planning, estimates are provided for the necessary equipment, personnel assets and total construction time required to construct these positions. In many cases, multiple types of equipment are capable of performing the same task, and are listed as alternatives. Consideration during planning should be given to such issues as equipment and operator availability, topographic and work area limitations, maneuverability, etc., and their impact on the construction effort. Note that based upon parameters such as foundation type and source of fill material, certain tasks – and their associated equipment – may be unnecessary. Only heavy equipment is listed below. Hand tools such as shovels, rakes, pliers, wire cutters, etc. will also be needed.

The indicated time required for construction includes the time associated with basic foundation preparation and construction of the position. Factors such as threat based urgency, equipment and material availability, poor foundation soils, knowledge of construction techniques, etc. can greatly affect time requirements. Therefore, the time indicated is an estimate only, and should be utilized when actual performance data for similar positions under similar conditions is not available.

Annex D-1

Small Observation Post  
NSN 5680-01-501-1462

The material required to construct this position are available in a pre-assembled package (NSN 5680-01-501-1462). If the materials are not ordered as a package, use the bill of materials listed in the table below.



Section Layout

## Bill of Materials

Item Description	NSN	Quantity
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	30
Composite Material Panels (12 ft. length)	5675-01-500-2803	4
Composite Material Panels (8 ft. length)	5675-01-500-2729	3
Toggle connectors (12 ft. length)	Incl. in NSN 5675-01-500-2803	3
Waterproof membrane (16 ft. x 20 ft.)	5650-01-504-5373	1
Infill material (cubic yards)	N/A	24

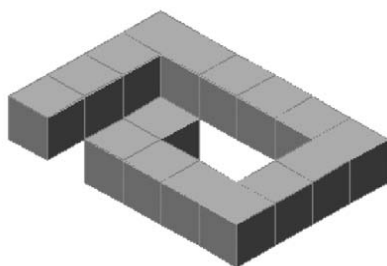
## Equipment, Personnel, and Time Estimate

Total Estimated Personnel Asset Requirements = 22 man-hours

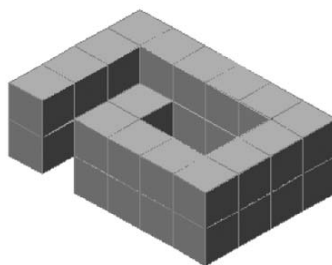
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect structure and place infill	front-end loader, skid-steer loader, SEE, HMEE	4	5 hr

1—Excludes equipment operators

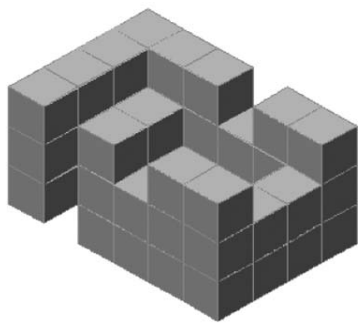
## General Construction Steps for Small Observation Post



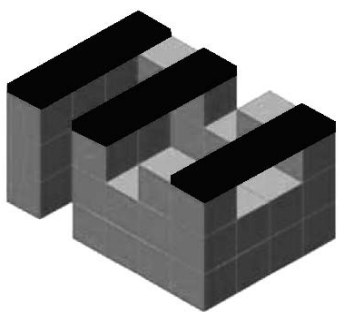
1. Place and fill first layer



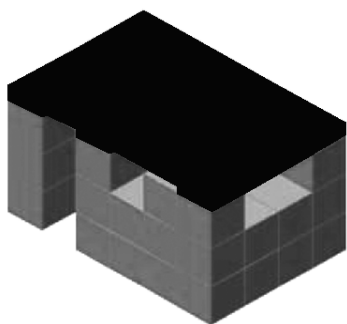
2. Place and fill second layer



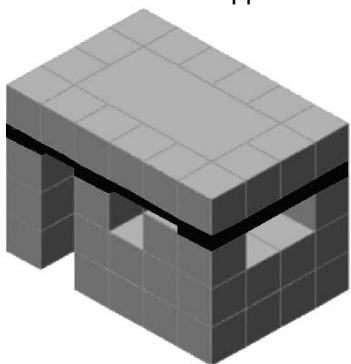
3. Place and fill third layer



4. Add roof support



5. Add roof layer

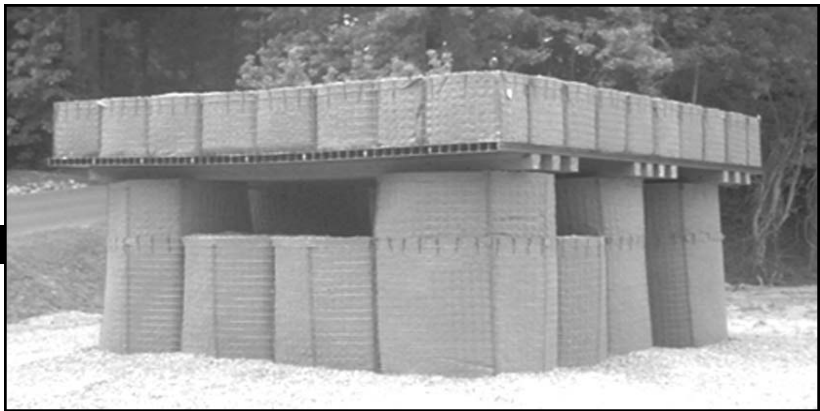


6. Add and fill overhead cover

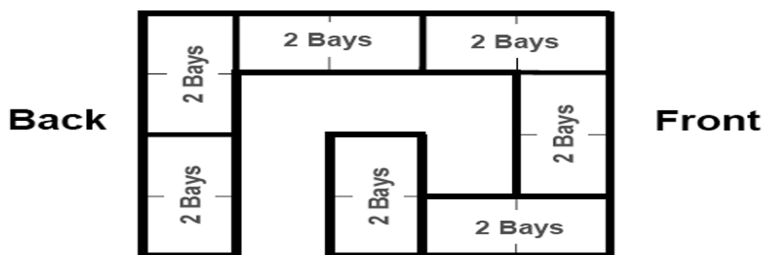
For additional details refer to *Construction Guide for Aboveground Small Observation Post* (available from USACE ERDC).

**Annex D-2**

**Large Observation Post  
(Wire and Fabric Container Version)**







## Section Layout

### Bill of Materials

Item Description	NSN	Quantity
Wire and Fabric Container (modified to 4.5 ft. H, 3.5 ft. W, 7 ft. L)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	7
Wire and Fabric Container (modified to 2 ft. H, 3.5 ft. W, 3.5 ft. L)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	6
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	16
Timbers (6 in. x 6 in. x 16 ft. length)	—	10
Composite Material Panels (20 ft. length)	5675-01-496-4896	8
Toggle connectors (20 ft. length)	Incl. in NSN 5675-01-496-4896	7
Waterproof membrane (16 ft. x 20 ft.)	5650-01-504-5373	1
Infill material (cubic yards)	N/A	70

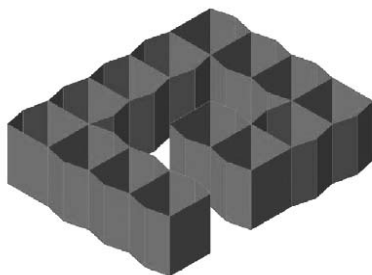
### Equipment, Personnel, and Time Estimate

Total Estimated Personnel Asset Requirements = 45 man-hours

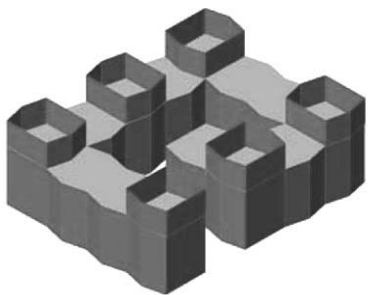
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	1 hr
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect structure and place infill	front-end loader, skid-steer loader, SEE, HMEE	6	7 hr

<sup>1</sup>—Excludes equipment operators

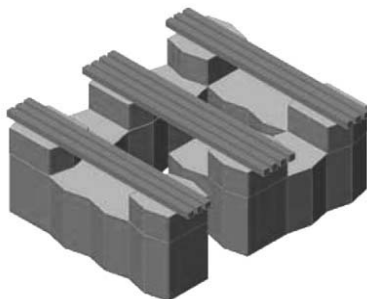
**General Construction Steps  
for Large Observation Post  
(Wire and Fabric Container Version)**



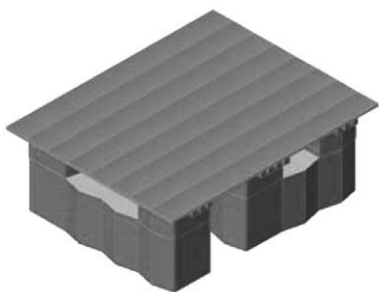
1. Arrange and fill first layer (section layout shown at right)



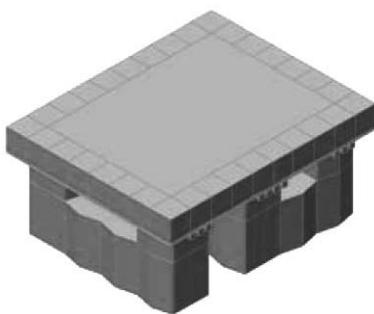
2. Arrange and fill second layer



3. Add timbers for roof support

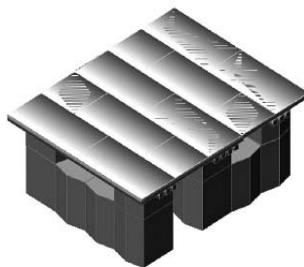
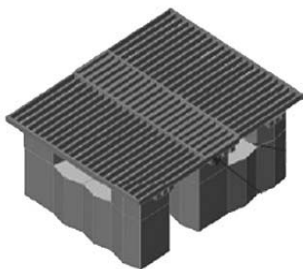


4. Add roof layer

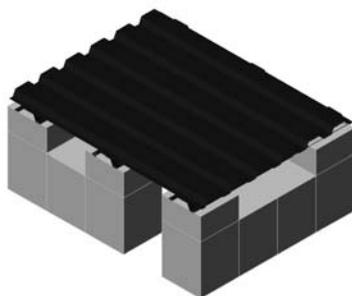


5. Arrange and fill overhead cover

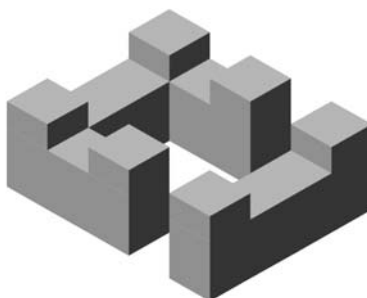
## Configuration Options:



Wooden Roof constructed with 2x6 timbers and 3/4" plywood



Sheet Pile Support and Roof constructed with sheet pilings



Entry Control Point or Guard House  
(modified layout for additional entrance)

For additional details refer to *Construction Guide for Aboveground Large Observation Post* (available from USACE ERDC).

Annex D-3

Large Observation Post  
(Metal Container Version)



Bill of Materials

Item Description	NSN	Quantity
Metal Revetment Protective Position Kit	Contact USACE ERDC	1
Steel Column – W8x10 (7'-1")	N/A	6
Steel Beam – W8x10 (18')	N/A	6
Steel Base Plate (3'x3'x1/2")	N/A	6
Steel Cap Plate (2'x2'x1/2")	N/A	6
Steel Angle (3"x3"x1/4"), 2-ft. long	N/A	12
Steel Angle (3"x3"x1/4"), 5-in. long	N/A	12
Composite Material Panel w/Toggle Connector, 22' long	5675-01-496-4896	9
Waterproof Membrane (18'x22')	5650-01-504-5373	1
Infill Material, cubic yard	N/A	70
Revetment Kit, 4'x8'x64' length	5450-01-535-7952	—
Revetment Kit, 2'x6'x104' length	5450-01-535-7955	—

## Bill of Materials (Continued)

Item Description	NSN	Quantity
Revetment Kit, 4'x10'x48' length	5450-01-537-7061	—
If individual kit components are not available, fashion the following kit pieces:		
16 Ga Side Panel, 2' H x 8' L	—	44
16 Ga End Panel, 2' H x 2' L	—	24
16 Ga End Panel, 2' H x 4' L	—	42
16 Ga Brace Panel, 2' H x 4' L	—	22
18 Ga Side Panel, 3' H x 4' L	—	24
18 Ga End Panel, 3' H x 4' L	—	8
2' Connecting Pin	—	190
3' Connecting Pin	—	30

The estimates of the necessary equipment and personnel assets required to construct this position are similar to those for the Wire and Fabric Version.

