FINAL DRAFT EDITION **EXPIRES 1 MARCH 2007**

JOINT FORWARD OPERATIONS BASE (JFOB) FORCE PROTECTION HANDBOOK

NOVEMBER 2005

FOR OFFICIAL USE ONLY

Distribution Restriction Statement on inside Front Cover

JOINT FORWARD OPERATIONS BASE (JFOB) FORCE PROTECTION HANDBOOK

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 15 November 2005. Other requests for this document will be referred to the Survivability Engineering Branch (GS-V), Geotechnical and Structures Laboratory, U.S. Army Corps of Engineers Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, Mississippi 39180-6199.

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

FOREWORD

Lessons learned during Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) revealed that forward operations bases face an increased threat posed by asymmetric forces. Consequently, the Director, Operational Testing and Evaluation (DOT&E) authorized a Joint Forward Operations Base (JFOB) Quick Reaction Test (QRT). This QRT, under the guidance of Army Test and Evaluation Command and the Joint Chiefs of Staff Deputy Directorate for Antiterrorism and Homeland Defense (J-34) developed this JFOB Handbook with significant assistance from U.S. Central Command.

The aim of this handbook is to describe those tactics, techniques, and procedures (TTP) and best practices suited to counter the rocket, artillery, mortar (RAM), and improvised explosive device (IED) threats to JFOBs in Iraq. The objective is to reduce the casualty rate during combat operations.

This handbook provides a quick-reference guide for a systematic approach to planning, developing, and improving JFOB defensive capabilities. The handbook is linked to the current evolution of forward operations bases by design and can be located on the Joint Staff Antiterrorism Enterprise Portal (ATEP) for access by users. The handbook is also available on CD and limited hard copy.

The JFOB Handbook is designed to be a quick look reference and is broken into major subject areas to facilitate use. The series of chapters is listed on the back of the book with a corresponding black tab by each title. The pages are striped with the corresponding tab at the appropriate level to allow the reader to quickly turn to the desired section of the handbook without wading through a series of appendixes.

PREFACE

Scope

This publication addresses force protection (FP) at joint forward operations bases (JFOBs) in the Iraq theater of operations. The focus is on defense against rockets, artillery, and mortars (RAMs) and vehicle-borne improvised explosive devices (VBIEDs). It describes how adversary and friendly courses of action (COAs) are evaluated and implemented to support the JFOB commander's decision making process. This publication is geared primarily towards engineer and FP specialists to assist with operational level FP planning. It also addresses "best practices" for defeating RAMs and VBIEDs.

Purpose

This publication has been prepared under the direction of the Office of the Secretary of Defense. As a result of a Quick Reaction Test program, a series of best practices for JFOB defense emerged from current doctrine, joint tactics, techniques and procedures (JTTPs), and current practices in theater. It provides recommendations for the exercise of FP by combatant commanders and other JFOB commanders for JFOB defense. It provides military guidance for use by the Armed Forces 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 includes tactics, techniques, and procedures (TTPs) available from the Combined Force Land Component Command (CFLCC) and Multinational Corps-Iraq (MNC-I) units that have been or are currently serving in the Iraq theater of operations. 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 this OSD QRT 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.

JAMES R. ROWAN
Colonel, U.S. Army
JFOB QRT Test Director

ACKNOWLEDGEMENTS

The JFOB Quick Reaction Test Director wishes to acknowledge the following organizations for providing exceptional support to process of development, printing, and distribution of the JFOB Force Protection Handbook Final Draft:

- Office of the Secretary of Defense, Joint Test and Evaluation, 4850 Mark Center Drive, Alexandria, VA 22311
- Joint Staff, J3 Deputy Director for Antiterrorism, Homeland Defense (DDAT/HD), Pentagon, NMCC, MB 917, Washington, DC 20318
- Joint Security Directorate, US Central Command, (CENTCOM), 7115 South Boundary Blvd., MacDill AFB, FL 33621
- Headquarters, US Marine Corps, Security Division, 2 Navy Annex, Washington, DC 20380
- Headquarters, Department of the Army, G357, Pentagon, Washington, DC 20300
- 3rd US Army, Fort McPherson, GA/Camp Doha, Kuwait
- Multinational Corps Iraq, Camp Victory, Iraq
- Army Test and Evaluation Command (ATEC), 4501 Ford Avenue, Park Center, Alexandria, VA 22311
- Joint Improvised Explosive Device Defeat Task Force, 400 Pentagon, Washington, DC 20310
- US Air Force Civil Engineer Support Agency, Tyndall Air Force Base, FL 32403
- 1st Cavalry Division, Building 28000, Fort Hood, TX 76544
- 412th Engineer Command, 1265 Porters Chapel Road, Vicksburg, MS 39180
- MANSCEN, Building 971, Parker Hall, Fort Leonard Wood, MO 65473
- US Army Corps of Engineers G3 Operations, 441 G Street, NW, Washington, DC 20014
- Geotechnical and Structures Laboratory, US Army Engineer Research and Development Center, 3909 Halls Ferry Road, Vicksburg, MS 39180
- 20th Engineer Brigade, Fort Bragg, NC 28310
- 420th Engineer Brigade, Bryan, TX 77803
- US Army Rapid Equipping Force, Fort Belvoir, VA 22060
- US Air Force Force Protection Battlelab, Lackland Air Force Base, TX 78236
- US Army Corps of Engineers, Protective Design Center, Omaha, NE 68102

CONTENTS

Chapter 1

COMMAND AND CONTROL AND THE BASE DEFENSE SYSTEM

Contents

INTRODUCTION

Since the cessation of combat operations and the declaration of sovereignty, negotiations have been required between the Interim Iraqi Government (IIG) and Coalition Forces for use of terrain for joint forward operations bases (JFOBs). A Status of Forces Agreement (SOFA) is being developed at this time. Much of the land currently used for JFOBs belongs to the IIG and consists of former military and government sites. Some land, however, does belong to local governments and individuals. Corps of Engineers Real Estate Teams (CRESTs) are the U.S. Government's real estate agents and acquire required real estate.

In most instances, units will occupy JFOBs that are mature, and master planning will be complete. JFOBs will remain dynamic as coalition forces and threats continue to change. The latest master planning information is found in MNC-I Operations Order 05-02. Some changes are planned, and some are not. Currently, there is a strategy to consolidate JFOBs. In all instances, consolidation will increase vulnerability, and force protection (FP) personnel must remain vigilant against over-consolidation on terrain.

The JFOB maintains and sustains the force while providing an island of relative security for service members to rest, rearm, and refit.

In Operation Iraqi Freedom (OIF), the JFOB has been a target of harassment by anti-Coalition and anti-Iraqi forces (AIF). The dominant tactics used to harass Coalition Forces and disrupt operations have been rockets, artillery, mortars

(RAMs), and improvised explosive devices (IEDs) that are either vehicle or man-pack delivered.

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 (ECPs), and in periods of heightened alert with spectators gathering in areas of recent attacks where they impede incident responders and create additional targets. See Figure 1-1 (Tenant Force Protection Responsibility).

TENANT UNIT COMMANDER'S RESPONSIBILITIES

- Participate in the preparation of base defense plans
- Provide, staff, and operate base defense facilities in accordance with base defense plans
- Conduct individual and unit training to ensure readiness for assigned defense tasks
- Provide his share of facilities, equipment, and personnel for the BDOC (base defense operations center) and, when appropriate, for the BCOC (base cluster operations center)
- Advise the base commander on defense matters peculiar to his units
- Provide for his own internal security
- Sustain and administer his units
- Provide support to the Base Commander

Figure 1-1. Tenant Force Protection Responsibility

TYPES OF JFOBS

In an effort to build a global network of capabilities with allies and partners, the Department of Defense (DoD) developed a global defense posture. It redefined basing for DoD to align with U.S. Defense Strategic Objectives. U.S. Central Command (USCENTCOM) Regulation 415-1 describes these categories of bases. This handbook only highlights contingency basing as it relates to Iraq. We acknowledge the concepts of global defense structure as it deals with strategy and the Planning, Programming, and Budgeting Execution System (PPBES), but for simplicity and consistency we will refer to all bases currently in Iraq as JFOBs.

Basing Categories

Basing falls into one of two categories: permanent or contingency. Permanent basing is associated with long-term strategic force stationing, while contingency basing is associated with short-term contingency operations. Specific locations and sizes of these bases are determined during the course of the contingency operation.

Permanent Basing. The basing of forces is dictated by the guidance published by the Secretary of Defense in the Integrated Global Presence and Basing Strategy (IGPBS). Bases included in the IGPBS are at those locations where the

U.S. is expected to have a long term presence or at key locations within the (area of responsibility (AOR) where there is a possible need to rapidly expand sites.

Contingency Operation Bases (COB). A contingency Base is usually occupied by an element larger than Unit of Action (UA) size from a single service or joint services. Its purpose is typically a command and control hub and/or regional logistics hub, characterized by advanced infrastructure for facilities and communications for the expected duration of the operation/exercise. A COB may include an airfield capable of C-130 or larger aircraft.

Contingency Operation Sites (COS). A contingency site is usually occupied by a UA size element or smaller capable of providing local and regional operations, security, and/or humanitarian assistance relief. The site, size, and capabilities are scalable to support rotation of forces or prolonged contingency operations. It is characterized by limited infrastructure and may be dependent on some contracted services.

Contingency Operation Locations (COL). A contingency location is usually occupied by a battalion-sized element capable of quick response to operations, security, civic assistance or humanitarian assistance relief. A COL will be dependent upon COS or COB for logistical support and is characterized by stark infrastructure primarily dependent on contracted services or field facilities. A COL consolidates to a COS as the contingency matures.

JFOB COMMAND AND CONTROL

For major JFOBs, dedicated security forces will be assigned to the base defense operations center (BDOC) and provide baseline security with augmentation by tenant units. Smaller operationally-based JFOBs provide self-protection. In all instances, tenants will be tasked to provide security support to include guard tower, ECP support, sector security support, key asset protection, and contractor escort. To help facilitate a quick understanding of the command and control (C2) relationships and responsibilities, excerpts have been extracted from key Joint Doctrine as it is related to operations in a non-linear battlespace.

Responsibility for base defense has been delegated to the senior terrain manager in OIF except where specified logistics and support bases belonging to Multinational Corps-Iraq (MNC-I) lie inside other Coalition AOR. These bases include general support (GS) hubs, relay points and rest and refueling areas. In this capacity, Joint Doctrine for base defense has been used to predominantly manage security in the combined operational area. JFOBs have used the force protection working group (FPWG) as well as electronic collaboration to become extremely effective in managing the JFOB FP program. See Figure 1-2 (Joint Operations Area (JOA) C2).

In the nonlinear battlespace, JFOBs can be joint or combined. They are mission, enemy, terrain, troops, and time available (METT-T) dependent and have the ability to mutually support other bases.

Managing and Planning of Base Camps. Commander, USCENTCOM will designate by operations order (OPORD) and/or frag order (FRAGO) lead agencies for managing and planning base camps. These designations (see following paragraphs) are LCLC, BOS-I and SAA. The “Base Matrix” is a term

to designate the matrix displaying location, base, LCLC, BOS-I, SAA and the corresponding lead, CJTF or Component.

Single/Joint/Combined Use. The combatant commander (COCOM) will determine (unless determined by higher authority) and announce the classification of bases in the area in accordance with policies established by the Chairman of the Joint Chiefs of Staff. A base may be a single service base or a joint base in which one service has primary interest or two or more services have coequal interest.

Lead Component for Joint Logistics and Contracting (LCLC). Lead

Component for Joint Logistics and Contracting – (replaces Executive Agent (EA)) – a component assigned responsibility by USCENTCOM as the lead for coordinating joint logistics and contracting within a designated country. The lead component has primary responsibility for coordinating common item and common service support or other administrative and support functions. Individual OPLAN, CONPLANs or OPORDs published by USCENTCOM address specific support responsibilities. The lead component ensures efforts are coordinated through the theater security cooperation point of contact (POC).

Base Operating Support Integrator (BOS-I). USCENTCOM will designate a component or Joint Task Force (JTF) as the BOS-I at each operating location. The BOS-I acts on behalf of all forces/Services on the camp. The BOS-I will coordinate contracting support and the efficient use of mission support resources. Where shortfalls or opportunities for efficiencies exist, USCENTCOM may task components/JTFs to provide or coordinate specific capabilities (e.g. services, infrastructure, security, and communications). The BOS-I will provide master planning for facilities and real estate. BOS-I responsibilities include collecting and prioritizing construction requirements and seeking funding support, environmental management and hazardous waste disposal.

Airfield Operations Manager/Senior Airfield Authority (SAA). This component is responsible for the control, operation and maintenance of the airfield to include the runways, associated taxiways, and parking ramps as well as land and facilities whose proximity affects airfield operations. The SAA is responsible for coordination of all component/JTF aircraft and airfield facilities (responsibilities will not be split among Services). The SAA controls flight line access and is responsible for the safe movement of aircraft in the airport traffic area and on all airfield surfaces. The SAA will develop and coordinate airfield improvement master plans with the BOS-I and submit them to the BOS-I for inclusion in the overall base master plans. The SAA will also seek funding from their component for airfield operations, maintenance and construction requirements.

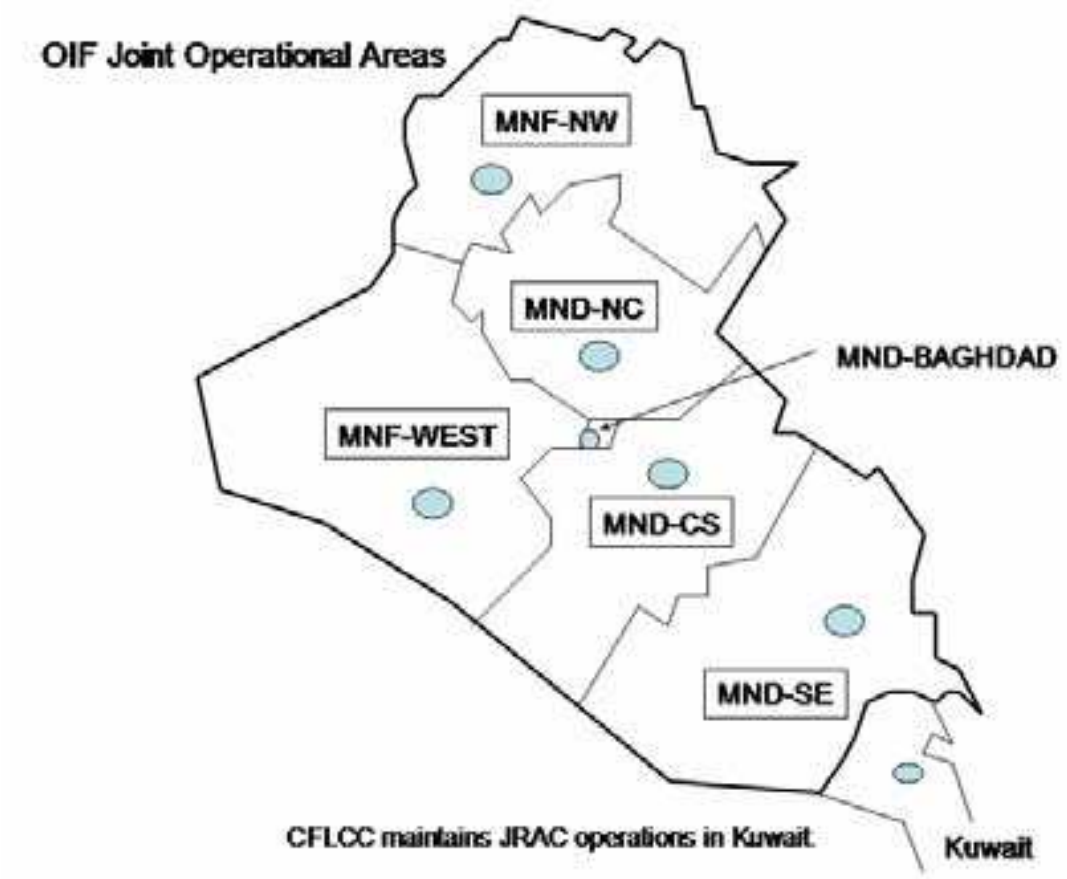


Figure 1-2. Joint Operations Area Command and Control

FUNCTIONS OF JFOBS

JFOBs can be located in urban or rural areas, on former Iraqi bases, in former palace complexes, on former religious sites, at critical points on main supply routes (MSRs), or on rivers. JFOBs can be single service, multi-service, or Coalition to include shared JFOBs with the new Iraqi Army.

JFOBs support a myriad of missions. The following section describes many of those missions with a brief description of the types of activities that will be conducted within the JFOB, as well as the types of assets that could be available to assist in FP.

Operational Support

Overwatch. This JFOB is used to provide elements that can respond to incidents and provide Stability and Support Operations (SASO) in a given area of operations. The mission can range from civil military support with a small force to major interface with the local or regional government. The base is operationally oriented, usually short lived, and austere in construction. Maximum use of existing facilities is encouraged.

Local Control. This JFOB is dedicated to interface with the local government in support of transition to Iraqi control. It provides support to security and reconstruction efforts in a local area and usually provides a mixture of

operational and support capability that interfaces with the local population. This base may also be a shared Coalition/Iraqi Forces base.

Regional Control. This JFOB is similar to a local control base but supports regional government, regional infrastructure, and security.

Strategic Overwatch. These major JFOBs work at the State level to execute overarching security programs to include stand up of police and army forces. They interface with senior government officials and are prime targets due to the high-level personnel operating in and around them. These JFOBs are of the most durable construction and have the highest level of security.

Command and Control. These JFOBs contain Brigade, Division, or Corps Command elements. They are usually located in former palace or military compounds near major centers of gravity for the operation. These JFOBs contain robust FP and have augmented security forces due to the high percentage of support personnel operating there.

River Crossing Control Point. These JFOBs are designed to protect key water crossings and are usually placed where a military fixed or float bridge has been used to create a temporary crossing, and a chokepoint has resulted. These areas are extremely vulnerable to indirect fire or VBIEDs as traffic can back up, and usually there is little time to do effective screening prior to crossing. Currently, these areas are off-limits to most civilian traffic, but as the nation of Iraq continues to gain control of its own security, more civilian traffic will become mixed with military convoys.

Traffic Control Point. These JFOBs are offensive in nature and combat oriented. They are usually temporarily placed in support of shaping operations and are becoming jointly run or controlled by Iraqi forces. They are prime targets of AIF and must be constructed with adequate overwatch and the ability to withstand effects of larger VBIEDs.

CEA Ammunition Storage Areas. These JFOBS are associated with the former Captured Enemy Ammunition (CEA) Program and current Unexploded Ordnance (UXO) Program. These JFOBs are used to secure, hold, turn over, and destroy former regime ammunition that is either unserviceable or is to be used by Iraqi security forces. They are usually formed around the ammunition storage areas, and many are lightly guarded. These areas are constantly pilfered by AIF for materials to be used in IEDs or for indirect fire munitions.

Detainee Operations. These JFOBs are used to house detainees awaiting release, interrogation, or turn over to Iraqi control. They are run as law enforcement and intelligence bases under the direction of the Deputy Commanding General for Detention at the force level. They are heavily fortified and isolated from friendly force operations. Insurgents target these JFOBs for media attention. They can become symbolic targets for attack.

Temporary Support to Kinetic OPs/Elections/Special Events. These are temporary JFOBs established to consolidate forces for special events, elections, or kinetic operations. Usually these JFOBs are established for a specific event and then dismantled after the event. Sometimes these JFOBs are warm bases in areas that will continue to occasionally require temporarily increased numbers of forces.

Multi-National Security Transition Corps-Iraq (MNSTC-I). The MNSTC-I JFOBs are established to provide for the training and handover of security operations to Iraqi Army, Iraqi National Guard, and Iraqi Police. These JFOBs are built and occupied by U.S. and Coalition Forces. As the Iraqi forces are trained and take over the security mission, the bases are turned over to them for operation centers.

Logistics Support

General Support (GS) Hub Ground. This JFOB supports Joint Theater Distribution and Sustainment. It is normally commanded by the senior logistics commander and usually requires augmented security forces due to the size of the facility and relatively light firepower of the units that occupy it. It is normally considered a favorite target for asymmetric threats because of its perceived vulnerability. It has large numbers of critical assets to be isolated and protected and requires a large amount of engineer support to harden and protect. It is usually embedded in the division battlespace but is usually a Corps asset.

GS Hub Air. This JFOB is quite similar to the ground JFOB with the added problem of needing protection from shoulder-fired weapons, which makes control of additional terrain a necessary FP requirement. Coordination with the terrain manager is vital to provide adequate defense against shoulder-fired weapons, such as rocket-propelled grenades (RPGs) and man-portable air defense (MANPADs) protection.

Rest Overnight. These JFOBs are placed along supply and sustainment routes to provide secure rest areas for convoys and combat patrols traveling through the battlespace. They have a cadre force to maintain the facilities and protect the area. High volumes of traffic create compressed targets and increase the likelihood that vehicle-borne improvised explosive devices (VBIEDs) may breach the facility. Extra care must be taken to assure vehicles are screened and quarantined if they are not under constant surveillance of convoy escorts.

Refuel on the Move. These JFOBs are temporary rest stops for convoys to refuel and move on. They are usually only lightly defended, and convoys must provide self-protection. Issues at these sites are the increased vulnerability of convoys to indirect fire weapons and snipers since most are usually protected by wire. Also, local vendors encroach into the area to sell to convoys and can approach vehicles close enough to detonate a man-packed IED.

.

Relay Points. These austere JFOBs are placed along the MSRs to provide safe havens in case of convoy break downs or emergencies, as well as retransmission capability for FM radios. They are small and dispersed and contain small numbers of cadre personnel. They are mainly in the southern area of Iraq and receive mainly harassing attacks. They have bermed sides and heavily defended access points. They are also capable of mutual reinforcement when required.

Ammunition Holding Areas. These Coalition areas, used to store friendly force ammunition, are heavily fortified, and isolated. They are designed and built to ammunition safety requirements. Issues here include protection from indirect fire weapons that could create sympathetic detonation of the stockpiles.

Power Projection. These are intermediate staging bases located outside the area of operations and are currently in Kuwait and Qatar. They project forces into the AOR and provide necessary support for the current operation. These are usually large areas with high concentrations people and equipment that are under the control of CENCOM and have their own mixture of military and contract security. These areas are much more vulnerable to VBIEDs than indirect fire weapons and are normally protected by fences, berms, and fortified barriers.

CONCLUSION

Understanding the C2 relationship for FP of JFOBs early is critical to the staff in establishing a successful program. This is a key operational task that requires a full commitment of resources and a great deal of synchronization to assure it does not conflict with mission tasks. Engage the commander early and often, and seek full participation of the entire staff to assure success.

RESOURCES

The following web sites contain information applicable to the joint intelligence preparation of the battlespace (JIPB) C2 and base defense process. They should be reviewed and evaluated to determine the availability of current data, information, and intelligence products relative to the joint force's battlespace and mission. Access to these sites requires a Secure Internet Secret Protocol Router Network (SIPRNET) connection.

The **U.S. Central Command (**USCENTCOM) SIPRNET site is located at http://www.centcom.smil.mil/.

The Multinational Forces-Iraq (**MNF-I**) website is located at http://www.iraq.centcom.smil.mil/mnfi_sipr.cfm.

The Multinational Corps-Iraq (**MNC-I**) website is located at http://www.iraq.centcom.smil.mil.

The U.S. Third Infantry Division (**3 ID**) website is located at http://www.idmtweb.id3.army.smil.mil/.

The Third Army U.S. Forces Central Command (**ARCENT**) site is located at http://www.swa.arcent.army.smil.mil/.

REFERENCES

USCINCCENT Operations Order 97-01B (Antiterrorism), 4 January 2002.

CENTCOM Reg 415-1. *Construction and Base Camp Development in the USCENTCOM Area of Responsibility (AOR). "The Sand Book,"* 1 December 2004.

JP 3-10. *Joint Security Operations in Theater*, 11 February 2005

Chapter 2

JFOB FORCE PROTECTION PLANNING PROCESS

Contents

INTRODUCTION

Operation Iraqi Freedom (OIF) has evolved into a rotational Task Force operation. This evolution affords planners from the deploying-unit opportunities to perform a seamless transfer of authority with the redeploying force. Although the battlespace remains dynamic and must adjust to political and operational events, a pattern of evolution has been established that includes a general transition to end state of joint forward operations bases (JFOBs). A deliberate program of increased force protection (FP) mixes military and contract construction to improve safety at the Coalition bases in Iraq. Upon deployment, force protection (FP) fragmentary orders (FRAGOs) are issued to the FP Annex to adapt the JFOB to changing conditions that would be expected as part of wartime operations. This chapter is organized chronologically to assist the deploying unit in pre-deployment planning, execution of the FP annex during deployment, and FP considerations for redeployment. Pre-deployment, deployment, and redeployment operations are summarized in Figure 2-1.The JFOB handbook process uses the Military Decision-Making Process (MDMP) (see Figure 2-2).

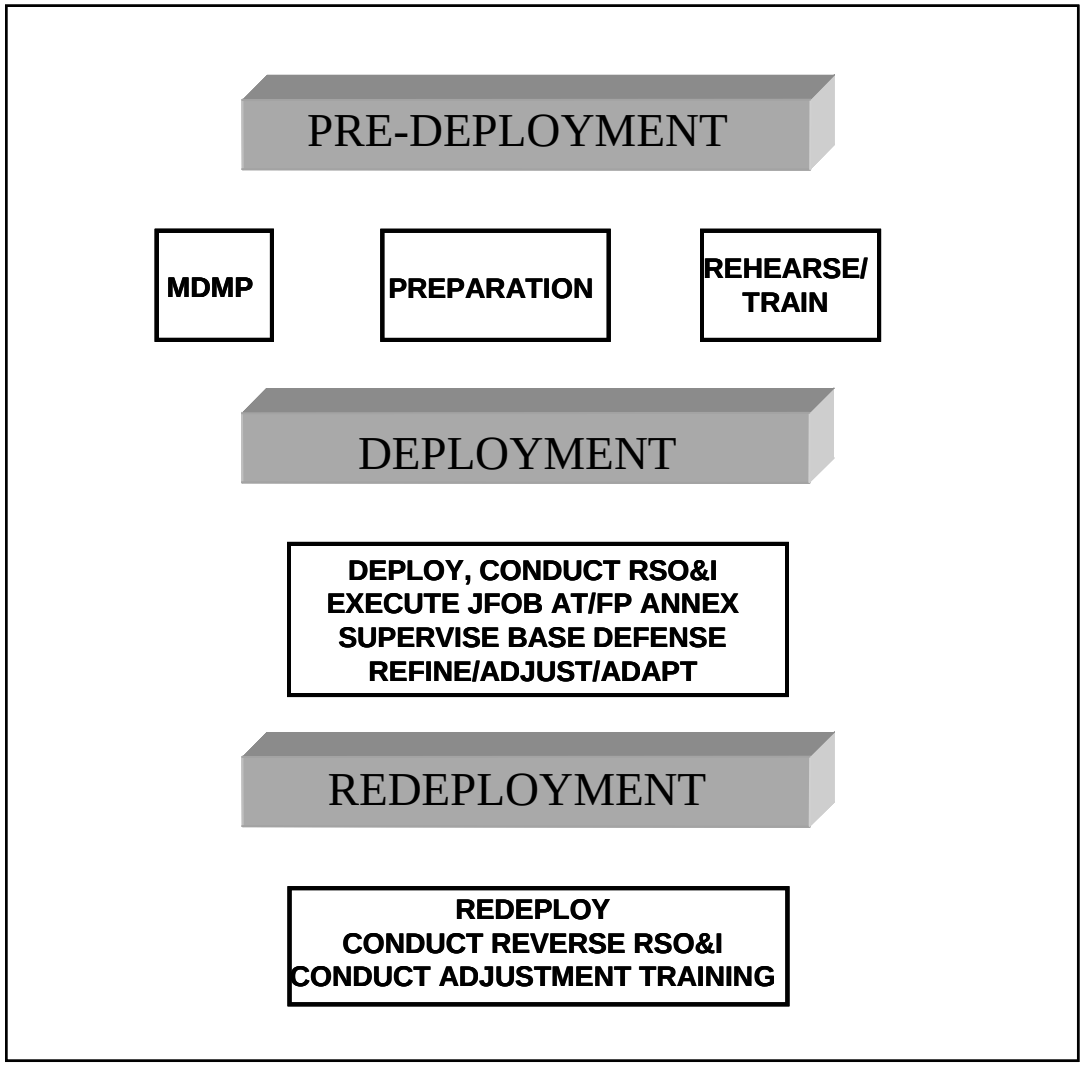


Figure 2-1. JFOB FP process summary

PRE-DEPLOYMENT

INTRODUCTION

During pre-deployment, the military decision-making process (MDMP) results in a Force Protection Annex (see Chapter 14, Force Protection Plan Template) that completes the FP planning for the Pre-deployment Phase. The nature of the rotating task force to Iraq currently allows planning time to develop a Force Protection Annex to the deployment OPORD using the MDMP. There is also time to prepare and rehearse execution of this mission as a part of the pre-deployment preparation and training prior to execution.

PLANNING FOCUS AREAS

Fifteen specific focus areas have been identified to support successful pre-deployment planning for JFOB Force Protection in support of OIF. These are:

Complying with MNC-I OPLAN 05-02. This is the comprehensive, effects-based plan that includes the theater basing master plan as it supports the commander's desired end state for OIF. This document is available on the Multinational Corps-Iraq (MNC-I) SIPR site and is the first document you should read as you plan the mission.

Integration of the Master Plan. This is the comprehensive plan that drives basing evolution in OIF. It is condition-based, but sequentially programmed for consolidating bases from local overwatch to regional overwatch and strategic overwatch. FP is driven by this plan and includes evolution from austere to containerize to concrete structures in some areas. This plan is a critical subset of the FP plan and will include installation property, critical equipment, communication systems, sensors and Class IV barrier materials that must be accounted for in your planning.

Developing a Continuity of Operations (aka COOP plan aka Battlebook). This is the electronic file cabinet and/or physical notebook that will be used to consolidate all resources, contact information, plans, sketches and other information as you perform mission analysis and develop forces and strategies to accomplish the FP mission. Development of this resource during pre-deployment enhances communication, cooperation and transition between deploying and redeploying forces. It minimizes turmoil and expedites the transition of authority for FP.

Finding Information. Operation Iraqi Freedom is a mature operation with numerous websites for research and collaboration. An initial part of research will include accessing the MNC-I, USCENTCOM and doctrinal lessons-learned sites. Development of a web resources reference is highly encouraged. While most information resides on SIPR sites, a large amount of information is available from open sources.

Establishing Relationships. As soon as possible, you should contact your counterpart at the site where you are deploying and establish a communication plan. Develop your list of information requirements and pass these forward to begin populating your Continuity of Operations Plan. Establishing communication with other units that will deploy as a part of your rotation is just as important. Also, exchange any specifics regarding commander's intent or mission change that may affect transition of authority.

Training and Tools Integration. The FP and security engineering areas are being rapidly overwhelmed by technologies and software tools that require special training or skills to be developed prior to mobilization. Identify these specific requirements through units currently in country, and schedule members of your FP staff for training or, as a minimum, provide information to your FP staff on what tools are available, how they are used and who is responsible for them.