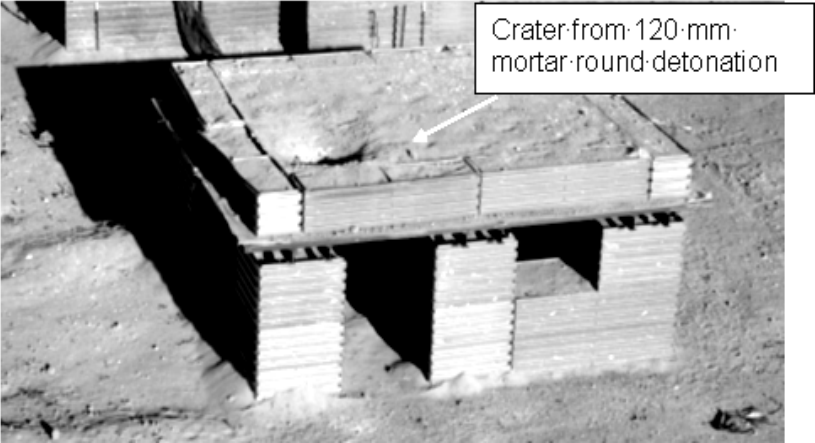
## Equipment, Personnel, and Time Estimate

Total Estimated Personnel Asset Requirements = 51 man-hours

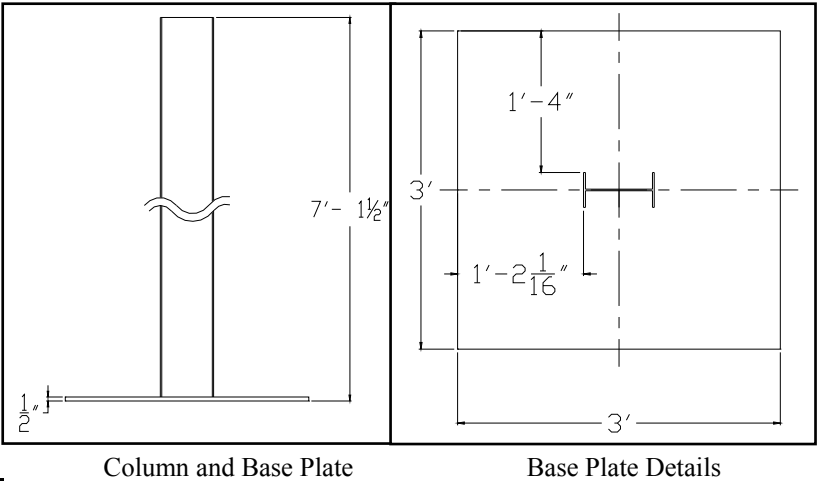
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	1 hr
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect structure and place infill	front-end loader, skid-steer loader, SEE, HMEE	6	8 hr

1—Excludes equipment operators

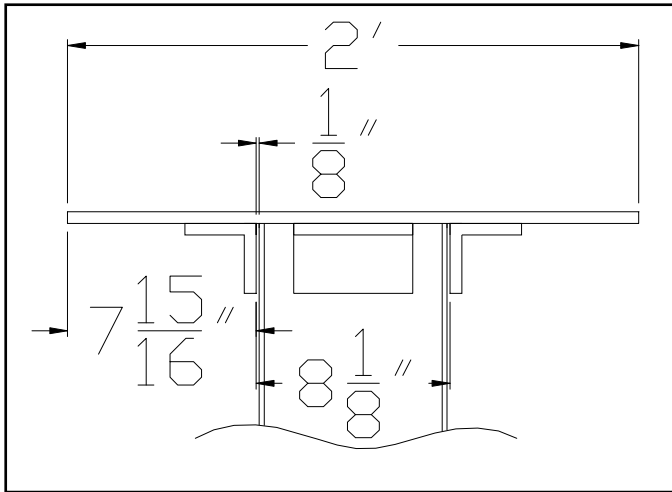
Results of static and live-fire tests conducted by the U.S. Army Engineer Research and Development Center (ERDC) have shown that this bunker design will protect from direct hits of 82-mm and 120-mm mortars and near-miss (4 ft.) of 122-mm rockets with no significant structural damage and no penetration of fragments through the sidewalls or roof.



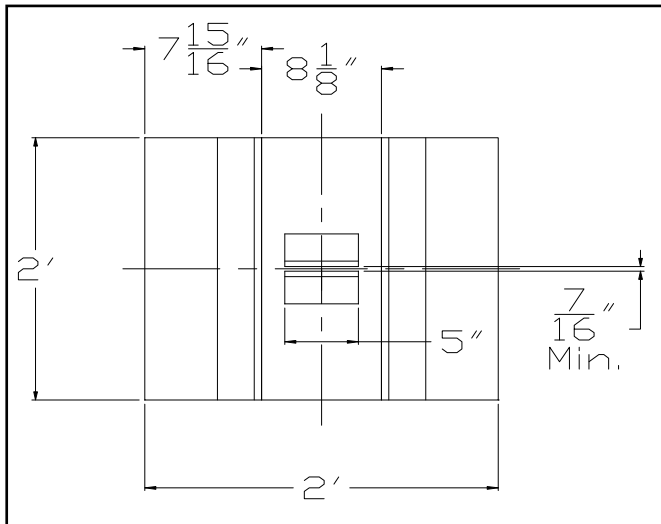
Six (6) columns are needed to construct this position. Fabricate using one (1) 3' x 3' x 1/2" plate and one (1) WBx10, 7'-1" length column. Fillet weld (minimum 3/16") all locations. Column and base plate steel details are shown below.



Six (6) cap plates are needed to construct this position. Fabricate using one (1) 2' x 2' x 1/2" plate, two (2) 3" x 3" x 1/2" 2-ft. angle iron, and two (2) 3" x 3" x 1/2" 5-in. length angle iron. Fillet weld (minimum 3/16") all locations. Cap plate details are shown below.

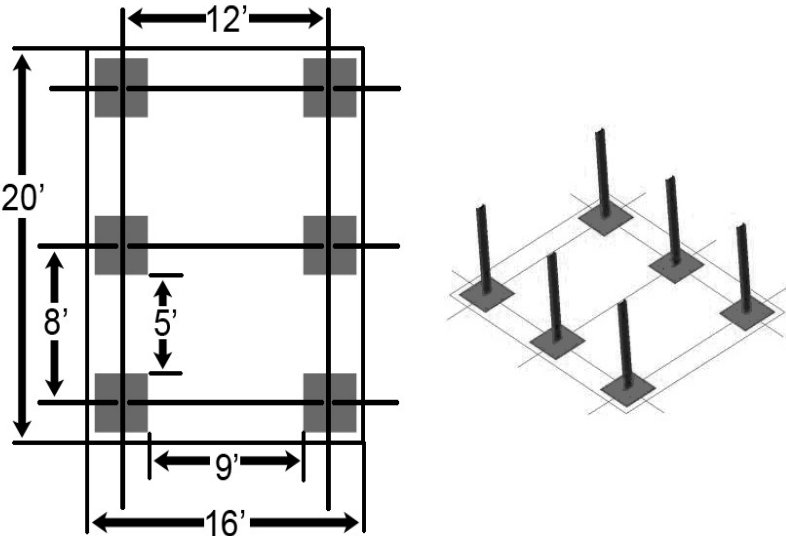


Cap Plate on Column

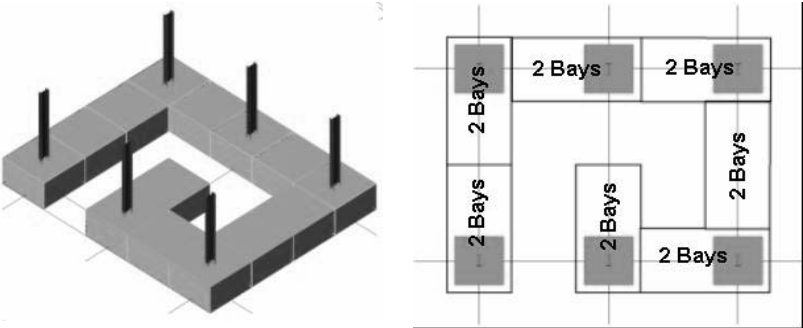


Cap Plate Details

General Construction Steps for Large Observation Post (Metal Container Version)

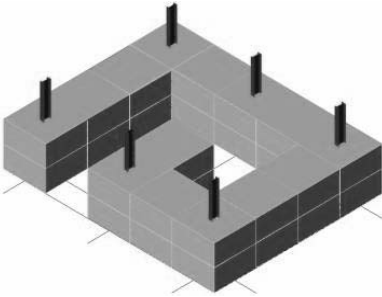


1. Level surface, locate, and place columns  
**Columns are very important for a stable structure!**

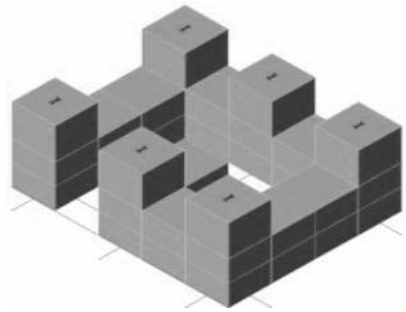


2. Arrange and fill first layer (section layout shown at right)

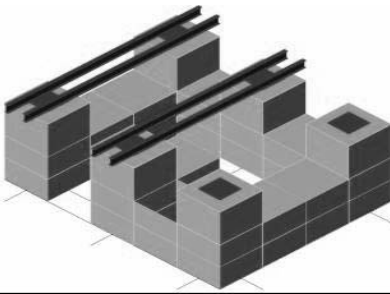




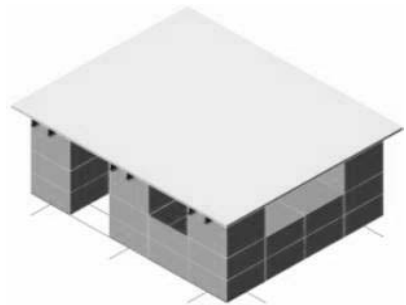
3. Arrange and fill second layer



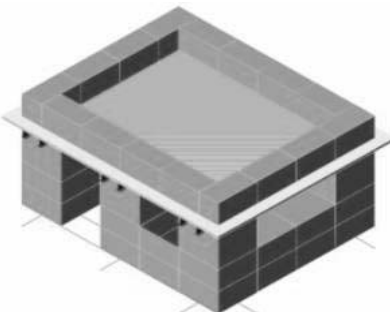
4. Arrange and fill third layer



5. Cap plates and add roof support



6. Add composite roof



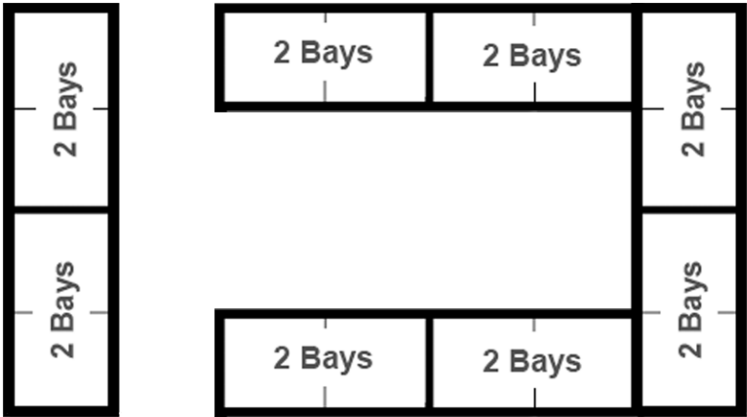
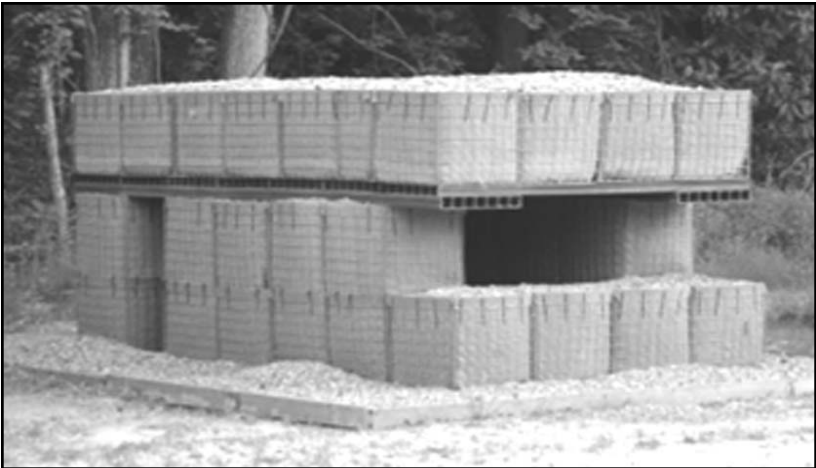
7. Arrange and fill overhead cover

For additional details refer to *Construction Guide for Aboveground Large Observation Post* (available from USACE ERDC).