Using Reach Back. Critical technical skills have been made available through Internet or video teleconference to units in support of OIF. Obtain contact information and list of services provided by these entities. Develop contacts with these organizations as part of your pre-deployment operation, and develop procedures to access and share information from these resources among units under your control to prevent redundant or conflicting requests for support. (See Chapter 15)

Performing Gap Analysis. After all available information has been gathered and all resources have been contacted, review the inputs you have to your continuity of operations plan and perform a gap analysis. Look for any policy, plan, resource or contact shortfall. Prepare requests for information or seek to answer these questions on the pre-deployment site survey.

Pre-Deployment Site Survey (PDSS). This event is used to develop relationships, ground truth information, perform inventories, take measurements and execute any planning support tasks that cannot be completed virtually. Whether or not you are a part of the PDSS team, you should provide a comprehensive information requirements package to be completed by the unit representative who travels to theater. Always be prepared to pass this information packet on short notice. A survey form is provided in Chapter 15.

Monitoring Evolution of Battlespace. Change and consolidation of bases along with adaptation of tactics, techniques, and procedures (TTPs) by anti-Iraqi forces (AIF) require constant monitoring of events in Iraq during pre-deployment operations. Specific efforts must be directed toward identifying and countering emerging threat TTPs and weapons. Research into TTPs of other international terrorist organizations can provide some predictive analysis of what will be employed next. Threat TTPs will continue to be more sophisticated and lethal.

Post Mobilization Training. Deployment centers have gone to great lengths to make post mobilization training as realistic as possible. Use this opportunity to perform your analysis and validate your plans in an interactive environment. Identify any special training requirements early and schedule mobile training team support. This support is readily available on request.

Use of Validation Exercises. FP should be integrated prominently into unit validation exercises. Commanders should have specifically identified their responsibilities and capabilities to support this mission and they must be integrated into the decision-making process to assure that FP requirements and antiterrorism (AT) measures do not create undesired effects as they relate to the commander's operational mission.

Development of Knowledge Management Sites. Once the planning process is complete, there will be a huge volume of information that will require effective knowledge management to keep updated and disseminated. For OIF 1 & 2, use of web pages to post and disseminate this information has been the most effective means. Deploying units are highly encouraged to transition those pages from returning units and upgrade them to meet incoming unit needs.

Relief In Place/Transition of Authority (RIP/TOA). This is the official handover of units responsibility and can become overwhelming if not planned

thoroughly. Review the proposed plan of the departing unit as soon as possible, and assure that your commander's intent is supported prior to approval of the schedule. Look for events that can be initiated or monitored virtually, and begin participation by video teleconferencing (VTC) or telephone when possible. Begin integrating events into schedules and SITREPs, and review inventories to locate and schedule handoff. Develop checklists when possible, and review these prior to deployment to enhance your ability to disseminate actions and control processes.

Use of the JFOB Handbook. This reference ties together processes, resources, tools, templates, TTPs, and the latest FP technologies that have been developed under DoD's Joint IED Defeat Task Force (JIEDD-TF) and the Counter Rocket Artillery and Mortar (C-RAM) Program under the direction of Training and Doctrine Command's (TRADOC's) Spiral Developments Branch. Many of these technologies have been pushed to the theater through TRADOC's Rapid Equipping Force (REF) and through operational needs statements (ONS) or combatant commander (COCOM) requested congressional appropriations. Use of this handbook supports information gathering, course of action (COA) analysis and plan development. The chapters of this book will be referenced in the appropriate places as we discuss the MDMP process in the next section of this chapter.

FP CONSIDERATIONS FOR JFOB MASTER PLAN

General. It is critical to include FP issues in the JFOB master plan to achieve the desired end state for FP. It also reduces the "short-term" decision-making that is historically observed in rotational operations where decisions favor measures that are implemented during "my watch." Master planning provides an integrated strategy for construction and maintenance of required facilities at the best possible cost. AT/FP and physical security concerns ensure adequate protection of personnel and assets and are critical to the development of JFOBs, including site selection and the development of the base camp layout (see Chapter 5). AT/FP and physical security (see Chapters 6 and 7) are essential considerations that influence the JFOB master plan.

Many JFOBs evolve over time from austere to permanent. The master plan level of detail depends on the maturity of the location, the speed at which the operational need for a base camp develops, and the expected length of stay. Master plans for expeditionary and/or initial standard camps can be simply a sketch of the camp, while master plans for temporary or enduring presence camps will include fully engineered construction plans based on complete surveys. Master plans will include land-use development maps and graphics and supporting construction project lists.

USCENTCOM Regulation 415-1, Construction and Base Camp Development in the USCENTCOM area of responsibility (AOR), commonly known as The Sand Book, provides the information needed by personnel developing the JFOB master plan.

MILITARY DECISION MAKING PROCESS

Military Decision-Making Process

- Receive Mission
- Analyze Mission
- Develop Courses of Action
- Analyze Courses of Action
- Compare Courses of Action
- Approve Courses of Action
- Produce Orders

Figure 2-2. The military decision-making process

Receive Mission. This is the first step in the MDMP. The mobilization order assigns who, what, when, where and why the mission will be accomplished. The key information for FP planners is the location that units will operate from, the current state of JFOBs, and current TTPs being employed by threat forces against them.

The mission and the commander's guidance should drive the planning process. A sample mission statement is provided in Figure 2-3 that may be refined and restated during the MDMP.

JFOB Mission Statement

1ST ASG conducts base defense on a continual basis NLT 10 Sept XX in MND-West to protect MNF-I personnel, infrastructure, and mission capability.

Figure 2-3. Example of a JFOB Force Protection mission statement

Analyze Mission. This is the second step in the MDMP. In order to take advantage of the time between alert and mobilization, early collaboration between the operating unit and its replacement is a must. This collaboration can use secure and non-secure internet, video teleconferencing, and telephone. Regularly scheduled exchanges can lead up to a well defined pre-deployment-site survey to complete the information-gathering process and a detailed mission analysis that results in sound COA recommendations to commanders. The commander's initial guidance becomes a key part of the MDMP process and provides the staff a reference during mission analysis and later during COA Development. A sample is provided in Figure 2-4.

JFOB Commander's Initial Guidance

- Identify and prioritize highest risk threats (default RAMS and VBIEDs)
- Establish BDOC for C2 of JFOB Defense
- Establish/take handoff or perimeter security and access control
- Maximize dispersion to mitigate frag/blast effects
- Establish/confirm full-height sidewall protection against frag/blast in high troop concentration facilities and sleeping areas
- Compartmentalize areas with high troop concentrations (DFAC, fest tents, gyms, chapel rec areas, internet cafes)
- Provide overhead cover and pre-detonation screens for facilities with high troop concentrations

Figure 2-4. Example of a Commander's initial guidance

Gather Information (Part of Analyze Mission). USCENTCOM has a robust classified web site that links to the deployed forces of the Multinational Corps – Iraq and Multinational Force – Iraq web sources for Iraq current operations. See Resources at the end of this chapter for a list of applicable web sites.

At these websites, units can bring themselves up to speed on FRAGOs, situation reports (SITREPS), and unit collaboration sites. The Antiterrorism Enterprise Portal (ATEP) contains classified and unclassified web locations that provide a great deal of information as well as links to tools and processes to aid planners and operators.

One of the historical problems that occur when units rotate is the loss of information as redeploying units take their sites off-line. It is important to link to current web sites to gather pertinent information before it disappears.

Detailed information related to pre-deployment planning, including checklists and templates, as appropriate, is provided in successive chapters.

- Receive/Develop JFOB Master Plan – Chapter 2 (Checklist below)
- Intelligence Considerations – Chapter 3
- Risk Assessment and COA Development – Chapter 4
- JFOB Site Selection and Layout – Chapter 5
- JFOB Perimeter and Internal Security – Chapter 6 and 7
- JFOB Protective Construction and infrastructure Assurance – Chapters 8 and 11
- Incident Response and Consequence Management – Chapter 9
- JFOB Communications – Chapter 10
- Resourcing – Chapter 12

- Training and Exercises – Chapter 13
- Plans Development – Chapter 14
- Pre-deployment Site Survey Checklist Tool – Chapter 15

Develop Courses of Action. The staff and/or working groups will meet to plan and adopt measures that coalesce into COAs. The COA development will include the latest technologies using reach back and forward deployed subject matter experts (SME). Planers should develop capabilities to secure the best mixture of DoD civilian and contractors to minimize FP impact on operational missions. COA development should not be limited by what you can't do; rather the group should be pro-active and think outside the box.

Analyze Courses of Action. COAs will be analyzed using a center of gravity concept. Refer to the base operating plan and the commander's guidance and the desired end state to measure effectiveness and compatibility. The analysis will include effects-based assessments that include the following criterion:

- Suitable. This COA will lead to mission accomplishment.
- Feasible. Ensure the COA is within the capability of the unit; i.e. ensure the resources are available to accomplish the task.
- Acceptable. The COA is within the bounds of legal, moral and host nation (HN) constraints.
- Distinguishable. Each COA should have unique characteristics that define tasks and that do not overlap with other COA.

Compare Courses of Action. This task requires a synchronization matrix that will weight the different COAs by giving a numerical value to each COA. The process analyzes strengths and weakness to include the advantages and disadvantages of each COA. The COA that provides the most likely opportunity for success will be chosen. The selected COA should:

- Pose minimum risk to the force and to mission accomplishment.
- Place the force in the best posture for future operations.
- Provide maximum latitude for initiative.
- Provide the most flexibility to meet unexpected threats and opportunities.

Course of Action Approval. The staff recommends a COA in a decision brief. The format for the decision brief is found in the JAT Guide. Components of COA approval include; the staff presenting the COAs to the commander with caveats. The staff will recommend their best COA. The commander may accept, modify, or require additional information before deciding which COA to accept.

Produce Orders. The staff prepares the orders by transforming the approved COA into a clear, concise concept of operations and approved information. If required, prepare a sketch that will become the basis for the operation overlay.

The orders and plans will provide required information for subordinates to avoid unnecessary constraints that inhibit initiative. The commander will review and approve orders production unless this authority has been delegated. The orders are briefed to subordinate commanders, using information from the FP plan. (See the template in Chapter 15 of this handbook)

Managing Information. At each step in the pre-deployment planning process, critical information should be shared and placed in continuity of operations plans. These plans are living documents that accompany the FP Staff to theater and are a part of their reference and knowledge management program. The template for a continuity of operations plan can be found in Chapter 14 of this handbook.

DEPLOYMENT

Deployment to Iraq or Afghanistan means receiving the handoff of a JFOB from the redeploying unit in most cases. This transfer should have been planned and coordinated in detail during pre-deployment between the incoming and outgoing organizations. Upon transfer of responsibilities, the unit will begin the FP program management, reassessment of the threat and vulnerabilities and begin the age-old process of continuously improving the defensive position until relieved or until the mission is completed. See the proposed execution checklist below:

EXECUTE FP PLAN AS PART OF THE OPERATIONAL ORDER DEPLOYED OPERATIONS CHECKLIST

Reassess Threat
- a. Types Used and Characteristics
- b. Patterns of Employment
- c. Effects of Threat Weapons

Reassess Vulnerabilities/Key Assets

Establish Perimeter Security
- a. Barriers
- b. Access Control
- c. Entry Control Points
- d. Guard Towers

Establish Internal Security
- a. FPCONs
- b. RAMs
- c. ROE
- d. Roving Patrols
- e. Incident Response
  - i. QRF
  - ii. Fire
  - iii. Medical
  - iv. EOD
  - v. MWD

Implement Structural Hardening
- a. Dispersion
- b. Full-height sidewall protection
- c. Compartmentalization
- d. Large Gathering Areas
- e. Perimeter Security
- f. Individual Living Areas
- g. Tents
- h. Temporary Buildings
- i. Windows
- j. Walls
- k. Roofs

Establish Incident Response Capability

Install Intrusion Detection and Surveillance Systems
- a. Active
- b. Passive

Install Mass Notification and Warning Systems
- Inspect Warning Systems – Giant Voice

Develop Consequence Management Capability

REDEPLOYMENT

Redeploying units should take the lead in battle handoff, particularly in FP because of their battlefield experience and the geopolitical knowledge they have gained during their rotation. The ramp-up in numbers during a battle handoff makes a particularly lucrative target to the insurgency, increasing both the likelihood of attack and the likelihood of success for inflicting casualties due to

increase occupancy of the JFOB. AT/FP officers must also be vigilant in ensuring that their units never let their guard down while in the combat zone, particularly in the last few weeks or days of a rotation. The FP in the JFOB and in-transit still apply.

TRANSITION TO FOLLOW-ON FORCE

- Battle handoff to follow-on force (own forces, multinational or HN)
- Or conduct base closure using proper techniques
- Complete relief of responsibility
- Reverse reception, staging, onward movement, and integration (RSOI)
- Readjust to peacetime environment
- Pass after-action report/lessons learned and improved TTPs to the arriving unit

RESOURCES

The following web sites contain information applicable to the joint intelligence preparation of the battle space (JIPB) FP planning process. They should be reviewed and evaluated to determine the availability of current data, information, and intelligence products relative to the joint force's battlespace and mission. Access to these sites requires a secure internet (SIPRNET) connection.

The **U.S. Central Command (**USCENTCOM) SIPRNET site is located at http://www.centcom.smil.mil/.

The Multinational Forces-Iraq (**MNF-I**) website is located at http://www.iraq.centcom.smil.mil/mnfi_sipr.cfm.

The Multinational Corps-Iraq (**MNC-I**) website is located at http://www.iraq.centcom.smil.mil.

The U.S. Third Infantry Division (**3 ID**) website is located at http://www.idmtweb.id3.army.smil.mil/.

The Third Army U.S. Forces Central Command (**ARCENT**) site is located at http://www.swa.arcent.army.smil.mil/.

The Antiterrorism Enterprise Portal (ATEP) is located at https://www.atep.smil.mil. This site provides a vast amount of topics, tools, and information related to antiterrorism planning. The unclassified site is located at https://atep.dtic.mil. Both sites require registration.

REFERENCES

JP 3-0. *Joint Operations.* Revision Second Draft, 9 May 05.

JP 3-10. *Joint Security Operations in Theater.* Revision First Draft, 11 February 2005.

JP 5-0. *Joint Operation Planning.* Revision Third Draft, 10 August 2005.

MNF-I FRAGO 517. *Antiterrorism Order.* 30 December 2004.

Multinational Corps Iraq. OPORD 05-02, 1 April 2005.

USCENTCOM Reg 415-1. *Construction and Base Camp Development in the USCENTCOM Area of Responsibility (AOR).* "The Sand Book," 1 December 2004.

USCINCCENT OPORD 97-01B. *Antiterrorism.* 4 January 2002.

Chapter 3

JFOB THREAT ANALYSIS

Contents

INTRODUCTION

The JFOB threat analysis process is based on the joint intelligence preparation of the battle space (JIPB) analytical process (Figure 3-1). Joint intelligence organizations use JIPB to produce intelligence assessments, estimates, and other intelligence products in support of the joint force commander's decision-making process. JFOB commanders can also use JIPB tactics, techniques, and procedures (TTPs) to develop their threat analysis. JIPB TTPs are detailed in Joint Publication 2-01.3.

Figure 3-1. The JIPB process (from Joint Publication 2-01.3)

Adversary capabilities are identified in terms of broad courses of action (COAs) and supporting operations that the adversary can take that may influence the accomplishment of the friendly mission. Failure to accurately evaluate the adversary may cause the command to be surprised by an unexpected adversary capability or result in the unnecessary expenditure of limited resources against adversary force capabilities that do not exist.

JFOB THREATS

U.S. military and civilian personnel deployed abroad are potential targets of asymmetric warfare. Force Protection (FP) is a security program designed to protect Service members, civilian employees, family members, facilities, and equipment in all locations and situations. It is accomplished through planned and integrated application of combating terrorism, physical security, operations security (OPSEC), and personal protective services and supported by intelligence, counterintelligence, and other security programs.

Threats to the JFOB are divided into three categories:

- **Level I threats** include adversary-controlled agents or sympathizers, terrorism, demonstrations, and civil disturbances.
- **Level II threats** include guerrilla units, unconventional forces, and small tactical units.
- **Level III threats** are conventional forces, air or missile attacks, and nuclear, biological, and chemical (NBC) weapons.

Security and intelligence analysts must take care not to evaluate adversary joint capabilities by mirror imaging U.S. joint doctrine. The joint doctrine of potential adversaries may be embryonic or nonexistent in many cases. Nevertheless, in virtually all cases, the components of an opposing force will at some level of command coordinate their operations according to a set of ad hoc or established procedures. The analyst must try to discern the adversary's doctrine and TTP, no matter how rudimentary it may appear.

JIPB PROCESS STEPS

DEFINE THE BATTLESPACE ENVIRONMENT

The battlespace, relative to FP, may incorporate an area larger than that associated with conventional warfare operations. The battlespace should include the locations of adversary forces (particularly terrorist groups, unconventional forces, and NBC delivery systems), as well as the likely targets of such forces (such as military housing units, transportation networks, and rear area installations).

- □ Identify the limits of the JFOB's operational area.
- □ Analyze the JFOB's mission and the JFOB commander's intent.
- □ Determine the significant characteristics of the JFOB's operational area.
- □ Establish the limits of the JFOB's areas of interest for each geographic battlespace dimension.

- ☐ Determine the full, multidimensional, geographic and non-geographic spectrum of the JFOB's battlespace.
- ☐ Identify the amount of battlespace detail required and feasible within the time available.
- ☐ Evaluate existing data bases, and identify intelligence gaps and priorities.
- ☐ Collect material and intelligence required to support further JIPB analysis.
- ☐ Consider which terrorist or potentially hostile groups are most likely to attack friendly personnel, equipment, and assets. Determine where they are normally based and what third countries may shelter and support them.
- ☐ Anticipate how additional missions, such as a noncombatant evacuation operation (NEO) or peacekeeping operation, may affect force protection.

DESCRIBE THE BATTLESPACE EFFECTS

- ☐ Analyze the military aspects of each dimension of the battlespace environment.
- ☐ Evaluate the effects of each battlespace dimension within the battlespace environment on military operations.
- ☐ Describe the effects of the battlespace on adversary and friendly capabilities and broad COAs.
- ☐ Determine the demographic issues that make protected areas or personnel attractive to terrorist groups or adversary unconventional forces.
- ☐ Assess the vulnerability of specific targets to attack. Consider both physical security issues and time constraints that might limit the availability of a target.
- ☐ Identify probable avenues of approach as well as infiltration and exfiltration routes.

EVALUATE THE ADVERSARY

Evaluate All Level I, II, and III adversary forces.

- ☐ Identify adversary centers of gravity (Those characteristics, capabilities, or localities from which an adversary force derives its freedom of action, physical strength, or will to fight).
- ☐ Update or create adversary models.
- ☐ Determine the current adversary situation.
- ☐ Identify adversary capabilities.
- ☐ Analyze the strengths and weaknesses of the adversary's reconnaissance, surveillance, and target acquisition (RSTA) capabilities against FP-related targets.
- ☐ Determine the sources of the adversary's information.
- ☐ Assess the degree of risk the adversary is willing to take in order to attack various types of FP targets.
- ☐ Determine which types of targets the adversary considers most valuable.
- ☐ Identify the goals, motivations, political or social grievances, dedication, and training of terrorist groups. Evaluate how these factors may affect target selection.
- ☐ Identify the adversary's preferred methods of attack such as bombing, kidnapping, assassination, arson, hijacking, hostage-taking, maiming, raids, seizure, sabotage, or use of NBC weapons.
- ☐ Determine how and from where the adversary receives external support.

DETERMINE ADVERSARY COURSES OF ACTION.

- ☐ Identify the adversary's likely objectives and desired end state.
- ☐ Identify the full set of COAs available to the adversary.
- ☐ Evaluate and prioritize each COA.
- ☐ Develop each COA in the amount of detail time allows.
- ☐ Identify initial collection requirements.
- ☐ Identify the adversary's most likely targets by matching friendly vulnerabilities against adversary capabilities, objectives, and risk acceptance.
- ☐ Assess the status of specific types of support activities that may indicate the adoption of a specific COA.
- ☐ Identify possible infiltration routes, assembly areas, and surveillance locations near each of the adversary's likely objectives.

Additional information and specific guidance can be found in Joint Publication 2-01.3 (*Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*).

JIPB ANALYSIS

While the following sections are not a complete JIPB treatment, the information and associated TTPs may be used for JIPB or other JFOB intelligence planning purposes.

1. The Battlespace Defined (see Figure 3-2)

a. **Mission Analysis.**

(1) On 19 March 2003, the United States and its Coalition partners began Operation Iraqi Freedom (OIF), the multinational effort to liberate the people of Iraq from the oppressive regime of Saddam Hussein. After nearly a dozen years of Hussein's non-compliance with UN Security Council Resolutions, the U.S. led a Coalition after months of diplomatic solutions failed. The Coalition fought to achieve these specific aims:

(a) Find and eliminate Iraq's weapons of mass destruction (WMD).

(b) Capture terrorists and disestablish suspected terrorist cells.

(c) Secure Iraqi oil fields and offshore oil terminals to preserve the environment and guard the Iraqi economy from sabotage.

(d) End UN sanctions and provide immediate humanitarian assistance.

(e) End Saddam Hussein's dictatorship.

Figure 3-2. The Iraq Battlespace (from *The World Fact Book*)

(f) Help the Iraqi people transition to a non-threatening, representative form of self-government.

(2) Although the military action concluded quickly, insurgent forces moved in, attempting to fill a power vacuum created by the dismantling of the Saddam Hussein regime. The resulting violence against Coalition forces was initially focused on disrupting transition work, embarrassing the United States and destroying the Coalition. Since the Iraqi national elections of 30 January 2005, more Iraqis have been killed than Coalition service members.

(3) Political and economic stability in post-Saddam Hussein Iraq depends on a government of all peoples of present-day Iraq. The transition to political pluralism is not easy because Iraqis lived more than three decades under Saddam Hussein's one-party dictatorial system. Coalition forces must ensure a peaceful

means for political parties to coexist, with respect to their differences. This political pluralism, which is one of the most elementary foundations of democracy, is a process that requires time to shape. The aim of the transfer of power from the U.S. and Coalition administration to the newly formed Iraqi government is a progressive shift of power, together with the consolidation of new Iraqi political institutions.

(4) The Coalition mission remains to organize, train, equip, and mentor Iraqi Security Forces, in order to support Iraq's ultimate goal of a unified, stable and democratic Iraq. The end state of the new Iraqi government is one which provides a representative government for the Iraqi people; is underpinned by new and protected freedoms for all Iraqis and a growing market economy; and is able to defend itself and not pose a threat to the region. The Coalition will continue to transition responsibilities to Iraqi Security Forces until the leadership and loyalty of the Iraqi Security Forces are sufficient enough to take on the insurgency and ultimately defeat it without the Coalition presence.

b. **Battlespace Boundaries**

(1) Iraq is located in the Middle East, bordering the Persian Gulf, between Iran and Kuwait. The total area is 437,072 sq km (land: 432,162 sq km; water: 4,910 sq km), roughly twice the size of the state of Idaho. Iraq is within the United States Central Command (USCENTCOM) Area of Responsibility (AOR)

(2) Iraq land boundaries total 3,650 km. Land boundaries along its border countries are Iran, 1,458 km; Jordan, 181 km; Kuwait, 240 km; Saudi Arabia, 814 km; Syria, 605 km; and Turkey, 352 km. Iraq's coastline is 58 km, with 12 nm of territorial sea.

(3) The Iraqi terrain is mostly broad plains. There are reedy marshes along the Iranian border in the south with large flooded areas and mountains along the borders with Iran and Turkey. The lowest point is the Persian Gulf (0 m elevation); the highest point is an unnamed peak (3,611 m elevation). Other notable peaks are Gundah Zhur (3,607 m elevation) and Kuh-e Hajji-Ebrahim (3,595 m elevation). The most significant natural hazards are dust storms, sandstorms, and floods.

2. The Battlespace Effects

a. **Weather and Climate.** The Iraqi climate is mostly desert, with mild to cool winters and dry, hot, cloudless summers. The northern mountainous regions along the Iranian and Turkish borders experience cold winters with occasionally heavy snows that melt in early spring, sometimes causing extensive flooding in central and southern Iraq.

(1) The extremely hot, dry, clear summer months last from May through October. Daytime temperatures range from 22-29°C (72-84°F) to 37-43°C (100-110°F). Maximum summer daytime temperatures can exceed 46°C (115°F). Temperatures are cooler in the northeast highlands. The summer months also feature strong winds and sandstorms. Baghdad averages five dust storms a month during July. During the winter, the mean minimum temperatures range from near freezing to near 5°C (41°F). Daily maximum temperatures rise to around 17°C (64°F); however, temperatures are colder in the highlands.

(2) Ninety percent of rain falls between November and April. Most of that falls between December and March. The remaining six months, particularly June through August, are dry. Precipitation is highest in the northeast highlands, which receives 760 to 1,000 mm (30 to 40 in.) of rain (and sometimes snow) annually. Mean annual rainfall ranges between 100 and 170 mm (4 to 7 in.) elsewhere in the country.

(3) The summer months also feature two types of wind. The southerly and southeasterly *sharqi* is a dry, dusty wind with occasional gusts of 80 km/hr that occurs from April to early June and again from late September through November. From mid-June to mid-September, the prevailing wind is called the *shamal*; it is a steady wind that blows from the north and northeast. The arid air brought by the *shamal* allows the sun to heat the land surface, but the constant breeze has some cooling effect.

b. **Terrain.** Within the Iraq area of operation (AO), there are two dominating battlespace environments: the desert, and the urban area. Each environment has unique effects.

(1) Desert environments are arid regions, usually partly covered by sand, having scant vegetation, an annual rainfall of 250 mm (10 in.) or less, and extreme temperature ranges. Precautions must be taken to protect individuals and equipment.

(a) *Personnel Effects.* The desert is not a pristine environment. Diseases commonly found in a desert environment include plague, typhus, malaria, dysentery, cholera, and typhoid. Potable water is the most basic need in the desert. In desert terrain, service members need approximately 9 quarts of water each day. It is important to separate drinking and non-drinking water. Drinking any water from an untested source is dangerous and will likely cause illness. Because of water shortages, sanitation and personal hygiene are often difficult to maintain in arid regions. If neglected, sanitation and hygiene problems may cripple entire units. Heat illnesses are common in desert environments. Psychologically, the monotony of the desert, its emptiness, and the fear of isolation can eventually affect

personnel. The relatively constant climatic conditions add to this monotony, and boredom lowers morale.

(b) *Equipment Effects.* The extreme conditions in an arid environment can damage military equipment and facilities. Temperature and dryness are major causes of equipment failure, and wind action lifts and spreads sand and dust, clogging and jamming anything that has moving parts. Vehicles, aircraft, sensors, and weapons are all affected. Rubber components, such as gaskets and seals, become brittle, and oil leaks are more frequent. The desert takes a particularly heavy toll on tires. Modern forces rely heavily on the electronics in computers, radios, sensors, and weapon systems. The intense heat of the desert adds to the inherent heat that electrical equipment generates. Heat must be considered with respect to weapon effectiveness as well. Besides heat, dust and sand are very serious impediments to the efficient functioning of equipment in the desert. Dust adversely affects communications equipment, such as amplifiers and radio teletype sets. The winds blow sand into engines, fuel, and moving parts of weapons, which can reduce equipment life by up to 80 percent. The sandblasting also affects optical glass and windshields, as sand particles can scratch the surface, damaging the equipment.

(c) *Combat Operations Effects.* The key to success in desert operations is mobility. Trafficability and cross-country movement are critical to tactics in the desert. Trafficability is generally good in the desert, but it cannot be assumed. Salt marshes, wadis, shifting sand, and/or rocky areas can render some areas unsuitable. Given ample fuel and water, however, areas can be circumvented. Because of the loose surface material, movement can easily be detected by the sand and dust kicked up. To avoid detection, movement at night is an option. Dust is still a problem, but temperatures are cooler, and the element of surprise is not necessarily lost. Logistical support is more critical in arid regions because of the few manmade features and the lack of resources available from the terrain. Logistics weighs heavily on desert operations, but it must not dictate the plan.

(2) Urban environments pose enormous difficulties for planning and conducting military operations. The heightened risk of collateral damage during operations in urban environments partially offsets U.S. technological superiority and provides adversaries with expanded opportunities to exploit U.S. military doctrine. Consequently, urban combat options available to planners and leaders are generally more restrictive. International law and

self-imposed political constraints also severely restrict maneuver options.

(a) The densities of both people and buildings in urban areas create familiar operational difficulties for a deployed force. Structures and public works infrastructure inhibit maneuver and firepower, open and close fields of fire, and severely degrade command and control (C2) capabilities. Urban residents create conditions for restrictive rules of engagement, increase stress on service members and logistics capabilities, and confuse threat identification. The nature of built-up areas themselves changes over time. The effects of rubble, population movements, and the psychological strain on service members that operate within an area dense with information and decision points degrade situational awareness and affect morale and decision-making capabilities.

(b) Urban populations are composed of many groups and subgroups. Each group has its own needs, interests, intentions, and capabilities. Relationships that exist among groups might play critical roles in operations. Cultural differences can strain relations between the friendly force and the resident population if not understood and appreciated. People going about their daily routines can unwittingly hamper friendly objectives.

(c) Urban population groups and subgroups increase the number of elements to be identified and assessed as potential threats to the friendly force. They also increase the number of potential groups able to assist the friendly force. The presence of noncombatants can escalate tactical actions to episodes of strategic importance. Current doctrine often engenders an “us-versus-them” mentality that might create gaps in intelligence and barriers to complete analysis.

c. **Socio-Political.**

(1) The *Coalition Provisional Authority* transferred sovereignty to the Iraqi Interim Government (IIG) in June 2004. The election of its president, Ghazi al-Ujayl al-YAWR, was held in January 2005.

(2) *Population Demographics.*

(a) Iraq has a population of approximately 25 million based on July 2003 estimates. The majority (75 percent) of Iraqis are Arabs, though there is a sizable Kurdish minority that comprises 20 percent of the population. The remaining 5 percent is comprised of Turkmen, Assyrian, and others. The Arab population is split between the Shi’a majority in the south and the Sunni, who live mostly in the central part

of the country around Baghdad. Arab Shiites are currently the majority in Iraq, comprising between 55 to 60 percent of the population; Sunni Kurds are estimated to comprise 20 percent and Arab Sunnis 15 to 20 percent of the total population. The Shi'a have been traditionally persecuted by the Sunni.

(b) The Kurds form a majority in the north and northwest of the country where they were forced to settle due to economic constraints and border crossing restrictions. Most are herdsmen and farmers, though many have moved to the cities, particularly Mosul, Kirkuk, and Sulaymaniyah. The Kurds are divided into three separate groups. These groups' inability to reconcile their differences prevented them from presenting a unified front to both Saddam and the world.

(c) Two Arab groups have not been assimilated into the population. The "Marsh Arabs," who inhabited the lower delta of the Tigris and Euphrates Rivers until the Iraqi government drained 90 percent of the marsh area, have fled to Iran. The second group is a small Bedouin population who wander the desert regions. Seventy-five percent of the population lives in the flood plains that make up only 25 percent of the total land area. Nearly 70 percent of the people live in urban centers, with Baghdad being the largest city.

(3) *Religion.* Islam is the state religion of Iraq. About 97 percent of the population belongs to either the Shi'a (60 percent) or the Sunni (37 percent) sect. The better-educated Sunni have traditionally dominated the government. Since 1958, most members of the government have been Sunni. The Kurds are also Sunni, but their religious practices differ from those of the Arabs.