Annex D-4

Aboveground Single-Bay Fighting Position  
NSN 5680-01-501-1235

The material required to construct this position are available in a pre-assembled package (NSN 5680-01-501-1235). If the materials are not ordered as a package, use the bill of materials listed in the table below.



Section Layout

## Bill of Materials

Item Description	NSN	Quantity
Wire/Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	23
Composite Material Panels (14 ft. length)	5675-01-500-2808	2
Composite Material Panels (8 ft. length)	5675-01-500-2729	7
Toggle connectors (8 ft. length)	Incl. in NSN 5675-01-500-2729	6
Waterproof membrane (8 ft. x 14 ft.)	5650-01-504-5373	1
Infill material (cubic yards)	N/A	20

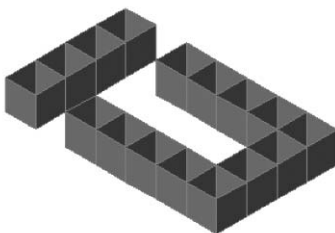
## Equipment, Personnel, and Time Estimate

Total Estimated Personnel Asset Requirements = 14 man-hours

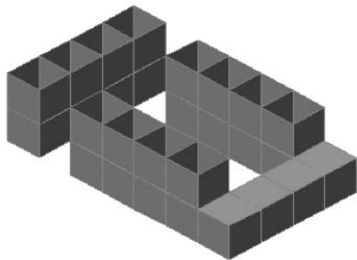
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect structure and place infill	front-end loader, skid-steer loader, SEE, HMEE	2	6 hr

1—Excludes equipment operators

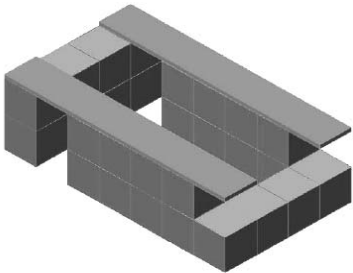
## General Construction Steps for Aboveground Single-Bay Fighting Position



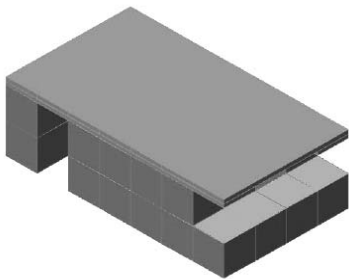
1. Arrange and fill first layer



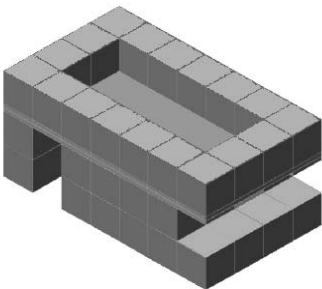
2. Arrange and fill second layer



3. Add roof support



4. Add roof panels



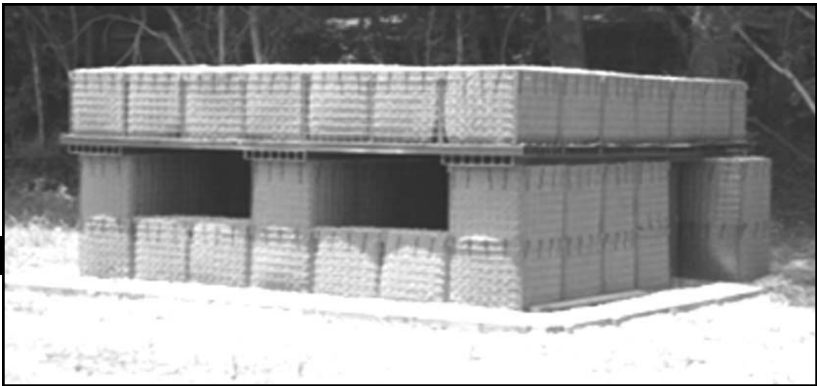
5. Add and fill overhead cover

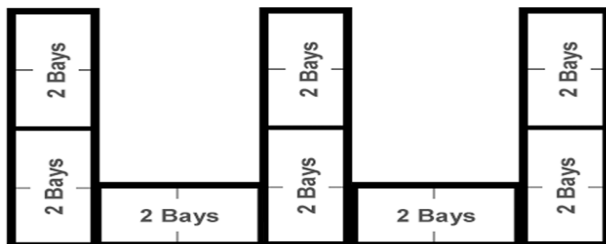
For additional details refer to *Construction Guide for Single-Bay Above-ground Fighting Position* (available from USACE ERDC).

**Annex D-5**

**Aboveground Two-Bay Fighting Position  
NSN 5680-01-501-1357**

The material required to construct this position are available in a pre-assembled package (NSN 5680-01-501-1357). If the materials are not ordered as a package, use the bill of materials listed in the table below.





## Section Layout

### Bill of Materials

Item Description	NSN	Quantity
Wire/Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	33
Composite Material Panels (14 ft. length)	5675-01-500-2808	6
Composite Material Panels (12 ft. length)	5675-01-500-2803	3
Toggle connectors (14 ft. length)	Incl. in 5675-01-500-2808	5
Waterproof membrane (14 ft. x 12 ft.)	5650-01-504-5373	1
Infill material (cubic yards)	N/A	30

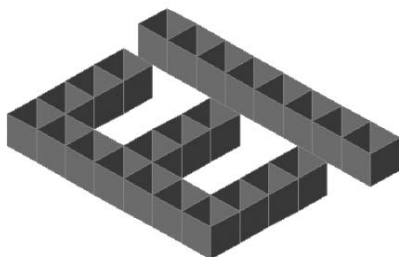
### Equipment, Personnel, and Time Estimate

Total Estimated Personnel Asset Requirements = 26 man-hours

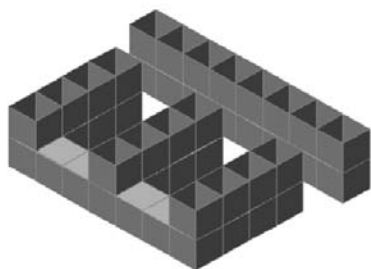
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, skid-steer loader, SEE, HMEE	2	30 min
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect structure and place infill	front-end loader, skid-steer loader, SEE, HMEE	4	6 hr

<sup>1</sup>—Excludes equipment operators

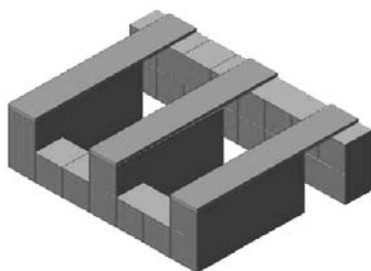
### General Construction Steps for Aboveground Two-Bay Fighting Position



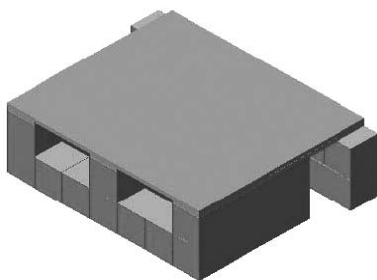
1. Arrange and fill first layer



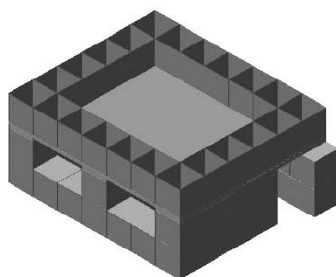
2. Arrange and fill second layer



3. Add roof support



4. Add roof panels



5. Add and fill overhead cover

For additional details refer to *Construction Guide for Two-Bay Aboveground Fighting Position* (available from USACE ERDC).

## Bunkers

These annexes provide descriptions and material requirements for several above- and below-ground personnel bunkers constructed with soil-filled wire and fabric containers. These bunker designs were developed and tested at the request of the Directorate of Training, U.S. Army Engineer School, Fort Leonard Wood, Missouri. Constructed properly, the bunkers in this section will protect from direct hits of 81/82-mm mortar rounds, and the sidewalls of the above-ground bunkers will stop the fragmentation from near-contact burst of up to 120-mm mortar, 122-mm rockets and 155-mm artillery rounds.

Overhead cover for each of the positions is composed of a roof system covered with 24 in. of fill material. Smaller roof systems are constructed with composite fiberglass material panels, and larger systems are constructed with steel sheet piling (See Figure D-12). Improvised roof systems can be used in the event the specified roof materials are not available. However, if improvised roof systems are utilized give close attention to ensure that they are adequately designed and properly constructed. Possible alternatives for the composite fiberglass roof materials include runway landing mats or wooden stringer roofs. When using wooden roofs, design and build them in accordance with the requirements stated in FM 5-103. For larger structures, sheet steel piling can not simply be replaced with wooden stringers! Improvised roof systems for these positions, will likely require steel beams to span the structure (a wooden roof deck could be used after placement of the steel beams). **It is especially critical that any improvised roof system be designed by a structural engineer to ensure it can safely carry the overhead cover.**

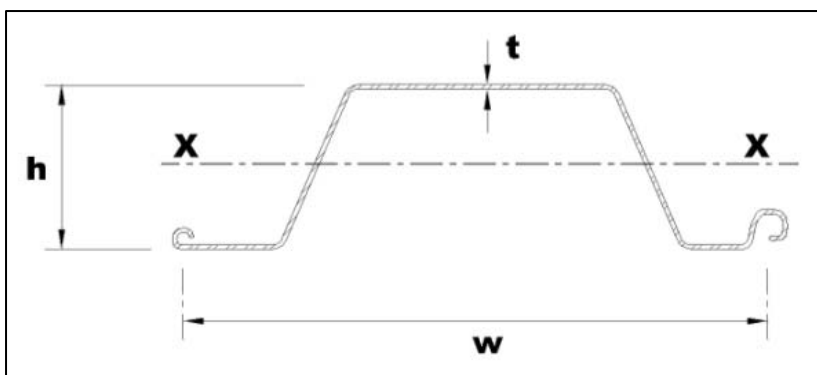


Figure D-12. Sheet Piling Material Requirements. Material is ASTM A572, Grade 50 steel. All piling should be primed and painted as required. Minimum Section Properties are Thickness ( $t$ ) = 0.2 in.; Height ( $h$ ) = 6 in.; Width ( $w$ ) = 27.5 in.; and X-axis section modulus ( $X$ ) = 6.3 cubic in/ft.

Planning estimates for materials and time are included here as they were in the Hardened Fighting and Observation Position section. Again, time indicated is an estimate only, and should be utilized when actual performance data for similar positions under similar conditions is not available.

Annex D-6

Aboveground 20 foot ISO/MILVAN  
Personnel Bunker



These bunkers are designed to provide protection for a standard 20 foot ISO/MILVAN container. This bunker requires sheet piling to construct the roof. If the piling used is of a different width than the specified dimensions, the required number of pieces in the BOM may change.