(a) The Islamic religion is based on the "submission to the will of God (Allah)" and governs everything from politics to crime and punishment to morality in daily life. The Koran and Sunnah are the two basic sources of Islamic teachings. Although Iraq is a secular country, the traditional Islamic culture predominates, with Koranic Law playing an active role in the day-to-day life in the country.

(b) The Islamic year is based on the lunar cycle, consisting of twelve months of 29 or 30 days each, totaling 353 or 354 days. Each new month begins at the sighting of a new moon. The Islamic Hijri calendar is usually abbreviated A.H. in Western languages from the Latinized "Anno Hegirae." Muharram 1, 1 A.H. corresponds to 16 July 622 C.E. (Common Era). The Hijrah, which chronicles the migration of the Prophet Muhammad from Mecca to

Medina in 622 A.D., is early Islam's central historical event. To Muslims, the Hijri calendar is not just a sentimental system of time reckoning for dating important religious events, e.g., Hajj (pilgrimage to Mecca); it has profound religious and historical significance.

3. Evaluation of the Adversaries

a. **Composition.** Forces in Iraq face a terrorist adversary using guerrilla style, low-intensity tactics. The terrorist opposition is probably made up of the following types of individuals and groups or has attracted similar individuals.

(1) Remnants of military forces still loyal to Saddam Hussein.

(2) Remnants of the Baath Party.

(3) Sunni Muslims loyal to Saddam Hussein.

(4) Disgruntled Iraqi citizens who have lost patience with the U.S.-led Coalition.

(5) Al Qaeda and other voluntary terrorist-type forces that have crossed over into Iraq to "liberate" the country from Coalition Forces.

b. **Tactics.** The term jihad is often used in reference to Osama bin Laden and related followers. They consider the terrorism that they perpetuate a jihad. The word jihad means struggle in Arabic. This means a struggle between the forces of Allah (good) and the forces of evil. Some examples (not all inclusive):

(1) In August 2003, the Jordanian Embassy in Baghdad was bombed, with 11 people killed.

(2) A terrorist bomb destroyed U.N. headquarters in Baghdad, killing 22 people.

(3) A car bomb killed 125 people in Najaf, including the prominent Shia leader Ayatollah Mohammed Baqr-al-Hakim.

(4) A female member of the Interim Governing Council was assassinated in September 2003.

(5) Dozens of people were killed when the Red Cross office in Baghdad was bombed.

c. **Key Adversary Groups.** The following paragraphs summarize the mission, strength, structure, and capabilities of some of the key insurgent groups in Iraq.

(1) **Saddam's Martyrs** ["Men of Sacrifice"] or Fedayeen Saddam (Including Former Regime Loyalists (FRL) or Baath Party Loyalists).

MISSION: Leading guerrilla-style attacks on Coalition Forces in Iraq. They were relied upon to protect the president and his family, put down dissent and carry out much of the police's dirty

work. Some of this work consisted of enforcing night time curfews, controlling main intersections and blocking entrances to major thoroughfares and sensitive areas.

STRENGTH: The Fedayeen numbered more than 15,000 (Spring 2003).

STRUCTURE: The Fedayeen Saddam was comprised of young and politically reliable paramilitary soldiers that may still be active against perceived domestic agitators and opponents of the former regime. These soldiers have been recruited from Tikrit, and areas within the Sunni Triangle. The unit reported directly to the Presidential Palace, rather than through the army command, and was also responsible for conducting patrols and anti-smuggling duties. The Leader was Qusay, one of Saddam's sons who were killed in Iraq. The deputy commander was Staff Lieutenant General Mezahem Saab Al Hassan Al-Tikriti.

CAPABILITIES: Small arms and rocket-propelled grenades, improvised explosive devices (IEDs), suicide bombings, and sniper shootings. They have also used deceptive tactics to unsettle Coalition troops and employed torture and assassination to hold Iraqi civilians hostage and, at times, to force them to fight.

UNIFORM: In the past they have worn all black outfits and sometimes civilian clothes.

LOCATION: Throughout Iraq, especially around Tikrit.

(2) **Ansar al-Islam** (Supporters of Islam in Kurdistan); Jund al-Islam; Soldiers of God.

MISSION: To establish an independent Islamic state in northern Iraq.

STRENGTH: About 700 members.

STRUCTURE: Ansar al-Islam is a radical Kurdish Islamic group that is supportive of the ideals of fundamental Islam. This group has ties with the Taliban and Al-Qaeda. It is the most radical group operating in the Iraqi Kurdistan region. Ansar al-Islam was established in December 2001 after a merger between Jund al-Islam, led by Abu Abdallah al-Shafi'i, and the Islamic Movement splinter group, led by Mullah Krekar. Both leaders are believed to have served in Afghanistan. The group is based in Biyarah and surrounding areas near the border with Iran.

CAPABILITIES: IEDs and car bombs (Toyota Land Cruisers). They have received small arms from Al-Qaeda training in Afghanistan. Al-Qaeda has also provided financial assistance to Ansar al-Islam. They claim to have produced cyanide-based toxins, ricin, and alfa toxin.

UNIFORM: Civilian clothes.

LOCATION: Based in the Kurdish-controlled northern provinces of Iraq. Its operations bases are in and around the villages of Biyarah and Tawela, which lie northeast of the town of Halabja in the Hawraman region of Sulaimaniya province bordering Iran.

(3) Formerly known as **The Special Republican Guard (SRG)** (although now referred to as **Baath Party Loyalists** or FRL).

MISSION: The SRG was responsible for escort and protection of Saddam Hussein during his travels, for protection of his presidential palaces, and for the security of Baghdad and was to act as an emergency-response force in case of a rebellion or a coup.

STRENGTH: 26,000 total troops; now dispersed amongst population.

STRUCTURE: This once elite paramilitary unit was founded in early 1992. Originally composed of thirteen battalions of 1,300 to 1,500 men each, this force grew to upwards of 26,000 troops in 13 battalions. Recruits were drawn from Tikrit, Baiji, al-Sharqat and small towns south and west of Mosul and around Baghdad.

CAPABILITIES: Air Defense, Small Arms, Human Shields. Rumors Saddam used SRG facilities as a storage space for his chemical and biological weapons.

UNIFORM: Civilian attire.

LOCATION: Baghdad and Vicinity of Baghdadal-Bu Nasir tribe.

(4) Formerly known as **Al Amn al-Khass** (Special Security Service); Special Security Organization; Presidential Affairs Department.

MISSION: Duties included protecting the Baath leadership in Iraq, monitoring personnel holding sensitive positions, enforcing loyalty of Special Security Service personnel to the regime, collecting and analyzing intelligence on the enemies of the state, and providing a rapid-response intervention force used during emergencies.

STRENGTH: Staff of 5,000 officers and soldiers.

STRUCTURE: The Brigade of Amn Al-Khass Special Branch elements included the Security Office. The Manager of the Director General's Office is Suleiman Hajim Al Nasiri, the Secretary to the Director General is Moyed Sami Ahmad Al Douri, and the Secretary to the Manager is Abbas Ayash Al Nasiri. The members of Amn Al-Khass were chosen because they had proved to be good soldiers and were extremely loyal.

CAPABILITIES: Small Arms.

UNIFORM: Civilian attire.

LOCATION: Located in the Hai Al Tashriya district of Baghdad.

(5) **Baath Party Loyalist** (means renaissance or rebirth in Arabic.).

MISSION: Its main ideological objectives were secularism, socialism, and pan-Arab unionism.

STRENGTH: 2.4 million people were Baath Party members although only a small number of those are conducting attacks against Coalition troops.

STRUCTURE: Command was once held by Saddam Hussein, who is now out of power.

CAPABILITIES: Rocket propelled grenade **(**RPG), IED, and other small arms.

UNIFORM: Civilian attire.

LOCATION: Founded in Syria, now spread throughout Syria and Iraq. Previous headquarters was in Basra, Iraq.

d. **Weapons.** The primary weapon threat against Coalition forces continues to be rockets, artillery, and mortars (RAMs) and IEDs.

(1) ***Improvised Explosive Devices (IED).*** An IED is a homemade device designed to cause injury or death by use of explosives alone or in combination with chemical, biological, or radiological (CBR) materials. IEDs can utilize commercial, military, or homemade explosives or military ordnance and ordnance components. IEDs fall into three categories.

(a) Package IEDs usually consist of mortar and artillery projectiles as the explosive device. The most common explosives used are military munitions, usually 120mm or greater mortar, tank, or artillery munitions.

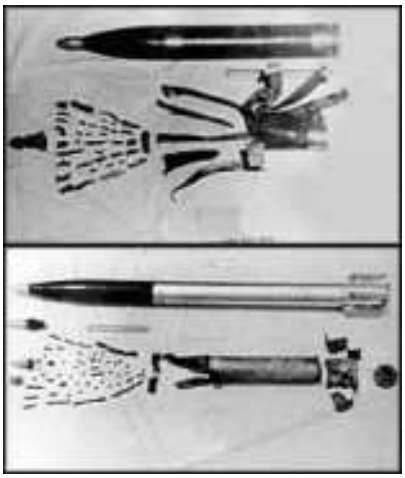
(b) Vehicle-Borne IEDs (VBIEDs) are devices that use a vehicle as the device package or container and delivery mechanism. VBIEDs use large amounts of explosives (from 100 to over 1,000 lb), limited only by the size of the vehicle. The explosive charge has included items like mortar rounds, rocket motors and warheads, artillery rounds, and plastic explosives. VBIED suicide bombs employ the same methods and characteristics of other package or vehicle bombs that use a command detonation firing system.

(c) A Suicide Bomb IED presents a difficult threat for Service members. The aim of the bomber is not to commit suicide, but to kill or injure as many other service members and civilians as possible. A person-borne suicide bomb usually employs a high-explosive and uses a switch or button the person activates by hand. Explosives with fragmentation can be contained in a vest, belt, or clothing that is specifically modified to carry this material concealed.

(2) ***Rockets.***

A rocket consists of a warhead containing the explosive material, a body containing the fuel powering the rocket's flight, and a tail in which the engine is located, which also stabilizes the rocket during its flight. Rockets can be launched by operators who are near the rocket launcher when it is fired, or by means of a delayed timer. The devices are easy to move and to conceal, and can be assembled on the back of a vehicle in order to make it quicker to move them to the launch site and take them away after firing.

The Katyusha (Little Katie) rocket is of Soviet origin. The term is now often used to describe small artillery rockets in general, whether they are Soviet-derived or originally built. The Katyusha rocket launcher has played an important part during conflicts in the Middle East, with the rockets used by almost all parties.



107mm Katyusha Rocket
Effective Range: 9 kilometers
Ammunition: 6.4-8 kg HE/Fragmentation Warhead
Other: Can be employed singly or in a multiple launch configuration (6-12 tubes)

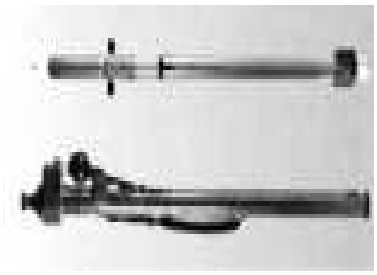
122mm Katyusha Rocket
Effective Range: 18 kilometers
Ammunition: 18 kg HE/Fragmentation Warhead
Other: Can be employed singly or in a multiple-launch configuration (30-40 tubes)

RPG-7
Shoulder-fired Anti-Tank Weapon
Effective Range: 500 meters
Rate of Fire: four to six rounds a minute
Ammunition: 72-105mm grenade launched from a 40mm tube
Other: Can penetrate 260mm armor

RPG-22
Shoulder-fired Anti-Tank Weapon
Effective Range: 300 to 500 meters

Ammunition: 73mm grenade
Other: AP Grenades can penetrate 600mm rolled homogenous armor

SA-7 GRAIL
Shoulder-fired Surface-to-Air Anti-Aircraft Rocket System
Crew: 1
Maximum Range: 5,500m
Minimum Range: 500m
Maximum Altitude: 4,500m
Minimum Altitude: 18m



SA-16
Shoulder-fired Surface-to-Air Anti-Aircraft Rocket System
Crew: 1
Maximum Range: 5,000m
Minimum Range: 500m
Maximum Altitude: 1,500m
Minimum Altitude: 10m

(3) ***Artillery.***

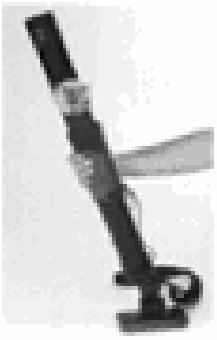
The indirect fire threat in Iraq is not from the direct employment of artillery. Instead, the threat is from IEDs that utilize artillery projectiles, fuses, primer, or propellant. Artillery munitions within the theater are common and easy to obtain. While any military device containing explosive material may be used as an IED, the NATO-standard artillery munitions (or equivalent) listed below are most common.

105mm Artillery Projectile
Use: Fragmentation and blast effect.
Body Material: Forged Steel
Filler Weight (NATO Equivalent): 4.60-5.08 lbs Comp B; 4.25-4.80 lbs TNT
Other: May use a fixed or semi-fixed configuration with propellant and primer contained in a cartridge or casing.

155mm Artillery Projectile
Use: Blast effect, fragmentation, and mining.
Body Material: Forged Steel
Filler Weight (NATO Equivalent): 6.98 kg Comp B; 6.62 kg TNT

Artillery Propellant
Used with separate-loading munitions, the explosive propellant is adjusted to vary the range of the projectile. Propellant comes in different sizes, configurations, and packages.

(4) ***Mortars.***



Al-Jaleel (M70) 60mm Commando Mortar
Crew: 1
Rate of Fire: 20 to 25 rounds a minute
Muzzle Velocity: 211 m/s
Maximum Range: 2,540 meters
Minimum Range: 60 meters
Ammunition: 60mm HE

Al-Jaleel 82mm Mortar
Crew: 8
Rate of Fire: 25 rounds a minute
Muzzle Velocity: 211 m/s
Maximum Range: 3,040 meters
Minimum Range: 85 meters
Ammunition: 82mm HE, Illumination, Incendiary, Smoke

Al-Jaleel 120mm Mortar
Crew: 5
Rate of Fire: 5-8 rounds a minute
Muzzle Velocity:
Maximum Range: 5,400 meters
Minimum Range: 200m
Ammunition: 120mm HE, Illumination, Incendiary, Smoke

Mortar Rounds
Use: Fragmentation, Blast Effect, Incendiary, Smoke, Illumination.
Body material and filler weights vary by projectile.

Mortar rounds, like artillery projectiles, are also used in IEDs.

(5) ***Small Arms.***

AK-47
Function: 7.62mm Assault Rifle
Rate of Fire: 100 rounds a min; cyclic 600 rounds a minute
Effective Range: 300 meters
Other: The AK-47 has become one of the most used assault rifles in the world. The modern version is the AKM rifle. Iraq has produced two copies: the 5.56mm and
7.62mm Tabuk rifles**.**

RPK-47
Function: 7.62mm Light Machine Gun
Rate of Fire: 150 rounds a minute in automatic mode
Effective Range: 460 meters
Other: The RPK-47 is essentially a variant of the AK-47 assault rifle with a longer, heavier barrel and is fed by a 30-, 40-, or 45-round box magazine.

PKM
Function: 7.62mm General Purpose Machine Gun
Rate of Fire: 250 rounds a min; cyclic 650 rounds a min
Effective Range: 1000 meters
Other: Can be fed by either 100-round magazine or 200/250-round belt boxes.

RPK-74
Function: 5.45mm Light Machine Gun
Rate of Fire: 150 rounds a minute in automatic mode
Effective Range: 800 meters
Other: The RPK is essentially a variant of the AK-74 assault rifle with a longer, heavier barrel and is fed by a 45-round curved box.