Bill of Materials

Item Description	NSN	Qty.
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	6
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	22
Sheet piling-18 ft. length (Skyline Steel CS 55 steel sheet piling or equivalent)	N/A	19
Sandbags Poly (Cloth or Acrylic material also available)	8105-00-142-9345 (Green) 8105-01-336-6163 (Sand)	100
Waterproof membrane (44 ft. x 18 ft.)	5650-01-504-5373	1
Infill material (cubic yards)	N/A	180



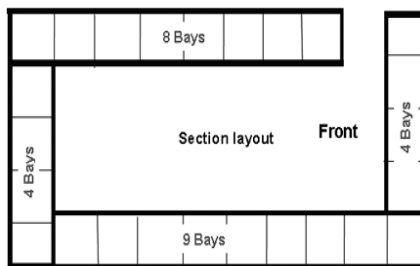
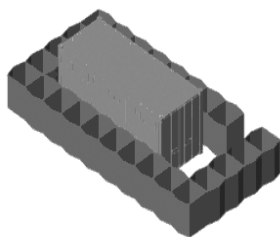
## Equipment, Personnel, and Time Estimate

Total estimated personnel asset requirements = 70 man-hours

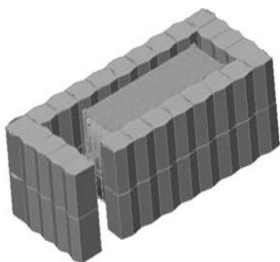
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, HMEE	2	1 hr
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Place ISO container	crane, forklift	2	30 min
Construct roof	front-end loader, HMEE	6	5 hr
Construct roof & place infill	forklift, crane (w/clamshell bucket for infill), HYEX	6	6 hr

1—Excludes equipment operators

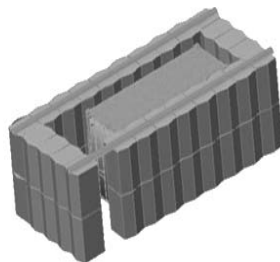
## General Construction Steps for aboveground ISO/MILVAN Personnel Bunker



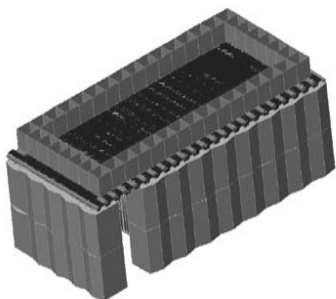
1. Arrange and fill first layer (section layout shown at right)



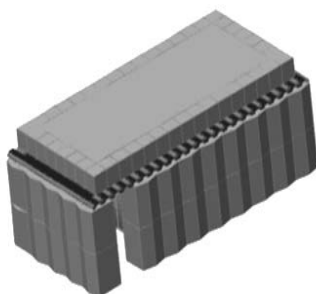
2. Arrange and fill second layer



3. Add sheet piling roof support



4. Add roof layer



5. Fill overhead cover

For additional details refer to *Construction Guide for Aboveground 20' Milvan Bunker* (available from USACE ERDC).

### Annex D-7

## HEMTT-LHS/PLS Bunker



These bunkers can be used to protect any equipment or materials that will fit inside.

HEMTT-LHS Bunker dimensions: 49 ft L x 28 ft. W x 16 ft. H

PLS Bunker dimensions: 32 ft. L x 21 ft. W x 14 ft. H

## Bill of Materials

Item Description	NSN	Quantity	
		HEMTT	PLS
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	18	5
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	31	40
Sheet piling-18 ft. length Skyline Steel CS 55 steel sheet piling or equivalent	N/A	19	13
Sandbags Poly (Cloth or Acrylic material also available)	8105-00-142-9345 (Green) 8105-01-336-6163 (Sand)	136	96
Waterproof membrane (44 ft. x 18 ft.)	5650-01-504-5373	1	1
Infill material (cubic yards)	N/A	470	170

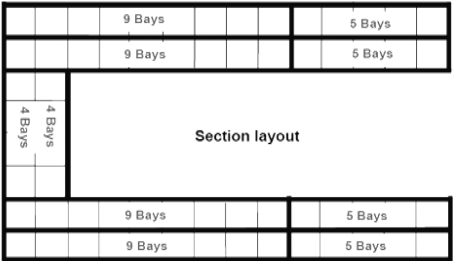
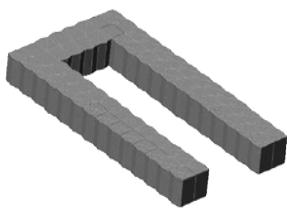
## Equipment, Personnel, and Time Estimate

Total estimated personnel asset requirements = 131 man-hours

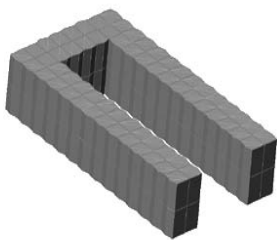
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, HMEE	2	1 hr
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 min
Haul infill material to site	dump trucks	varies	varies
Erect walls and place infill	front-end loader, HMEE (lower level), crane w/clamshell or HYEX (upper levels)	8	10 hr
Construct roof	crane, HYEX, front-end loader or HMEE (assist w/piling)	8	3 hr
Construct overhead cover	crane (w/clamshell bucket for infill), HYEX	8	3 hr

1—Excludes equipment operators

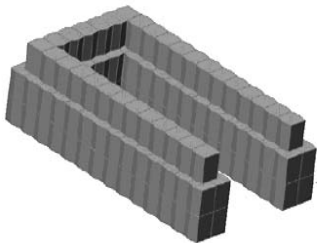
General Construction Steps  
for HEMTT-LHS/PLS Bunker



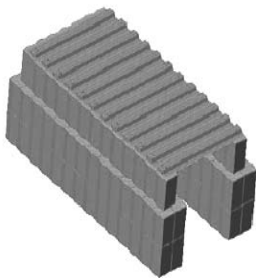
1. Arrange and fill first layer (section layout shown at right)



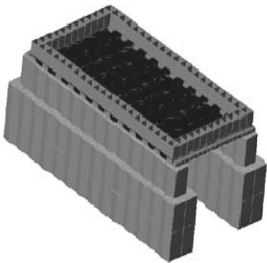
2. Arrange and fill second layer



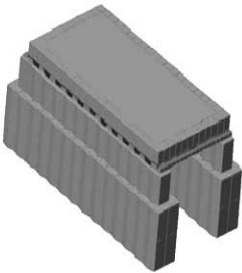
3. Arrange and fill third layer



4. Add sheet piling roof support



5. Add roof layer



6. Fill overhead cover

For additional details refer to *Construction Guide for HEMTT-LHS/PLS Bunker* (available from USACE ERDC).

## Annex D-8

### **Belowground 40 foot ISO/MILVAN Container Personnel Bunker**



An ISO container can be used to construct a below-ground personnel bunker IF THE CONTAINER IS REINFORCED WITH STEEL FRAMES to support the static soil loads and the dynamic loads from contact burst rounds on the bunker's soil cover. If the container is not reinforced, it may collapse under the static loads or from a weapon detonating on top, posing a serious hazard to personnel inside.

Material requirements, fabrication details, and time estimates are provided herein. The indicated time required for construction does not include fabrication times for the structural steel assemblies. If steel assemblies are not pre-fabricated, add the appropriate time and resources into the estimates provided (time estimates are provided for installing steel assemblies in the container).

**Bill of Materials—Revetment Walls and Roof**

Item Description	NSN	Qty.
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	4
Wire and Fabric Container (2 ft. x 2 ft. x 4 ft.)	5680-99-001-9397 (Green) 5680-99-968-1764 (Sand)	4
Composite Material Panel 10 ft. L	5675-01-500-2671	6
Toggle connector 10 ft. length	Incl. in NSN 5675-01-500-2671	5
Sandbags Poly (Cloth or Acrylic material also available)	8105-00-142-9345 (Green) 8105-01-336-6163 (Sand)	20

**Bill of Materials—Structural Steel Assembly**

Item Description	Quantity
TS 3 x 3 x 3/16" steel frame (min. yield stress= 50 ksi)	20
2" x 1/4" flat bar, 20'-3" length (min. yield stress= 50 ksi)	8
2" x 1/4" flat bar, 6'-4" length (min. yield stress= 50 ksi)	8
3-1/2" x 3-1/2" x 1/4" "L", 19'-6" length (min. stress yield= 50 ksi)	4
3/8" dia. Bolts, 4-1/2" long, 1-1/2" thread length min w/self-locking nuts	80
Plate washers, 7/16" I.D., 1-1/4" O.D., 1/8" thick	16
3/8" dia. Lag screws, 1-1/2" long	38

**Equipment, Personnel, and Time Estimate**

Total estimated personnel asset requirements = 49 man-hours

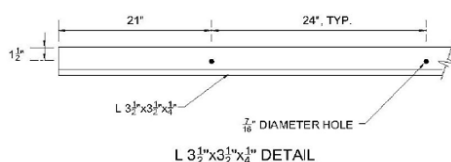
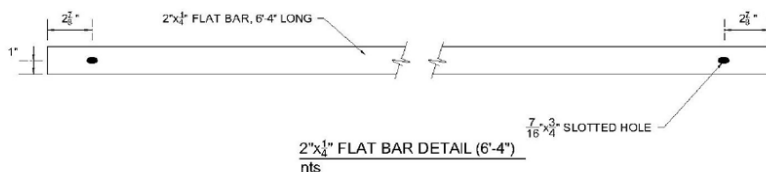
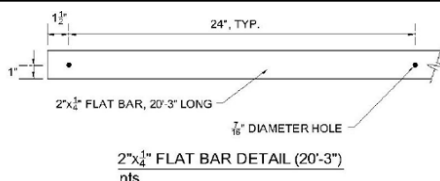
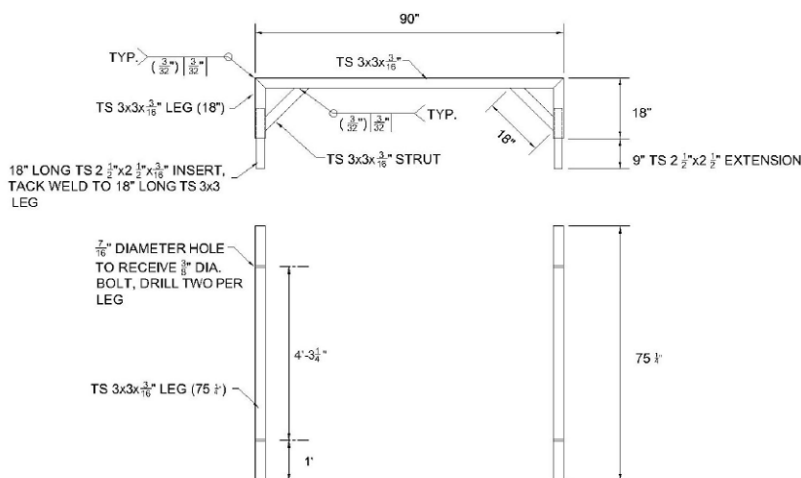
Task	Equipment Required	Personnel Required <sup>1</sup>	Time Required
Install steel assemblies in container	-	4	4 hr
Position excavation	HYEX	1	4 hr
Place ISO container	crane	2	30 min
Erect and fill revetment walls	HYEX	6	3 hr
Place and cover roof panels	HYEX	6	1 hr
Backfill position	HYEX	1	4 hr

<sup>1</sup>—Excludes equipment operators

## Frame Fabrication Details

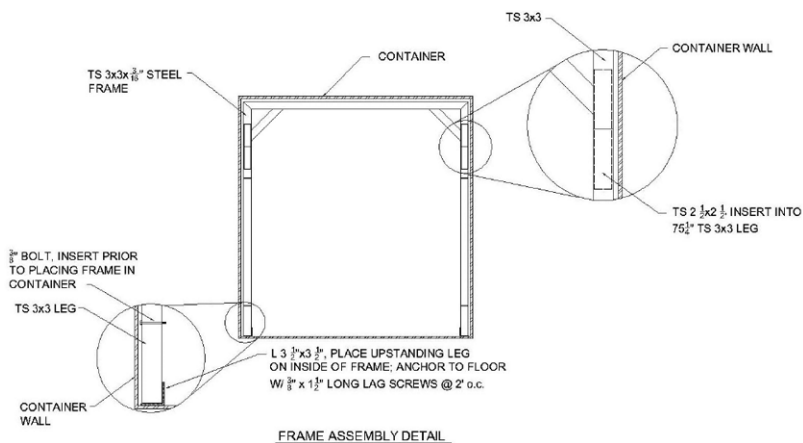
Steel frames are fabricated in 3 pieces, and can either be assembled in the container before shipping, or assembled upon arrival to final destination.

Reference detail below for frame fabrication requirements. Note that this frame configuration is based upon a standard 8 ft. wide, 8 ft. tall container.



## Steel Frame Assembly and Installation

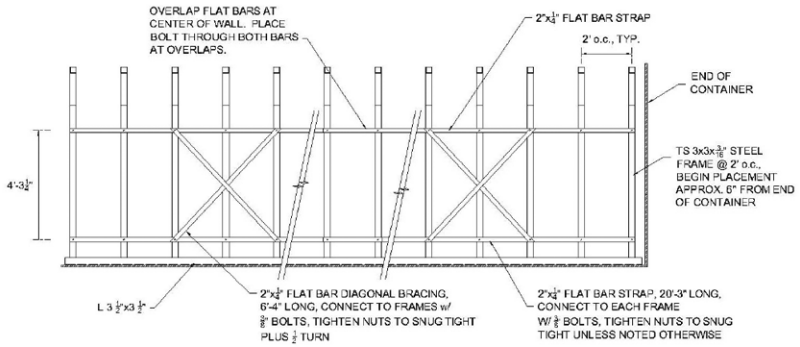
- Place two L 3-1/2 in. angles end-to-end on floor along each wall. Place angle with upstanding leg on inside of frame. Anchor angle to floor with 3/8 in. lag screws at 2 ft o.c. (Ensure anchor placement will not interfere with frames).
- Assemble steel frame by inserting 9 in. long TS 2-1/2 in. x 2-1/2 in. extensions into 75-1/4 in. long TS 3 x 3 legs. Place legs of frame into track formed between L3-1/2 in. angle and container wall (Note that 3/8 in. bolts must be inserted into frame legs prior to placing frame in container).



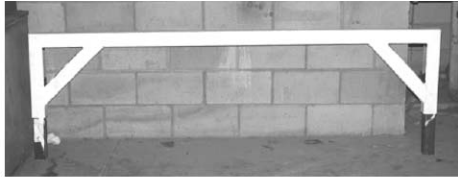
- Install assembled frames at 2 ft o.c. Begin frame placement approximately 6 in. from end of container.
- Connect (2) 20 ft-3 in. long flat bar straps to each frame with 3/8 in. bolts and self-locking nuts. Bolts must be inserted into frame legs prior to placing frame into container. Adjust frame placement as necessary to connect each frame to straps. Overlap straps 2 ft-3 in. at center of wall.
- Place 2 sets of 6 ft-4 in. flat bar diagonal bracing on each wall. Connect bracing to frames with 3/8 in. bolts, plate washers, and self-locking nuts.



# Soil-Filled Container Applications



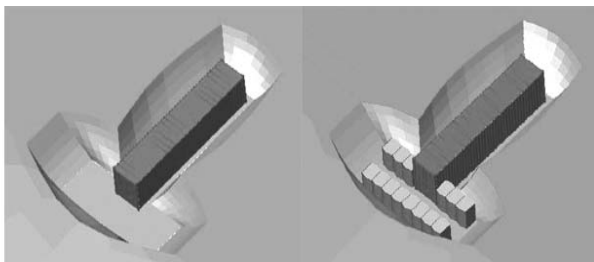
FRAME INSTALLATION DETAIL



Steel Frame assembly and Installation (clockwise from top: Upper portion of frame; Frames installed at 2' o.c.; Flat bar strips attached to frames; Flat bar connected to frame with bolt-- note head of bolt is on outside of frame; diagonal bracing in place)

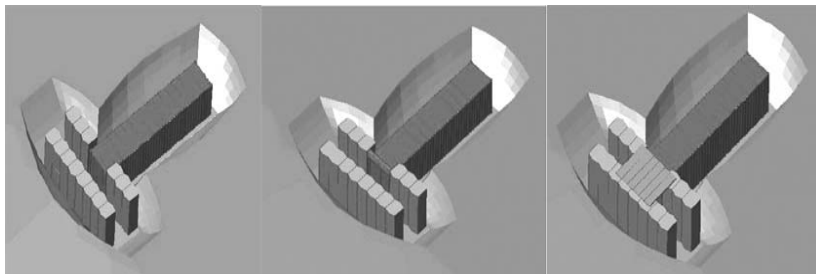
## General Construction Steps for Belowground ISO/MILVAN Container Bunker

Steps 1-2:  
Fabricate,  
assemble, and  
install reinforcing  
frames



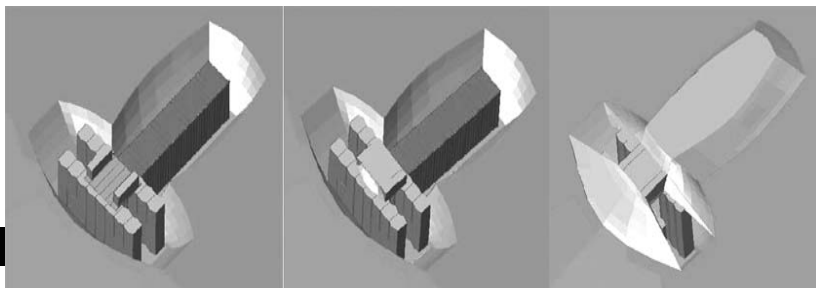
3. Excavate site and  
place container

4. Place and fill 1st re-  
vetment layer



5. Place and fill 2nd  
revetment layer

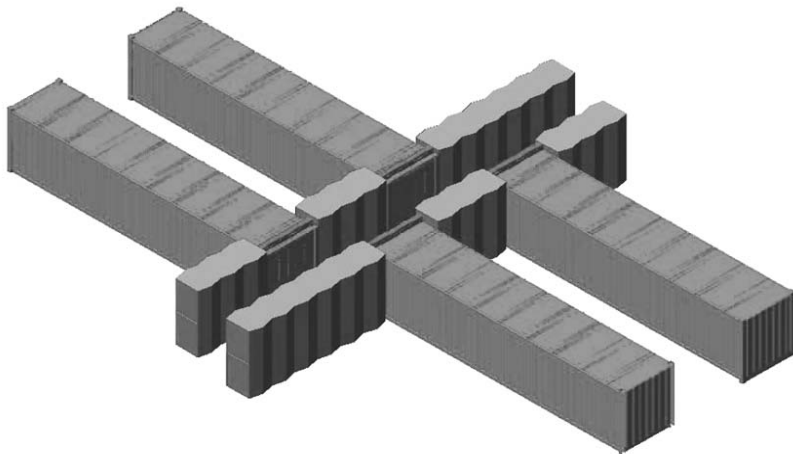
6. Level roof support and place composite  
panels on revetment walls



7. Add roof overhead cover

8. Backfill position

- Complete bunker by backfilling void space around container, and placing 4 ft. of soil on top of container. Ensure internal steel framework is properly installed prior to backfilling.
- When placing fill, ensure only 2 ft. of cover is placed on fiberglass roof.
- Camouflage position as appropriate.
- Ensure adequate air supply for personnel in shelter.
- No open flames allowed inside of bunker (possibility of carbon monoxide poisoning).



## Bunker Complex

In the event it is necessary to provide multiple bunkers in close proximity, a bunker complex can be established in the fashion indicated above. Each ISO/MILVAN container will have to be reinforced with steel frames as previously described. Note that the roof panels and soil cover are not shown in this illustration for clarity.

For additional details refer to *Construction Guide for Reinforced Below-ground 40' Milvan Bunker* (available from USACE ERDC).

**Annex D-9****Helicopter Revetments**

Revetments can also be used to protect open stores of material and equipment (See Figure D-13). This annex provides information on using soil-filled wire and fabric container revetments for making protective enclosures. These structures are designed to compartmentalize and protect helicopters from near-miss of RAMs, although they could be used for any storage that does not require overhead cover. These designs were developed by the ERDC and the Directorate of Training, U.S. Army Engineer School.

The indicated time required for construction includes the time associated with basic foundation preparation and construction of the position. Factors such as threat-based urgency, equipment and material availability, poor foundation soils, knowledge of construction techniques, etc. can greatly impact time requirements. Therefore, the time indicated is an estimate only and should be utilized when actual performance data for similar positions under similar conditions are not available.

Metal containers of similar sizes can also be used to construct these revetments. However, required quantities of materials may differ from the listed bills of materials. This is a result of different available dimensions for the equivalent metal containers. Plan for their construction accordingly.

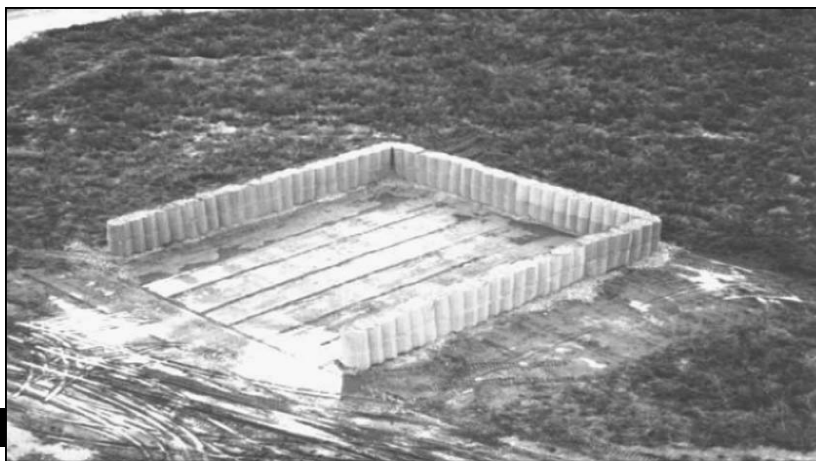


Figure D-13. Typical helicopter revetment

Bill of Materials for Various Soil-Filled Wire and Fabric  
Helicopter Revetments

Item Description	NSN	AH-64/ UH-60 Apache/ Black- hawk	OH-58 Kiowa Warrior	AH-1 Cobra	UH-1 Iroquois (Huey)	CH-47 Chinook	CH-53 Super Stallion
Wire and Fabric Container (4.5 ft. x 3.5 ft. x 32 ft.)	5680-99-001-9396 (Green) 5680-99-835-7866 (Sand)	16	11	14	14	11	11
Wire and Fabric Container (7.5 ft. x 7 ft. x 91 ft.)	5680-99-126-3716 (Green) 5680-99-169-0183 (Sand)	---	---	---	---	4	4
Infill material (cubic yards)	N/A	340	230	300	290	1000	1000

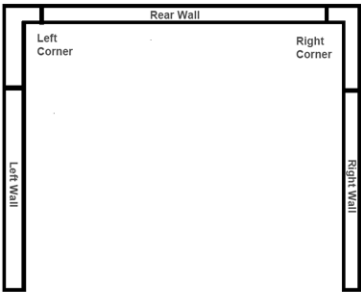
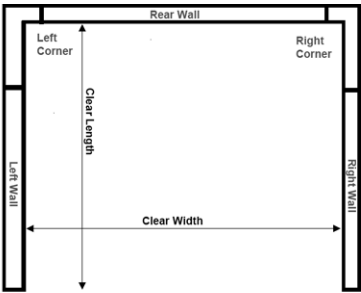
**Equipment, Personnel and Time Estimates**