AL QUDS
Function: 7.62mm Squad Automatic Rifle
Rate of Fire: cyclic 680 rounds a minute
Effective Range: 300+ meters
Other: The Al Quds is an Iraqi manufactured heavy barreled version of the 7.62mm AKM assault rifle and uses the standard AKM 30-round box magazine.

4. Adversary Courses of Action (COAs).

a. There are several competing interests among adversary groups in Iraq. In all cases, the objectives are to retain control in Iraq and to destroy, damage, or impede Coalition forces' attempts to enforce democratic processes in Iraq.

(1) FRLs want to retain psychological dominance over the Iraqi populace. Attacks against Coalition Forces, driven by a sense of revenge against Americans, are seen as an Arab victory. The desired end state is a return to power and influence.

(2) Religious fundamentalist cells, foreign fighters and Iranian insurgents initially looked to establish safe havens capable of survival. Their goals are to influence the frustrated populace, kill Americans, fight the Jihad ("Holy War") and kill Americans. The desired end state is expulsion of "infidels" from Middle East/Holy Land.

(3) Ethnic infighting and violence are characterized by demonstrations, protests, tribal territorial and economic disputes, and disputes over religious tolerance and minority rights. Groups typically suffer from a real or perceived political power imbalance, with a feeling of disenfranchisement by their populations. Ethnic issues are historically embedded and very divisive. Desired end states are usually one group displacing the other.

(4) Adversary terrorist tactics appear to be shifting away from Coalition Forces and toward the Iraqi populace. Some examples (not all inclusive):

(a) Previously most of the targets had been U.S. personnel and officials associated directly with U.S. reconstruction efforts. Since late October 2003, more Iraqi citizens appear to be targeted.

(b) The suicide bombing of an Italian police base in Nasiriyah in November 2003 may also signal that terrorist forces

have shifted their attacks to regions located outside the capital.

(c) The murder of Japanese diplomats and Spanish civilians working in Iraq appears to indicate that terrorists are targeting allied personnel in an effort to discourage Coalition countries from sending support to U.S. forces in Iraq.

b. **Courses of Action.**

(1) ***COA 1 (Improvised Destructive Devices).*** Adversary forces gain residence on Coalition base camps and facilities as employees of a contractor company. The adversary cell then obtains gasoline, diesel, propane, chlorine, or other hazardous materials. The materials are fashioned into weapons and transported to a high-value target (HVT). The device is then deployed or detonated against the population.

(2) ***COA 2 (Smuggled Explosives).*** Adversary forces enter Coalition base camps and facilities while employed as Police Service, Iraqi National Guard, or Local Nationals (LNs) with an appropriate escort. Insurgents drop explosive materials at a predetermined location while conducting business within the facility. Another adversary working or living on the base recovers the explosive material and incorporates it into an IED. The IED is then delivered to a pre-selected HVT where it is detonated, causing death and/or damage to Coalition Forces or materiel.

(3) ***COA 3 (Stolen or Salvaged Explosives).*** An adversary cell living or working on an installation steals or salvages explosives from poorly guarded facilities or agencies. Using their jobs to gain knowledge of HVTs, the adversaries select a target. An IED device is built in an object, which is placed on the HVT. The device is detonated either by timer or by radio.

(4) ***COA 4 (Most Dangerous).*** Any of the above COAs with an added indirect fire attack or secondary device placed to target first responders and cause maximum casualties.

c. **Proven Adversary Tactics, Techniques, and Procedures (TTP) To Date.**

(1) ***Luring or distracting service members to commit attacks.*** Any distraction, for example a pregnant woman attempting to detonate a car bomb close to a checkpoint, is possible. In one instance, a civilian vehicle pulled up to a traffic control point, and one of the occupants got out and asked for a medic. When the service member turned to call for a medic, the civilian pulled a pistol and shot the service member. Demonstrations can also be used to carry out attacks. Adversary groups may utilize demonstrators to get close to Coalition forces, attack and then

use the demonstrators as human shields to avoid being targeted.

(2) ***Using motorcycles.*** Iraqi paramilitary forces are possibly using motorcycles for transport. Motorcycles are used to move throughout cities easier than cars or trucks.

(3) ***Using flares and other devices as a warning signal.*** One observed system uses a red flare to mean a soft-skinned vehicle is in motion/leaving a JFOB. A red flare followed by a green flare means a soft- skinned vehicle is approaching an ambush point/kill zone. If a green flare alone is used, then an armored vehicle is in motion/leaving a JFOB. Other warning techniques include honking horn to warn of approaching patrols, flashing lights on and off in a continuous manner, and whistle blowing.

(4) ***Attacking convoys with RPGs from trucks.*** Members of adversary groups in small panel or pickup trucks attempt to get in and amongst Coalition convoys and fire RPGs into a Coalition vehicle from the rear of the truck.

(5) ***Using IEDs to ambush U.S. patrols on roadways.*** Adversaries use 155 mm artillery shells along with C4 explosives along major supply routes. VBIED attacks are also used.

(6) ***Using Mosques as safe havens for meetings, planning, and storing weapons.*** Mosques are being used not only as cover but also to buy and sell various types of weapons and possibly to make explosives. Adversary groups are also using locations near mosques for nightly meetings to plan Coalition attacks. Weapons, including mortars, RPGs and machine guns are being kept in houses collocated with the mosques.

(7) ***Smuggling Weapons.*** Adversary groups utilize trucks previously used to carry food or water to people in Iraq. Once food is delivered, the truck is loaded with weapons and goes out the same way it entered. The trucks can be utilized to bring weapons into the country as well. Almost any vehicle can be used for this purpose, and adversaries have resorted to hiding weapons on animals. Taxis are also suspected of smuggling concealed weapons and money inside car doors, trunks, or hidden compartments. Coffins have also been used to smuggle weapons between cities.

(8) ***Conducting surveillance of U.S. or Coalition Forces prior to an attack.*** Multiple intelligence reports indicate adversaries conduct surveillance of Coalition Forces prior to attacks.

(9) ***Employing booby-trapped caches.*** Caches may be reported to lure Coalition Forces to a cache site that has been booby trapped.

(10) ***Operating weapons markets*.** Merchants sell weapons out of cars or from crates that are set up on ground. When they see Coalition forces, they move into the market and hide weapons in the vegetables, animals, automotive parts and other sections of the market until Coalition forces leave. Some weapons markets even operate out of public bathrooms. Black market weapon dealers have bribed local police. They pay police officers to lie to Coalition forces so they can continue to sell the weapons.

(11) ***Making bombs*.** Adversaries make bombs from soda and milk cans. Children may be paid up to 150 Iraqi Dinar to pick up empty soda cans and return them to the bomb maker.

(12) ***Conducting ambushes*.** Coalition forces may be led on a "wild goose chase" to look for attractive targets, and then the unsuspecting Coalition force may be ambushed by armed assailants or may be led into a booby-trapped area. Adversaries may throw grenades at stationary targets at checkpoints and at vehicles when they break down.

RESOURCES

The following data bases and Intelink sites contain information applicable to the JIPB process and should be reviewed and evaluated to determine the availability of current data, information, and intelligence products relative to the joint force's battlespace and mission. The Intelink portal provides resources to a variety of intelligence information. Intelink is available on SIPRNET at http://www.ismc.sgov.gov.

Modernized Integrated Data Base (MIDB) is accessible via Intelink and contains current, worldwide Order of Battle (OB) data organized by country, unit, facility, and equipment.

NIMA National Exploitation System (NES) permits users to research the availability of imagery coverage over targets of interest and to access historical national imagery archives and imagery intelligence reports. NES is accessible via Intelink.

Country Knowledge Bases and Crisis Home Pages contain the best and most up-to-date intelligence products available from the Intelligence Community and are accessible via the Defense Intelligence Agency (DIA) Intelink Home Page.

Signals Intelligence (SIGINT) On-line Information System (SOLIS) data base contains current and historical finished SIGINT products.

Modernized Defense Intelligence Threat Data System (MDITDS) is a collection of analytic tools that support the retrieval and analysis of information and intelligence related to counterintelligence, indications and warning, and counter terrorism.

Community On-Line Intelligence System for End Users and Managers (COLISEUM) data base application allows the user to identify and track the status of all validated crisis and non-crisis intelligence production requirements.

The following data bases are accessible via **Secure Analyst File Environment** (SAFE) Structured Data Files:

Intelligence Report Index Summary File (IRISA) contains index records and the full text of current and historical intelligence information reports.

All Source Document Index (ASDIA) contains index records and abstracts for hardcopy of all source intelligence documents produced by DIA.

Intelligence Collection Requirements (ICR) is a register of all validated human intelligence (HUMINT) requirements and taskings.

The Antiterrorism Enterprise Portal (ATEP) is located at https://www.atep.smil.mil. Menu items to the left of the main page include Country Threats and Intel sections.

The National Geospatial Intelligence Agency (NGA) provides timely, relevant, and accurate geospatial intelligence in support of national security. Their web site is located at http://www.nga.smil.mil.

The USCENTCOM SIPRNET web page is located at http://www.centcom.smil.mil. Intelligence information related to the USCENTCOM AOR can be found under the Intel Directorate (http://ccj2.centcom.smil.mil).

REFERENCES

1st Infantry Division Soldier's Handbook to Iraq (APO AE: First Infantry Division, 2003). (Available from www.globalsecurity.org/military/library/ report/2003/)

DA PAM 550-3 (Area Handbook Series). *Iraq: A Country Study*, 1990. (Mil. Pubs.)

FM 2-0. *Intelligence*, 17 May 2004. (Available from www.train.army.mil)

FM 34-3. *Intelligence Analysis*, 15 March 1990. (Available from www.train.army.mil)

FM 34-81-1. *Battlefield Weather Effects*, 23 December 1992. (Available from www.train.army.mil)

FM 34-130. *Intelligence Preparation of the Battlefield*, 8 July 1994. (Available from www.train.army.mil)

"Iraq." *The World Fact Book* (Washington DC: Central Intelligence Agency, 2005). (Available from www.cia.gov/cia/publications/factbook/ index.html)

Iraq: An Introduction to the Country and People (Washington, DC: Marine Corps Institute, 2003). (Available from www.globalsecurity.org/military/ library/report/2003/)

Iraq Country Handbook (Washington DC: U.S. Department of Defense Intelligence Production Program, 2002). (Available from www.globalsecurity.org/wmd/library/news/iraq/2002/iraq-book.htm)

JP 2-0. *Doctrine for Intelligence Support to Joint Operations*, 9 March 2000. (Available from www.dtic.mil/doctrine)

JP 2-01. *Joint Intelligence Support to Military Operations*, 7 October 2004. (Available from www.dtic.mil/doctrine)

JP 2-01.1. *Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting*, 9 January 2003. (Available from www.dtic.mil/ doctrine)

JP 2-01.3. *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*, 24 May 2000. (Available from www.dtic.mil/doctrine)

JP 2-03. *Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations*, 31 March 1999. (Available from www.dtic.mil/doctrine)

JP 3-07. *Joint Doctrine for Military Operations Other Than War*, 16 June 1995. (Available from www.dtic.mil/doctrine)

JP 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 1998. (Available from www.dtic.mil/doctrine)

JP 3-10.1. *Joint Tactics, Techniques, and Procedures for Base Defense*, 23 July 1996. (Available from www.dtic.mil/doctrine)

Chapter 4

RISK ASSESSMENT

Contents

INTRODUCTION

A JFOB risk assessment is a prioritized list of risks with associated information such as vulnerabilities that are the basis of the risk. The assessment is the result of a risk analysis. This chapter describes the risk analysis concept for a JFOB and explains how this analysis is used to develop the risk assessment.

There are eight major components of a risk analysis. They are identify key assets, including critical infrastructure; determine threat likelihood for threat-asset pairs; determine and assess vulnerabilities of assets; assess incident response (IR) capabilities; develop event likelihood rating data; develop consequences data; assign risk score and priority; produce risk analysis products (See Figure 4.1).

The risk analysis process in this chapter is appropriate for JFOB pre-deployment, deployment, and redeployment operations phases. In pre-deployment a risk analysis could involve anything from planning for a new JFOB with whatever level of information is available to planning for deployment to a mature JFOB that has performed risk analyses and has implemented risk mitigation courses of action (COAs). A risk analysis can be performed with partial information. For example, the total list of units that will occupy the JFOB may not be certain until deployment. Once deployed, a unit can improve the defensive situation by assessing and reducing risks based on real, rather than projected, interpreted, or second-hand information.

Performing a risk analysis should be a task-organized team effort under the operations officer's lead and should involve the force protection officer (FPO), security, legal, facilities engineering, chemical, biological, radiological, and nuclear (CBRN) representative, and other subject matter experts as needed. It is possible for one person or a small group to work through the process and

develop a draft for review with team members having expert knowledge in selected areas.

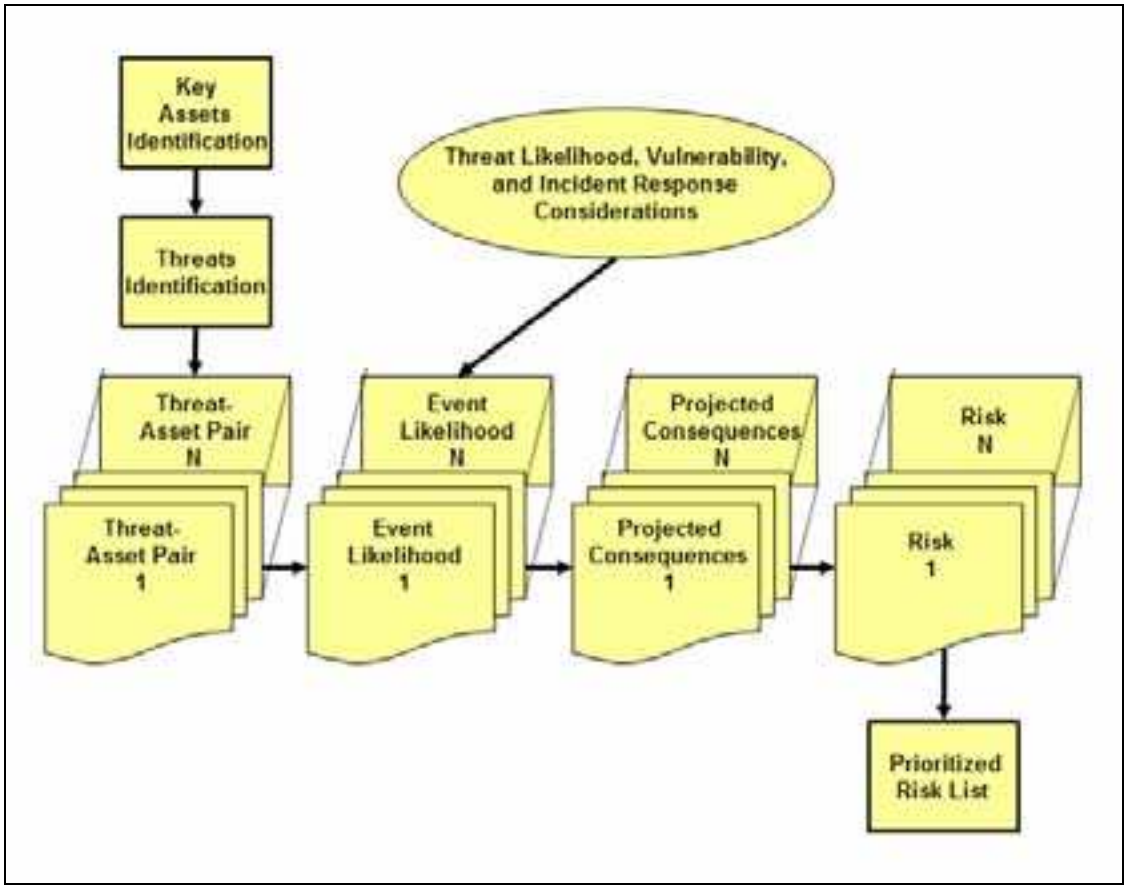


Figure 4-1. Risk Analysis Process Overview

RISK ANALYSIS APPROACH ALTERNATIVES

This chapter provides information on two risk analysis approaches, the expedient solution approach and the formal solution approach. The expedient solution approach is advocated when there is a compressed schedule or information uncertainty. An expedient solution approach shortcuts the formal solution approach. An expedient solution approach could be followed by a formal solution approach when more information becomes available and there is sufficient time to use it. The formal solution approach provides a more complete answer.

Expedient Solution. This can be used with or without a computer, requires at least a minimum tool set of maps and field risk analysis forms (see pp 4 – 20-22), and relies heavily on estimates. For example: “based on your experience, estimate the number of fatalities when the vehicle-borne improvised explosive device (VBIED) detonates at this location.”

Formal Solution. This requires the use of a computer and relies more on computerized tools. For Example: “use the AT Planner tool to calculate the number of VBIED fatalities.”

TOOLS

Performing a risk analysis follows a logical, relatively simple process that is complicated by the number of assets, threats, and vulnerabilities that must be investigated with some combination of tools. The following is a basic list of tools that can be of assistance in following the step-by-step process, reducing the work effort, developing an audit trail, and simplifying communication.

Common Operating Picture Graphics. This is required for expedient or formal solution use. Detailed maps of the JFOB site provide a way to visualize many information categories, such as asset locations. The maps can be any version of sketches, overhead imagery, or aerial photography. They can be used for annotating such information as perimeter and entry control point (ECP) locations and layouts, key assets locations, highest risk assets, vulnerable locations and notes, and incident response team routes. Maps of the surrounding region can be used to annotate information, such as possible attacker approaches and potential indirect fire sites. These maps are likely classified CONFIDENTIAL or SECRET.

Joint Antiterrorism (JAT) Graphics. Personnel using a computer to do a risk analysis will find the JAT Guide provides a no-cost-ever, geographic information system tool called JAT Graphics, which can be used on practically any personal computer. JAT Graphics can be used to produce common operating picture graphics/maps with annotation and map overlays to any level of detail. Unclassified overhead imagery at a 1 m or 0.6 m resolution is helpful for detailed planning; data with higher and lower resolution can also be used. See Chapter 15 for more information and references. Training is required, so the JAT Guide contains self-training materiel. Engineer staff is a possible location for personnel experienced with this type tool, and other similar tools may be available at the JFOB.

Asset Value Rating, Threat Likelihood Rating, and Vulnerability Rating. These are formal solution tools. The JAT Guide contains these tools used in determining risk (see Risk Equation on page 4-5). These tools require the use of a computer. Each tool provides a series of questions, and the answers to the questions are used to calculate the asset value, threat likelihood, and vulnerability ratings.

Incident Response (IR) Capability Rating. This formal solution tool is included in the JAT Database and requires the use of a computer.

JAT Database. This is a formal solution tool. The JAT Guide contains a JAT Database tool (run with Microsoft EXCEL) that requires a computer. The current condition workbook in the JAT Database is synchronized with the risk analysis step-by-step process. When the current condition workbook is completed, the result is a prioritized risk list. This tool also contains other workbooks used to develop and compare risk mitigation action sets. Training is required, and the JAT Guide contains self-training material. Further information is provided in Chapter 15.

Field Risk Analysis Tool. This expedient solution tool, a paper-and-pencil tool substitute for the JAT Database is provided to assist personnel with performing a

risk analysis when a computer is not available. This tool is located later on pp 4 – 20-22.

Antiterrorism (AT) Planner. This formal solution, high-quality engineering model can be used to calculate the blast effects of bombs external to a facility. The output includes projected fatalities and serious injuries (personnel inside and outside the facility) and facility damage. AT Planner can also be used to determine standoff distances required to reduce blast effects to a designated level and to ascertain the benefits (or lack of benefits) of facility upgrades in decreasing attack consequences. The model is provided in the JAT Guide. It requires training, so a user's manual is included. Personnel on the engineer staff are probably familiar with this model.

Force Protection (FP) Plan Template. An FP Annex to the operations order (OPORD) should contain risk analysis results. An FP Annex template is provided in Chapter 14.

RISK ANALYSIS OVERVIEW

A risk analysis is a systematic, rational, and defendable process for identifying, quantifying, and prioritizing risks. The outcome of a risk analysis is a list of risks and the vulnerabilities that are the reasons for the risks. All or part of the prioritized risk list is recommended to the commander for mitigation. The outcome of the risk analysis is important, variations in the prioritized list that do not affect the outcome nor impact resources are not. Using the process in this handbook to perform a risk analysis for a JFOB, different teams with equivalent knowledge, skills, and capabilities will produce the same outcome.

Normally, the highest risks are recommended for mitigation, although a different strategy could be used. For example, the strategy could be to improve the defense at all mass gathering locations, regardless of their rank on the prioritized risk list.

The JFOB risk priority list and the sequence in which actions to mitigate the risks on the list are implemented are two different topics. Resource requirements, availability and implementation time for different type mitigation measures can determine the sequence in which problems are resolved.

The implementation schedule for a specific action may require interim protection measures. For example, it may be necessary to use an expedient entry control point (ECP) at some perimeter location while building up the required ECP with the required capabilities.

RISK EQUATION

The risk equation is shown below (Figure 4-2). The expedient solution employs the event likelihood and consequences, while the formal solution uses threat likelihood, vulnerability, and IR details to develop the threat likelihood. Either solution will use whatever consequences estimates are provided, although the formal solution strongly advocates the use of tools such as AT Planner.

Risk = Event Likelihood x Consequences

Event Likelihood = Likelihood of specific threat activity involving a specific asset (threat-asset pair)

= Threat Likelihood x Vulnerability x Incident Response Ratings

Consequences = Projected event fatalities, serious injuries, property and equipment damage, and mission degradation outcome for the attack.

Figure 4-2. Risk equation

Note in Figure 4-2 that neither event likelihood nor risk is the same as vulnerability, although vulnerability plays a large role in determining risk. Every asset has vulnerabilities, possibly even significant vulnerabilities. However, the risk can still be negligible since the threat likelihood might be low or the consequences of an attack may be rated negligible. Conversely, the highest risk situations could have low vulnerabilities, but the projected consequences could drive the risk to the high-priority end of the scale.

A risk analysis is performed at the level of threat-asset pairs; i.e., risk is assigned to each possible attack against each asset. This pairing means the different type of attacks and possibly the different attack points at the same asset location must be considered, i.e., suicide bomber at the entry or within the office space, or VBIED at the entrance or loading dock. Since it is too time consuming and difficult to consider all possible situations, the process emphasizes reducing the work by concentrating on more-versus-less likely events and making estimates to determine events with high-versus-low consequences, such as number of projected fatalities. This process is called filtering.

When risks have been prioritized, it is possible to group them into categories such as baseline and threat-asset pair specific by reviewing the vulnerabilities that cause the risk. Baseline refers to vulnerabilities that impact the entire JFOB or sections of it**.** Examples of baseline vulnerabilities include the following:

- *Proximity of multiple assets sufficiently close to the perimeter to permit significant damage from a VBIED outside the perimeter.*
- *Lack of training for entry control facility guards on the rules of engagement for a potential VBIED attempting to run the gate.*
- *The presence of conspicuous rocket or mortar aim points, such as towers, in close proximity to high-population areas that provide attackers with an increased likelihood of attack success.*

Threat-asset specific refers to vulnerabilities that impact a single asset. *An example is lack of dining facility (DFAC) access control that could reduce the possibility of hand-carried explosives for that specific asset location.*

RISK ANALYSIS PROCESS

The risk analysis process

- Quantifies (assigns a numerical value) to the event likelihood of suffering damage or loss and to the consequences for a specific critical asset and other assets affected in the attack if the attack occurs.
- Prioritizes the JFOB risks.
- Includes the commander's guidance and intent in the risk determination and prioritization.

In conducting a risk analysis, you should perform the steps which are described in the following sections.

Step	Formal Solution	Expedient Solution
1	Identify key assets and select those to be included in the risk analysis.	Same.
2	Link threats to the selected assets, and develop threat likelihood ratings for the threat-asset pairs.	Reduce to: Link threats to the selected assets.
3	Develop vulnerability ratings for the threat-asset pairs, and identify vulnerabilities that could be exploited by the attackers.	Reduce to: Identify vulnerabilities that attackers could exploit.
4	Develop incident response (IR) ratings for the threat-asset pairs, and identify IR-related vulnerabilities additional to those in step 3.	Reduce to: Identify IR-related vulnerabilities.
5	Use the threat likelihood, vulnerability, and IR rating results to determine event likelihood.	Reduce to: Estimate event likelihood.
6	Develop projected consequences data for the threat-asset pairs and identify vulnerabilities additional to those in step 3 that enable the consequences.	Same.
7	Develop risk scores and a prioritized risk list.	Same.
8	Develop risk analysis products that can be used to brief higher level personnel and that can be used in the FP plans (see Chapter 14) and in developing COAs to mitigate the risks.	Same.

IDENTIFY KEY ASSETS, INCLUDING CRITICAL INFRASTRUCTURE

It is DoD policy that commanders are responsible for protecting personnel and property subject to their control and maintaining their mission capability. Key assets are those personnel (military and civilian) and property (equipment, material, infrastructure) that are likely to have a high priority for protection and have high risk. Key assets include people and property both inside and outside the perimeter under control of the commander and infrastructure inside and outside the perimeter like power and water that may be needed for the mission. The infrastructure may not be under the commander's control.

A risk assessment will normally focus on a list of key assets. The identification and ranking of key assets is used to filter the list of all key assets down to those to be considered in the risk analysis. Assets are not usually locations, although every asset is found at some location. The DFAC is not the asset; the asset is the personnel in it. However, locations are usually used to identify assets. It is generally the location of the asset and its characteristics that can affect the likelihood of and vulnerability to attack.

> *For example, the location of billeting near the base perimeter and in easy view from off base may make personnel located there more likely to be attacked with a VBIED; the closer billeting is to the perimeter, the higher the vulnerability of the personnel to the blast and fragments.*

At a minimum, a key asset list will probably include:

- Mission essential personnel, equipment, material, and infrastructure.
- Large concentrations of personnel.

The following non-prioritized checklist should be considered in developing the JFOB key asset list. The objective is to shorten the list of all assets to those worth considering in a risk analysis.

Checklist for Key Assets

□ DFAC
□ Postal exchange/base exchange (PX/BX)
□ Operations Center
□ Housing, Latrine and Shower
□ Office
□ Education Center
□ Post Office
□ Laundry
□ Morale, welfare and recreation (MWR) (Fitness and Sport, Community Center, Theater)
□ Chapel
□ Fixed and Rotary Wing Aircraft (parking areas and maintenance)
□ Vehicles (hard stands, maintenance, etc.)
□ Water and Sewage
□ Power
□ Fuel, Storage and Distribution Points
□ Main Support Area (MSA)

- ☐ Guard Force
- ☐ Quick Reaction Force (QRF)
- ☐ Medical Facilities and Equipment
- ☐ Fire Facilities and Equipment
- ☐ Engineer Facilities and Equipment
- ☐ Explosive Ordnance Disposal (EOD) Capabilities

After listing JFOB key assets, review the list and ensure there is a reason why each entry is on the key asset list; otherwise, filter the list. The following is a quick checklist; if the answer is not "yes" to at least one of the following questions, the asset should be a candidate for filtering.

- ○ Is it a mission essential vulnerable area (MEVA)?
- ○ Is it high risk personnel (HRP)?
- ○ Is it a high risk target (HRT)?
- ○ Is it an asset that should receive special consideration due to higher Headquarters (HQ) guidance or interest?
- ○ Is it required for IR or consequence management operations?
- ○ Is it critical infrastructure needed to maintain mission?
- ○ Is there some other reason for including it on the list?

Rank the remaining key assets in the list.

- ○ Expedient solution. Examine the list and sort the assets from extreme-to-negligible value.
- ○ Formal solution. Use the computer Asset Value Rating Tool in the JAT Guide to determine an asset value rating from 1.0 (extreme) to 0.0 (negligible) value rating.

At this point, the list may still contain more assets than can be worked in a risk analysis in the available time. If so, select a shorter final list. One strategy is to start with the assets on the top of the list and select any assets that receive protection by regulation.

During or at the conclusion of the risk analysis work, additional assets can be added to and worked through the risk analysis process if there is sufficient time. Note that working a restricted list through the process and then mitigating the risks often will impact assets that did not make the final cut for the risk analysis. For example, improving the JFOB ECP against VBIEDs will reduce risk for such an attack for all assets inside the perimeter regardless of whether they made the final list.

DETERMINE THREAT LIKELIHOOD FOR THREAT-ASSET PAIRS

Chapter 3 provides information for developing a JFOB threat assessment.

While this handbook is scoped to rockets, artillery, mortars (RAMs), and improvised explosive devices (IEDs), the risk analysis process provided in this handbook can be used for a wide range of threats. The Intelligence Threat Assessment must be interpreted to project likely

- Threats identification.

- Threat types and general and specific threat tactics.
- Threat COAs against assets.

Starting with the list of key assets, develop threat-asset pairs by associating likely threats with each asset. As shown in Figure 4-3, there are four possible threat-asset pair relationships. You can keep records and develop the data by using the Field Risk Analysis Tool or the JAT Database tool in the JAT Guide (see Tools section above).

Figure 4-3. Possible threat-asset pair relationships

Threats Identification. Identifying the threat provides an answer to the question: Whom should I defend against? The following checklist can be used.

☐ International Terrorist (IT)
☐ Domestic Terrorist (DT)
☐ Left-Wing Extremist (LE)
☐ Right-Wing Extremist (RE)
☐ Other (O)

Threat Type and General and Specific Threat Tactics. Identifying the threat type and general and specific tactics answers the question: What type attack should I defend against? Use the following checklist, which contains RAMs and different type IEDs (the default threats for this handbook), and other threats. You can expand the list to include additional threat types and general and specific threat tactics. See Table 4-1.

Threat COA. Describing the likely threat tactics/COA for each threat-asset pair means to describe a reasonable, realistic attack scenario that occurs at a time favorable for the attacker. Up to this point, the information contains generalities such as "VBIED." A projected threat COA provides enough information to plan a defense strategy. As an example, if the tactic is an IED: What is the estimated IED size; how is it delivered; is it a suicide attack or will the attacker attempt to escape; what is the attacker's route; how does the attacker get past defenses to the target; what happens if the attacker is intercepted?

Threat Type	General Threat Tactics	Specific Threat Tactics
Explosive and Incendiary Devices (IED)	Moving or Stationary Vehicle Device	Explosive or Fuel On Ground Surface
		Explosive or Fuel On Water Surface
		Explosive Below Ground Surface
		Explosive Below Water Surface
	Hand Delivered Device	Mail Explosive
		Backpack/Suitcase Explosive
		Supplies Explosive
		Body Explosive
		Blunt Force Projectile
		Grenade
		Improvised Incendiary
		Improvised Explosive
Standoff Weapons	Indirect Fire	Mortar Rocket Artillery
	Direct Fire	Antitank
		Shotgun or Low Power Rifle
		High Power Rifle
		Pistol
	MANPADS	MANPADS
Contamination	Airborne Contamination	Chemical
		Biological
		Radiological
	Waterborne Contamination	Chemical
		Biological
		Radiological
Nuclear (WMD)	On/Proximity of Installation	On/Proximity of Installation
	Vicinity of Installation	Vicinity of Installation

Table 4-1. Threat Types and General and Specific Tactics

Threat Likelihood Rating. Skip this section if the expedient solution is used.

Each threat-asset pair can be assigned a threat-likelihood rating, a number in the range 0.0 to 1.0, where the low end means negligible likelihood and the high end means extreme likelihood The threat likelihood can be different for different threat-asset pairs, and this difference influences the risk analysis results. Enter the results in the JAT Database or in the Field Risk Analysis Tool sheets provided later in this chapter.