Aircraft	Task	Equipment Req'd.	Personnel Req'd. (excluding operators)	Time Req'd.
AH-64 Apache/ UH-60 Blackhawk	1	A	2	45 min
	2	B	varies	varies
	3	C	8	8 hr
OH-58 Kiowa Warrior	1	A	2	30 min
	2	B	varies	varies
	3	C	6	8 hr
AH-1 Cobra	1	A	2	45 min
	2	B	varies	varies
	3	C	8	7 hr
UH-1 Iroquois (Huey)	1	A	2	45 min
	2	B	varies	varies
	3	C	8	7 hr
CH-47 Chinook	1	A	2	1 hr 30 min
	2	B	varies	varies
	3	D	10	16 hr
CH-53 Super Stallion	1	A	2	1 hr 30 min
	2	B	varies	varies
	3	D	10	16 hr
<p><b>KEY:</b></p> <p><b>Task:</b></p> <ol style="list-style-type: none"> <li>1. Prepare site and level foundation</li> <li>2. Haul infill material to site</li> <li>3. Erect walls and place infill</li> </ol> <p><b>Equipment Required:</b></p> <ol style="list-style-type: none"> <li>A. Bulldozer, DEUCE, ACE</li> <li>B. Dump Trucks</li> <li>C. Front-end loader, HMEE</li> <li>D. Front-end loader w/clamshell bucket, HYEX</li> </ol>				

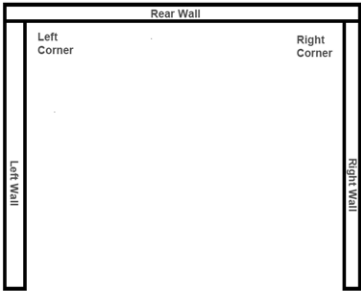
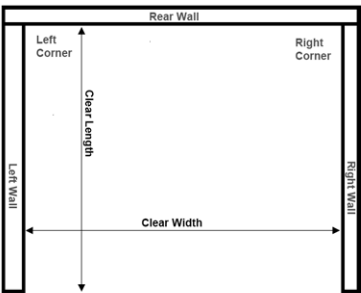
Layout Dimensions for Various Helicopters

Helicopter	Wire and Fabric Container Size	Quantity	Length (ft)	Width (ft)
Blackhawk/Apache	4.5 x 3.5 x 32 ft.	16	82	78
Kiowa	4.5 x 3.5 x 32 ft.	11	53	57
Cobra	4.5 x 3.5 x 32 ft.	14	78	64
Iroquois (Huey)	4.5 x 3.5 x 32 ft.	14	67	71
Chinook	7.25 x 7 x 91 ft.	4	126	91
2 <sup>nd</sup> layer	4.5 x 3.5 x 32 ft.	11	—	—
Super Stallion	7.25 x 7 x 91 ft.	4	112	112
2 <sup>nd</sup> layer	4.5 x 3.5 x 32 ft.	11	—	—

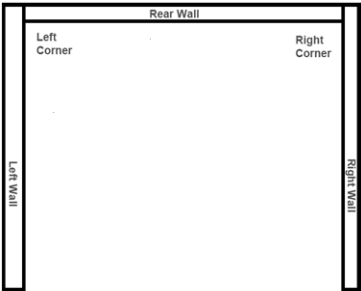
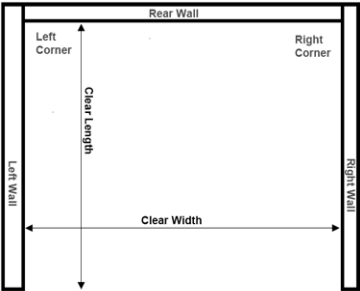
**Section Layouts.** Aircraft currently in use constitute a broad range of sizes and configurations. Specific layouts differ for each type of aircraft and are provided below.



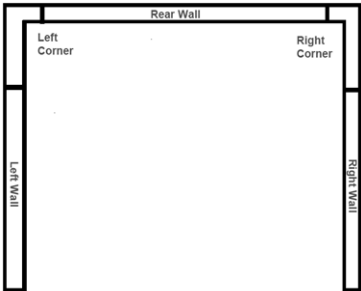
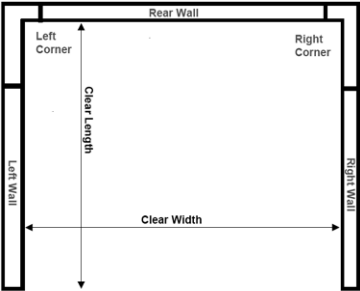
AH-64 Apache/ UH-60 Blackhawk  
(left: first layer; right: second layer)



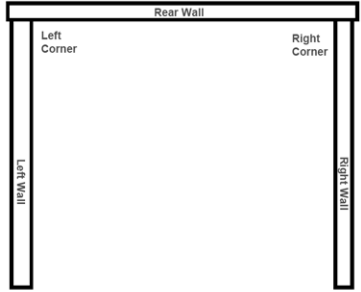
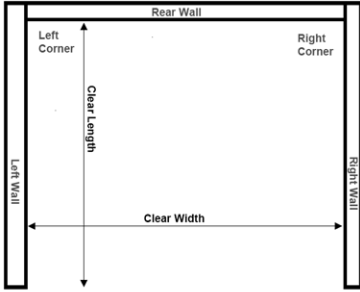
OH-58 Kiowa (left: first layer; right: second layer)



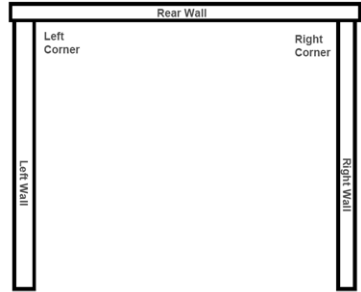
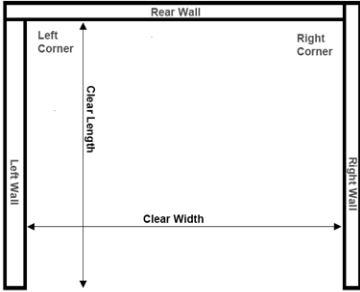
AH-1Cobra (left: first layer; right: second layer)



UH-1 Iroquois "Huey" (left: first layer; right: second layer)



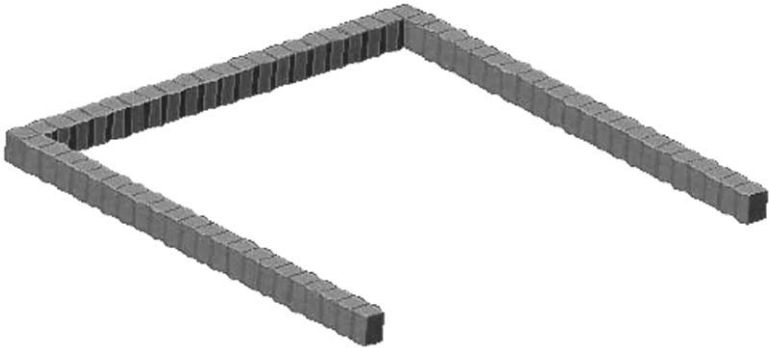
CH-47 Chinook (left: first layer; right: second layer)



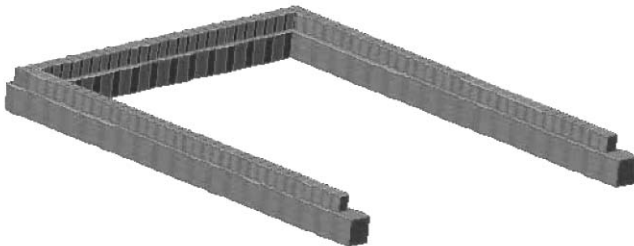
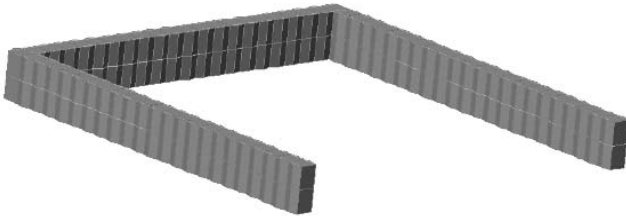
CH-53 Super Stallion (left: first layer; right: second layer)



## General Construction Steps for Helicopter Revetments)



1. Arrange and fill first layer



2. Arrange and fill second layer (above: Apache, Blackhawk, Kiowa, Cobra, Huey; below: Chinook and Super Stallion)

For additional details refer to *Construction Guide for Helicopter Revetment* (available from USACE ERDC).

## Resources

The following references are available from the Survivability Engineering Branch, Geotechnical and Structures Laboratory, U.S. Army Engineer Research and Development Center (ERDC). Most can be accessed on ATEP (<https://atep.dtic.mil>) or in the reference section of the JAT Guide. Contact ERDC ([GSL-Info@erdc.usace.army.mil](mailto:GSL-Info@erdc.usace.army.mil)) for further information.

*Concertainer® Construction Techniques*, May 2003.

*Executive Summary of Investigation & Field Verification of Metal Revetments Systems Subjected to 120mm Mortar & 122mm Rocket*, November 2004.

*Construction Guide for Helicopter Revetment (Apache, Blackhawk, Kiowa Warrior, Cobra, Huey, Chinook, Super Stallion)*, May 2003

*Overview and Summary of Results for Experimental Validation of Compartmentalization Measures for High Troop Concentration Facilities in U.S. Base-camps*, February 2005.

*ERDC Compartmentalization Techniques*, December 2004.

*Investigation and Field Verification of Fragment Protection from various RAM Threats*, July 2004.

*Executive Summary of Investigation & Field Verification of Fragment Protection from 82mm & 120mm Mortars*, October 2004.

*Quick Look Report: Pre-Detonation and Fragment Shielding Experiments for Rocket, Artillery, and Mortar (RAM) Threats*, September 2004.

*Overhead Protection Design Process*, December 2004.

*Quick Look Report: Phase III - Pre-Detonation and Fragment Shielding Experiments for 60-mm, 82-mm & 120-mm mortar (RAM) Threats*, November 2004.

*Fact Sheet: Field Expedient Protective Positions*, June 2003.

*Construction Guide for Aboveground 20' Milvan Bunker*, May 2003.

*Construction Guide for Reinforced Belowground 40' Milvan Bunker*, May 2003.

*Construction Guide for HEMTT-LHS/PLS Bunker*, May, 2003.

*Construction Guide for Two-Bay Aboveground Fighting Position*, May 2003.

*Construction Guide for Single-Bay Aboveground Fighting Position*, May 2003.

*Construction Guide for Aboveground Large Observation Post*, May 2003.

*Metal Revetment Protective Position Construction Guide*, June 2005.

*Metal Revetment Assembly Construction Guide*, November 2005.

*Construction Guide for Small Observation Post*, May 2003.

## Appendix E

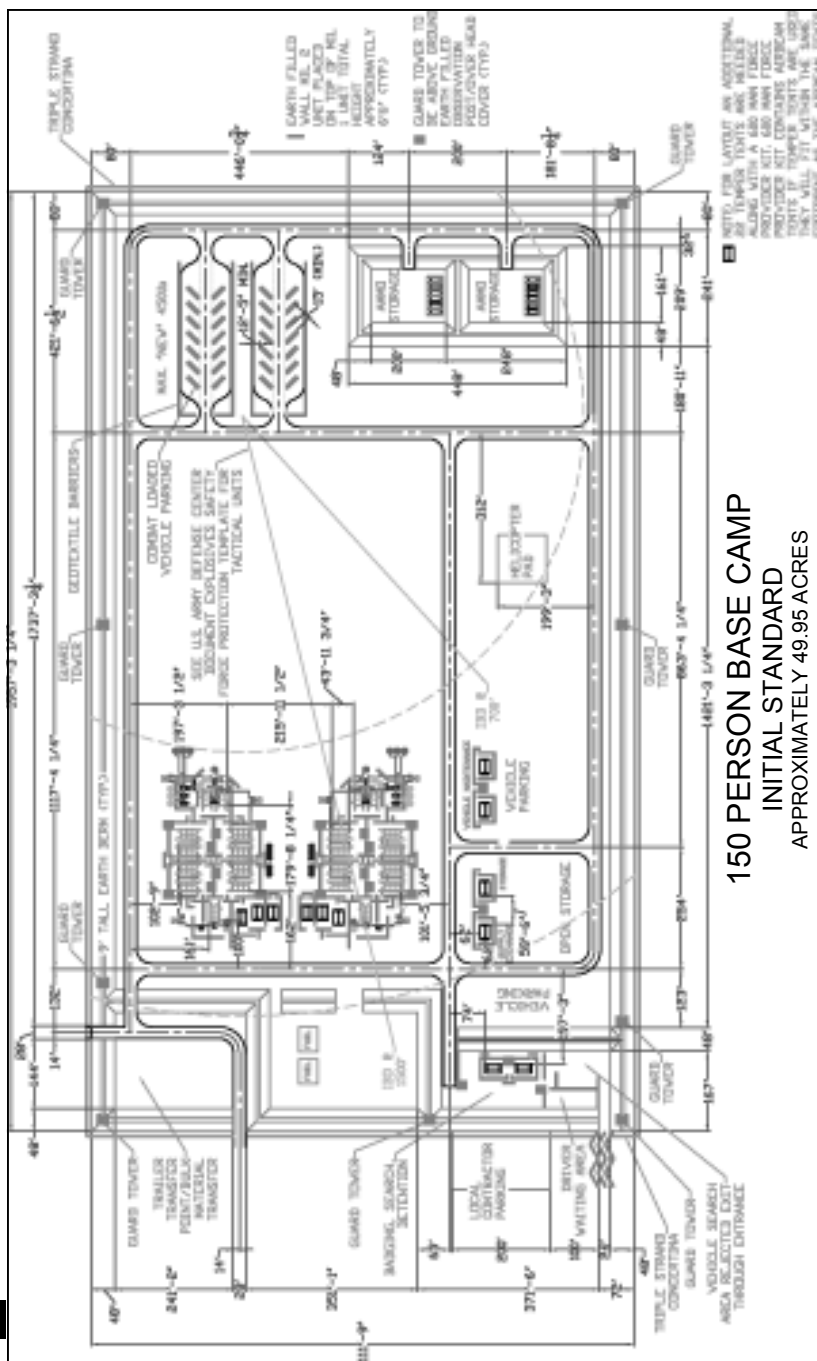
# Tent Camp Layouts

This appendix contains a set of conceptual site layouts for 150- and 600-person tent camps that link technology and material solutions to TTPs. This graphic representation (See Figures E-1 through E-4) provides the visual integration of risk mitigation capability into a single product that facilitates protective planning and execution. A digital version of these drawings can be found on the Antiterrorism Enterprise Portal (ATEP) at <https://atep.dtic.mil>. These drawings are also available from the Theater Construction Management System (TCMS) program at USACE, Huntsville, Alabama (<http://www.tcms.net>).

**Tent-Camp Concept Background and Assumptions.** In providing a configuration for a 150-person or more camp, it is impractical to make a “one-size fits all” layout. Therefore, the figures in this chapter provide a conceptual layout for camp components. The layouts are meant to be **descriptive and not restrictive**. In other words, the threat, the location, amount of materials, force protection analyses, and other factors will determine the best layout of camp components (housing, power production, water treatment, etc.).

In reviewing these layouts, the user may make certain adjustments as necessary as long as force protection is not compromised. For instance, parking spaces for vehicle maintenance or spaces near the BDOC can be made smaller or larger depending on the situation.

Materials required for construction of these tent camps are detailed in the TCMS program. The bunkers surrounding the high occupancy areas of the camp are a modified version of the Aboveground Small Observation Post (NSN: 5680-01-501-1462; See Appendix D). Observation windows will not be used in the “bunker” configuration and should be replaced with additional 2x2x4 Soil-filled wire and fabric containers. Each soil-filled wire and fabric barrier wall is comprised of 2x2x4 ft. (See Figure E-5) or 4x3x32 ft. units (See Figure E-6). Together, the units are stacked on top of each other to create a 6.5 foot tall barrier.



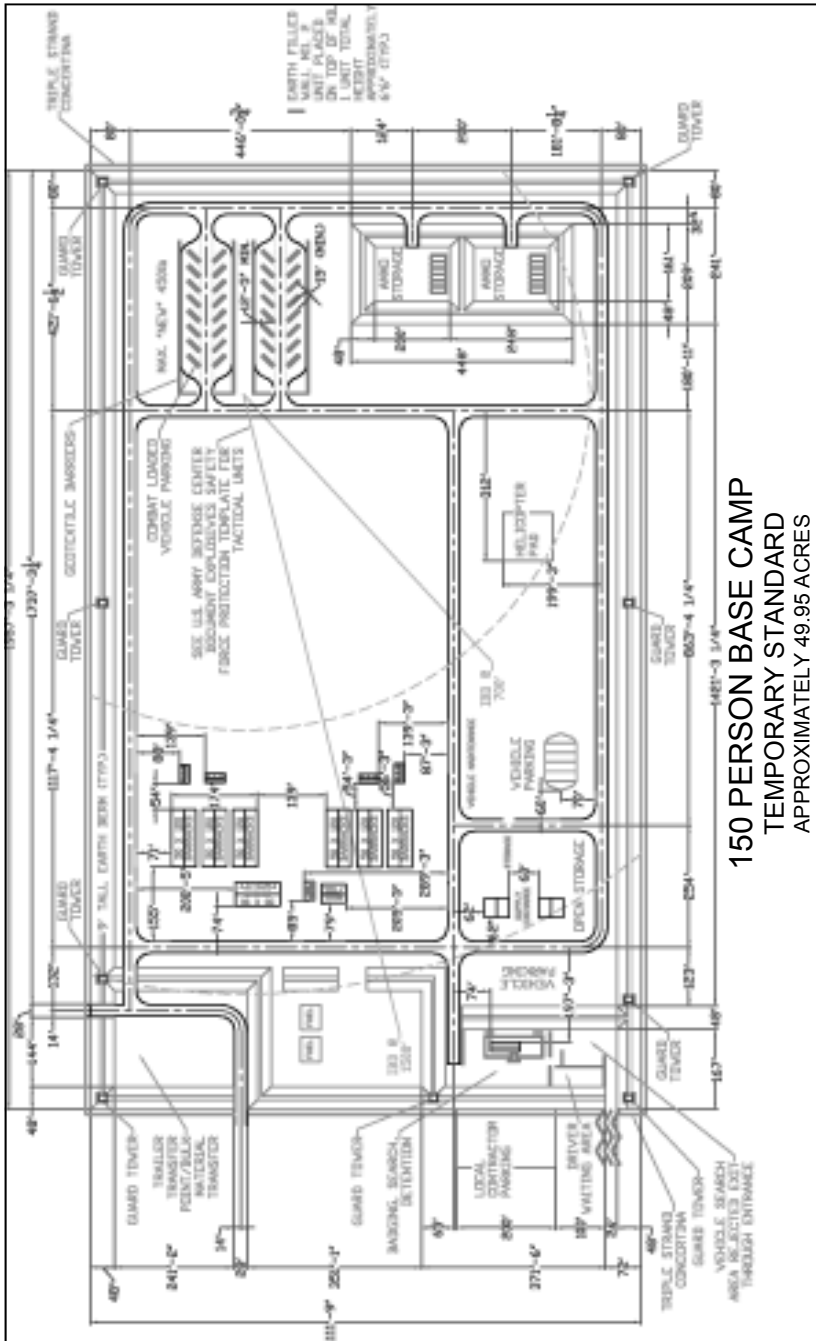


Figure E-2. 150 Person Tent Camp—Temporary Standard



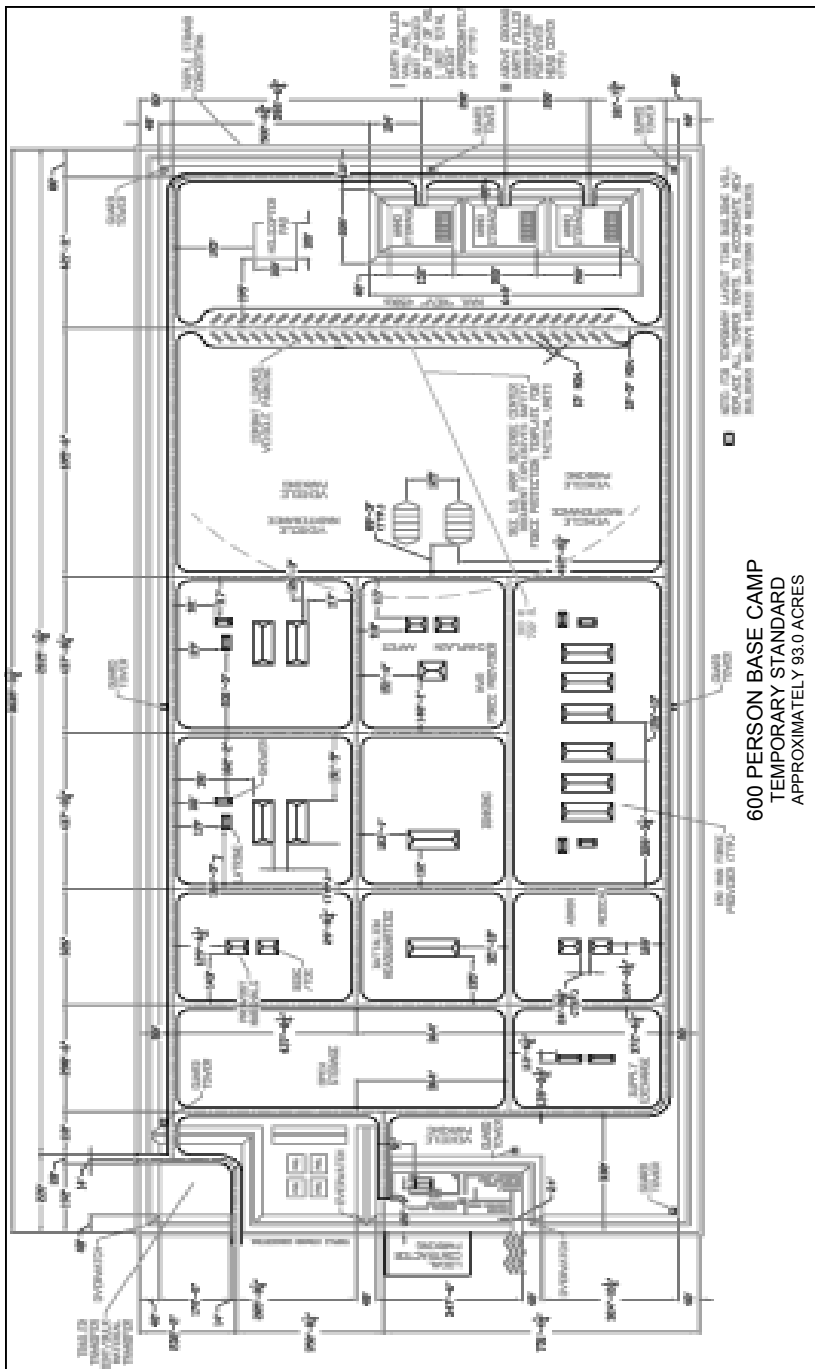


Figure E-4. 600 Person Tent Camp—Temporary Standard

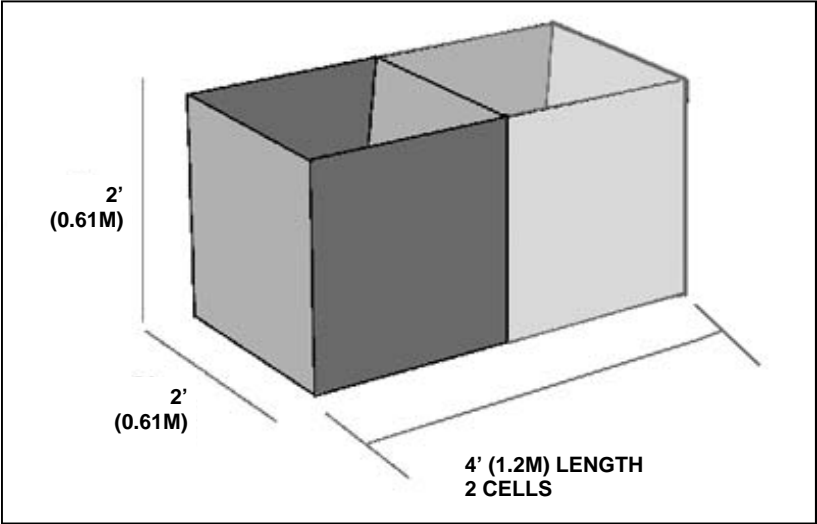


Figure E-5. 2x2x4 Ft. Wire and Fabric Soil-Filled Barrier Unit

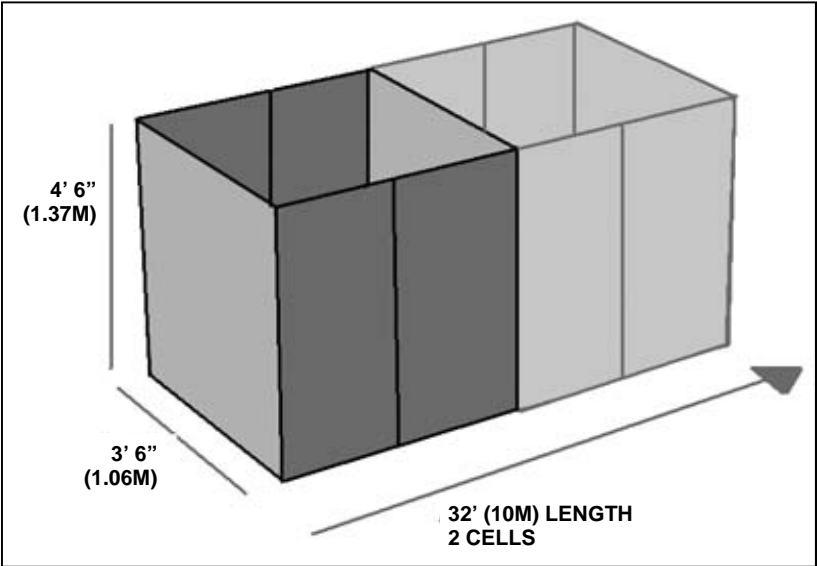


Figure E-6. 4x3x32 Ft. Wire and Fabric Soil-Filled Barrier Unit



## Appendix F

# References

### Department of Defense

*Defense Federal Acquisition Regulation Supplement: The 1998 Edition* (including DACs 91-1 through 91-13 and Departmental Letters 98-001 through 98-021), 17 August 1998 (updated 20 October 2008). (available at <http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>)

DoDI 2000.16. *DoD Antiterrorism (AT) Standards*, 2 October 2006 (including Change 2, 8 December 2006).

DoDI 3020.45. *Defense Critical Infrastructure Program (DCIP) Management*, 21 April 2008.

DoD O-2000.12-H. *DoD Antiterrorism Handbook*, February 2004.

*National Defense Strategy*. Washington DC: Department of Defense, June 2008.

*The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington DC: Joint Chiefs of Staff, 2004.

### Chairman of the Joint Chiefs of Staff

CJCSI 3470.01. *Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution*, 15 July 2005 (Current as of 9 July 2007).

CJCSI 5261.01E. *Combating Terrorism-Readiness Initiative Fund (CbT-RIF)*, 27 April 2007.

CJCSI 7401.01C. *Combatant Commander Initiative Fund (CCIF)*, 15 August 2007.

CJCSM 3122.01. *Joint Operation Planning and Execution System (JOPES) Volume I (Planning Policies and Procedures)*, 14 July 2000 (w/ Change 1, 25 May 2001).

CJCSM 3122.02C. *Joint Operation Planning and Execution System*

*(JOPES) Volume III (Crisis Action Time-Phased Force and Deployment Data Development and Deployment Execution)*, 22 March 2004.

CJCSM 3122.03A. *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance*, 31 December 1999 (w/Change 1, 6 September 2000).

## **Joint Publications**

*Contingency Contracting: A Joint Handbook* (YFV 08-01 Jan 08), January 2008.

*Joint Antiterrorism Program Manager's Guide* (JAT Guide) Version 3.0, August 2008.

JP 1-02. *DOD Dictionary of Military and Associated Terms*, 12 April 2001 (As amended through 17 October 2008).

JP 2-0. *Joint Intelligence*, 22 June 2007.

JP 3-0. *Joint Operations*, 17 September 2006 (Incorporating Change 1, 13 February 2008).

JP 3-01. *Countering Air and Missile Threats*, 5 February 2007.

JP 3-07.2. *Antiterrorism*, 14 April 2006.

JP 3-09. *Joint Fire Support*, 13 November 2006.

JP 3-10. *Joint Security Operations in Theater*, 1 August 2006.

JP 3-11. *Operations in Chemical, Biological, Radiological, and Nuclear (CBRN) Environments*, 26 August 2008

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

JP 3-15. *Barriers, Obstacles, and Mine Warfare for Joint Operations*, 26 April 2007.

JP 3-16. *Multinational Operations*, 7 March 2007.

JP 3-31. *Command and Control for Joint Land Operations*, 23 March 2004.

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

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

JP 3-50. *Personnel Recovery*, 5 January 2007.

JP 3-52. *Joint Doctrine for Airspace Control in the Combat Zone*, 30 August 2004.

JP 3-57. *Civil-Military Operations*, 8 July 2008.

JP 4-0. *Joint Logistics*, 18 July 2008.

JP 4-02. *Health Service Support*, 31 October 2006.

JP 4-03. *Joint Bulk Petroleum and Water Doctrine*, 23 May 2003.

JP 5-0. *Joint Operation Planning*, 26 December 2006.

JP 6-0. *Joint Communication Systems*, 20 March 2006.

*Joint Sniper Defeat Handbook* (GTA 90-01-013), August 2008.

### **Multiservice Publications**

FM 3-24 / MCWP 3-33.5. *Counterinsurgency*, 15 December 2006.

FM 3-100.12 / MCRP 5-12.1C / NTTP 5-03.5 / AFTTP (I) 3-2.34. *Risk Management: Multiservice Tactics, Techniques, and Procedures for Risk Management*, 15 February 2001.

FM 6-02.72 / MCRP 3-40.3A / NTTP 6-02.2 / AFTTP(I) 3-2.18. *Tactical Radios: Multiservice Communications Procedures for Tactical Radios in a Joint Environment*, 14 June 2002.

TM 5-853-2 / AFMAN 32-1071 Vol. 2. *Security Engineering Concept Design*, 12 May 1994.

### **Air Force Publications**

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

AFDD 2-4.4. *Bases, Infrastructure, and Facilities*, 13 November 1999.

AFH 10-222 V3. *Civil Engineer Guide to Expeditionary Force Protection*, 1 May 2008.

AFH 10-222 V14. *Civil Engineer Guide to Fighting Positions, Shelters, Obstacles, and Revetments*, 1 August 2008.

AFH 10-2401. *Vehicle Bomb Mitigation Guide*, 1 September 2006.

AFI 90-901. *Operational Risk Management*, 1 April 2000.

AFMAN 10-401 V2. *Planning Formats and Guidance*, 1 May 1998.

AFPAM 90-902. *Operational Risk Management (ORM) Guidelines and Tools*, 14 December 2000.

*U.S. Air Force Entry Control Facilities Design Guide*, 18 February 2003.

### **Army Publications**

AR 525-13. *Antiterrorism*, 11 September 2008.

AR 525-26. *Infrastructure Risk Management (Army)*, 22 June 2004.

DA Pam 190-51. *Risk Analysis for Army Property*, 30 September 1993.

DA Pam 420-11. *Facilities Engineering Project Definition & Work Classification*, 7 October 1994.

FM 3-07. *Stability Operations*, 6 October 2008.

FM 3-34. *Engineer Operations*, 2 January 2004.

FM 3-90. *Tactics*, 4 July 2001.

FM 3-100.21. *Contractors on the Battlefield*, 3 January 2003.

FM 4-02. *Force Health Protection in a Global Environment*, 13 February 2003.

FM 4-02.2. *Medical Evacuation*, 8 May 2007.

FM 5-0. *Army Planning and Orders Production*, 20 January 2005.

FM 5-19. *Composite Risk Management*, 21 August 2006.

FM 5-415. *Fire-Fighting Operations*, 9 February 1999.

FM 6-0. *Mission Command: Command and Control of Army Forces*, 11 August 2003.

FM 6-99.2. *U.S. Army Report and Message Formats*, 30 April 2007.

FM 100-10-2. *Contracting Support on the Battlefield*, 4 August 1999.

### **Navy/Marine Corps Publications**

MCO 3500.27B. *Operational Risk Management (ORM)*, 5 May 2004.

MCO P5530.14. *Marine Corps Physical Security Program Manual*, 21 December 2000.

MCWP 5-1. *Marine Corps Planning Process*, 5 January 2000 (w/Change 1, 24 September 2001).

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

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

MIL-HDBK-1013/14. *Department of Defense Handbook: Selection and Application of Vehicle Barriers*, 1 February 1999.

NWP 5-01. *Naval Operational Planning*, 1 May 1998.

OPNAV Instruction 3500.39B. *Operational Risk Management (ORM)*, 30 July 2004.

UG-2031-SHR. *User's Guide on Protection Against Terrorist Vehicle Bombs*, May 1998.

### **Unified Facilities Criteria**

UFC 4-010-01. *DoD Minimum Antiterrorism Standards for Buildings*, 8 October 2003 (Including Change 1, 22 January 2007).

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for*

*Buildings*, 8 October 2003 (Including Change 1, 19 January 2007).

UFC 4-020-04FA / TM 5-853-4. *Security Engineering: Electronic Security Systems*, 1 March 2005.

UFC 4-021-01. *Design and O&M: Mass Notification Systems*, 9 April 2008.

UFC 4-022-01. *Security Engineering: Entry Control Facilities / Access Control Points*, 25 May 2005.

## Other

Lauritsen, Brad, and Aldo E. McKay. "Design and Evaluation of Novel Counter-Mobility Barrier Systems." San Antonio, TX: Advanced Technology Office, Applied Research Associates, Inc. (available at [http://www.buildingsecurity.us/docs\\_pubs.php](http://www.buildingsecurity.us/docs_pubs.php))

Magness, Thomas H., and James Ahern. "CTC Notes – 'SWEAT.'" *Engineer* Vol. 35, July-September 2005, pp. 18-19.

Peay, Binford J. H. III. "Correlating Medical Forces Forward." *Joint Force Quarterly* Vol. 14, Winter 1996-97, pp. 70-74.

Schumitz, Robert. "Operational Contracting in Support of Operation Iraqi Freedom," Briefing slides, 2005 Annual Army Contingency Contracting Conference, 20 April 2005.

Taylor, George P. Jr. "Air Force Capability-Based Medical Planning." *U.S. Medicine* Issue 58, January 2004.

Taylor, Scott R., Amy M. Rowe, and Brian M. Lewis. "Consequence Management in Need of a Timeout." *Joint Force Quarterly* Vol. 22, Summer 1999, pp. 78-85.

**Joint Forward Operations Base (JFOB)**  
**Survivability and Protective Construction Handbook**  
(formerly titled *The JFOB Force Protection Handbook*)  
**GTA 90-01-011**

FOURTH EDITION  
THIRD EDITION  
SECOND PRINTING (EDITION)  
FIRST PRINTING (EDITION)

MARCH 2009  
APRIL 2008  
DECEMBER 2006  
NOVEMBER 2005

1	The Operational Environment
2	Community Engagement
3	Command and Control
4	Risk Management
5	Planning
6	Site Selection and Layout
7	Critical Infrastructure Assurance
8	Security
9	Access Control
10	Protection
11	Standoff
12	Barriers and Obstacles
13	Entry Control Structures
14	Sidewall Protection
15	Compartmentalization
16	Overhead Cover
17	Lighting
18	Sensor Systems
19	Existing Structures
20	Protective Structures
21	Joint Combat Outposts
A	Abbreviations and Acronyms
B	Force Protection Conditions
C	Materiel Support
D	Soil-Filled Container Applications
E	Tent Camp Layouts
F	References

**FOR OFFICIAL USE ONLY**