- Formal solution. Use the computer Threat Likelihood Rating Tool in the JAT Guide to estimate a threat likelihood rating. Any type of attacks that have occurred at the JFOB or at other JFOBs in the region should be on the high end of the threat likelihood rating scale.

DETERMINE AND ASSESS VULNERABILITIES OF ASSETS

Identifying and understanding the vulnerabilities of an asset are important in determining how it could be protected from loss.

For each threat-asset pair, the vulnerability assessment answers the questions "How susceptible is the asset to this attack and why?" Although terrorist threats cannot be controlled by defensive actions, they can be assessed, and the vulnerability of assets to those threats can be mitigated.

Vulnerabilities are the component of overall risk over which the commander has the most control and greatest influence. Teducing vulnerabilities normally results in reduced risk. The overriding concept of antiterrorism vulnerability reduction is the focus in two broad areas: (1) preventing a terrorist incident from occurring (i.e., prevent the VBIED from reaching the asset), and failing that, (2) substantially mitigating the effects of a terrorist act (i.e., provide standoff so the attack effectiveness is greatly reduced, and have IR and consequence management capabilities needed to save lives and recover rapidly).

Determine Vulnerabilities. The JFOB vulnerabilities can be determined by working the two following tasks. These tasks can be worked simultaneously.

Review available sources. If there are available information sources containing previously recognized vulnerabilities, review the sources to become informed. This task may apply more or less to the situation, depending on availability, quality, and timeliness of sources. Deployment may be into a bare base with no prior history beyond knowledge of attacks occurring in the region. Reviewing sources assists in recovering previously developed information, adding insights for new personnel, and providing a basis for better vulnerability identification. Some or many of the vulnerabilities identified in available sources may have been mitigated.

- □ Most recent Risk assessment
- □ JFOB FP program review.
- □ Most recent FP plan, with vulnerability contents.
- □ Joint Service Vulnerability Assessment (JSIVA) or higher headquarters (HHQ) FP Program reviews.
- □ Self-assessments.

- ☐ Counter intelligence (INTEL), law enforcement (LE) liaison, INTEL support capabilities.
- ☐ Physical security plan deficiencies and other FP vulnerability observations.
- ☐ IR Capabilities.
- ☐ Consequence management plan capabilities.
- ☐ FP exercise results, lessons learned.
- ☐ JSIVA checklist.
- ☐ Installation vulnerabilities reported to HQ.
- ☐ Joint and Service lessons learned databases.
- ☐ HQ FP plans.
- ☐ Logistics and medical support.
- ☐ Memorandum of Agreement/Memorandum of Understanding (MOAs/MOUs) with host nation (HN).

Conduct a vulnerability assessment. This task is conducted for each threat-asset pair, and the task can start before the list of threat-asset pairs is finalized. The task involves determining the vulnerabilities for each threat-asset pair. Vulnerabilities normally have a major impact on the risk analysis assessment results. "Fixing the vulnerabilities" is the approach to mitigating risk, so it is important to collect this information in preparation for later developing defensive COAs.

There are DoD-provided tools to assist in assessing asset vulnerability to include the JAT Guide and Core Vulnerability Assessment Management Program (CVAMP). Some JFOBs also use one or both of the following tools that combine threat, asset value, and vulnerability. These are MSHARP, which combines mission, symbolism, history, accessibility, recognizability, population, and proximity, and CARVER, which combines criticality, accessibility, recoverability, vulnerability, effect, and recognizability. MSHARP and CARVER are discussed in detail in DoD 2000.12H.

Only the JAT Guide vulnerability assessment process is presented in this JFOB handbook. For each threat-asset pair, consider the threat COA from start-to-finish, considering the threat tactics and the vulnerabilities that would enable the attackers' success. Consider an outside-in approach from outside the perimeter, through the JFOB Perimeter, to the asset location perimeter (if there is a separate asset perimeter, such as an enclave or second-layer fence), and for cases where the asset is located inside a structure, consider the asset location exterior and asset location interior. Some attacks involve direct and indirect fire from outside the perimeter, and part of the threat COA involves avoiding detection prior to attack and rapid escape without having to penetrate any of the defensive layers. Other attacks employ COAs that include penetrating the perimeter and getting as close as possible to the asset planned for attack. Yet others depend on penetrating all defensive layers to bring a man-packed IED into a populated area within a structure.

> *For example, vulnerabilities for a "mortar attack-DFAC" could include: lack of any or lack of full height sidewall protection; lack*

of DFAC compartmentalization to limit casualties; lack of ability to keep potential mortar launch areas under inspection.

Vulnerability Rating. If the formal solution is used, the task also involves determining the vulnerability rating for each threat-asset pair using a tool in the JAT Guide. Each threat-asset pair can be assigned a vulnerability rating, a number in the range 0.0 to 1.0, where the low end means negligible vulnerability and the high end means extreme vulnerability.

- Expedient solution. NA
- Formal solution. Use the Vulnerability Assessment Tool in the JAT Guide.

ASSESS INCIDENT RESPONSE CAPABILITIES

FP incident response is a short-lived, often confused, creative, fast-paced flow of events after an attack or other life-threatening or damage-causing event. The response is immediate action taken to save lives or prevent suffering or protect against further harm to forces, facilities, equipment, or supplies. Incident response is covered in Chapter 9.

If a capability is not available, consider placing the deficiency on the vulnerability list as contributing to the risks. If the JFOB IR capability stops the attack or some part of it, the capability can affect the risk. The capability still saves lives, mission capability, and property even if it does not stop the attack. Terrorist IR can be accomplished simultaneously with Terrorist Consequence Management (TCM), but TCM normally starts after assessment of the incident.

Conduct an Incident Response Assessment. Concentrate on the threat-asset pair mass-casualty situations (Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE)) since these situations are the ones in which an IR capability will possibly reduce risk. An IR capability may not provide any risk reduction in a mass-casualty situation in which a single backpack IED detonates in a gathering area, but could reduce risk in an attack involving two backpack bombs with the second timed to explode to catch emergency responders. It is very difficult to achieve an IR capability level that has a major effect on the risk analysis results; most attacks are detected as or after, rather than before, they occur.

When determining an IR capability, consider the following:

□ How would you rate your installation's ability to detect (insert threat-asset pair information here)?

□ How would you rate your installation's ability to assess (insert threat-asset pair information here) this situation?

□ How would you rate your installation's ability to respond (insert threat-asset pair information here)?

□ How would you rate your installation's ability to provide medical support (insert threat-asset pair information here)?

Incident Response Rating. If the formal solution is used, the task also involves determining the IR rating for each threat-asset pair using a tool available in the JAT Guide. Each threat-asset pair can be assigned an IR rating, a number in the range 0.0 to 1.0, where the low end means negligible vulnerability and the high end means extreme vulnerability."

- Expedient solution. NA
- Formal solution. Use the JAT Guide An IR Tool is embedded within the JAT Database. Consult the instructions for the JAT Database.

DEVELOP EVENT LIKELIHOOD RATING DATA

The event likelihood rating for each threat-asset pair is the product of the threat likelihood, vulnerability, and IR ratings for that threat-asset pair. As shown in the Figure 4-2, Risk Equation.

The event likelihood for each threat-asset pair is the relative likelihood of that event occurrence.

- Expedient solution. Select a number in the range of 1 – 9 (negligible-to-extreme likelihood). Consider the threat likelihood vulnerability and IR capability when making this determination. If similar threat-asset situations have occurred at the JFOB (or even in the region), or a threat assessment indicates that attack tactics are evolving in this direction, the event likelihood should be high to extreme.
- Formal solution. The Database Tool in the JAT Guide is used to record the threat likelihood, vulnerability, and IR ratings, and the event likelihood rating is automatically calculated in the database. Consult the instructions for the JAT Database.

DEVELOP CONSEQUENCES DATA

Each threat-asset pair has projected consequences, and it is essential to estimate those consequences in determining risk. A series of five factors listed below is used in determining attack consequences. Data for the consequences are in different units.

- Fatalities (number of people). Each person is counted as a person regardless of rank, income, importance to the mission, or other characteristics.
- Serious Injuries (number of people). Same as above.
- Property Damage (thousands of $). The replacement dollar value of real property. The value is not a function of property type, use, or importance to the mission.
- Equipment Damage (thousands of $). The replacement dollar value of equipment. The value is not a function of equipment type, use, or importance to the mission.

- Mission Degradation (rating scale value). The effect of the fatalities and serious injuries and property and equipment damage on the installation mission.

The first step in a consequence analysis is to interpret the attack scenario, which includes an attack time line and situation favorable for the attacker (i.e.,, the DFAC has its normal maximum population; it is rush hour at the main gate). Examine the scenario, i.e., the projected threat COA, tactics, and weapon for each threat-asset pair, and develop the projected consequences data. Include collateral effects of an intended target in the vicinity. Collateral effects can be greater than the effects on what you identify as the intended target; *i.e.,, a VBIED at the main gate could also heavily damage nearby structures and cause other vehicle and pedestrian fatalities and serious injuries.*

The consequences data estimate can be based on experience, or you can use some estimator tool or computer-based engineering model. The JAT Guide contains the AT Planner for blast effects (requires a computer; see Tools above). Determining consequences can lead to important additional insights into vulnerability. An example is discovering the minimum standoff from a specific location, like a road, determining the amount and location of hardening required to reduce consequences of a VBIED to a negligible level, or identifying the construction reasons for the fatalities and injuries.

Different consequence estimation procedures vary in the quality of the estimate (error bars for the estimated values) for the same scenario and input data, and there is a tendency to overestimate consequences when the estimate is based on expert opinion rather than a tool. However, expert opinion can be used in either the expedient or formal solution.

Mission degradation consequences refer to the installation's mission degradation and not to the target's mission degradation. The mission degradation consequence of an attack is related to the number and type of fatalities and damage resulting from the terrorist event and the psychological and emotional response to the attack in addition to its physical consequences. Fatalities and damage could be high, yet mission degradation low, and vice-versa. Select a number from Table 4-2 that best describes the mission degradation consequences.

The fatalities, serious injuries, property damage, and equipment damage consequences data must be converted to the same units. Use the rating scale that involves the level of concern for the consequences as shown in Table 4-2.

Rating Scale Value	Description of Level of Concern
1	Negligible
2	Negligible to Low
3	Low
4	Low to Moderate
5	Moderate
6	Moderate to High
7	High
8	High to Extreme
9	Extreme

Table 4-2. Consequence Data Conversion

The mission degradation determination and rating scale conversion for other factors such as projected fatalities is a JFOB-specific decision based on many important considerations, such as the value of human life and health, legal ramifications, political sensitivity, etc., and the commander's guidance must be used. It is helpful to set up conversion rules such as if there are zero fatalities, there is negligible concern and if there are 10 or more fatalities, there is extreme concern. You do not have to convert the mission degradation data with Table 4-2 since this is determined at the outset when you use the rating scale.

Helpful Hints

- When examining any consequence factor, there is some point at which there is negligible concern for the number of fatalities (probably 0 fatalities), serious injuries (probably 0 serious injuries), property damage (can live with it with no-need-to-repair/replace or minimum cost), etc.
- When examining any consequence factor, there is some point at which there is extreme concern for the number of fatalities (x fatalities), serious injuries (x serious injuries), etc. If the consequences rise above those judged of "extreme concern," (50 or 100 or 200 fatalities) the rating for projected fatalities is still 9=extreme.

If you are using the

- Expedient solution, you must manually record the data (i.e.,, projected fatalities) and the rating scale value for each type consequence using the Field Risk Analysis Tool. Consult the instructions for the tool on pp 4 – 20-21.
- Formal solution, use the JAT Database Tool to record the consequences data. You also must provide rules for converting consequences data to a rating scale value; the conversion is then automatically performed as you record the consequences data into the database. Consult the instructions for the JAT Database.

RISK SCORE AND PRIORITY

A risk analysis results in a risk score and risk priority for each threat-asset pair. The following describes these results.

- Risk Score. This is the commander's level of concern for the combination of event likelihood and consequences for the specific risk situation; a value that expresses the relative risk for the situation. A minimum score means there is negligible concern about the situation and/or the threat event likelihood is nil or the projected consequences are nil, and no mitigation is needed. A very high score means there is extreme concern for all risk factors and the threat event likelihood is very high. Situations with high risk scores are more important for mitigation than those with low scores. A comparison of the scores for 2 situations provides a way to determine how different the situations are on the risk scale and provides more information than the risk priorities (see next bullet). Situations with similar scores really have equivalent priorities even though the numbers differ by a small amount.

- Risk Priority. This is the relative ranking of the situation risks for the threat-asset pairs. 1 = highest risk. This is the ordering of the threat-asset pairs from highest-to-lowest risk.
- The same procedures should be used in calculating risk for all threat-asset pairs. Since a number of factors are considered in calculating the risk score, the score value is not sensitive to minor changes in procedures and/or rules for consequences conversion to rating scale or changes in event likelihood values. You can confirm this fact by varying decisions or data values and checking the impact on the threat-asset pairs risk scores and the before- and after-variation risk priority list.

If you are using the

- Expedient solution, after calculating the risk score using the Field Risk Analysis Tool, you can assign a risk priority by arranging the threat-asset pairs (one piece of paper for each threat-asset pair) from highest-to-lowest risk score; Priority 1 = highest risk. Consult the instructions for the tool.
- Formal solution, the JAT Database Tool within the JAT Guide automatically calculates, the risk scores and priorities in the database. Consult the instructions for the JAT Database.

RISK ANALYSIS PRODUCTS

Various data and information developed during the risk analysis have important uses.

- Risk situations recommended to the commander for mitigation with supporting information such as reasons for the risks.
- Input to the FP annex to the OPORD; see Chapter 14.
- Input to the base defense operations center (BDOC) standing operations procedure (SOP) for the JFOB; see Chapter 14.
- Part of the justification for un-resourced requirements.

TWO METHODS FOR CALCULATING RISK

Two methods are suggested for developing the event likelihood data (assets, vulnerability, and IR capability), the consequences data, and determining and prioritizing risk.

- Expedient solution. Pencil-and-paper based method provided in this chapter. A simplification of the computer-based process.
- Formal solution. Computer-based method provided in the JAT Guide. A full-capability process.

Computer-Based Process. The JAT Guide (see description and instructions for access in Chapter 15. Tools/Acronyms) contains a complete description of the procedures as well as tools and templates for performing a risk analysis.

The data such as the list of critical assets, vulnerabilities, and consequences of an attack are classified (see DoDI 2000.16). Performing a risk analysis involves

use of the JAT Database in the JAT Guide. Instructions and self-training for use of the JAT Database are provided within the JAT Guide.

The JAT Guide and/or tools used in the JAT Guide process are contained on a CD or DVD package widely distributed to all Services' FP personnel. If you do not have a copy, someone in your vicinity probably does. Also, you can request a CD or DVD package; see the JAT Guide information in Chapter 15. The latest updates to the JAT Guide can be downloaded using an automatic updater similar to the Microsoft Windows updater when you check for updates through the Secret Internet Protocol Router Network (SIPRNET) or Non-Classified Internet Protocol Router Network (NIPRNET).

Risk Analysis Field Process. The pencil-and-paper-based process is contained in the following three pages; instructions are on the first two pages.

RISK ANALYSIS FIELD PROCESS INSTRUCTIONS

1. **SECURITY CLASSIFICATION.** Blank data collection sheets are FOUO. Completed sheets are CONFIDENTIAL or SECRET.

2. **Purpose.** This tool is used to quickly develop threat-asset pair data (potential specific threat attacks against specific assets), assign risks, and prioritize them based on their risk. The results can be used in a subsequent process to select the risks you want to mitigate, possibly the highest risks, and the actions you take to mitigate the selected risks.

3. **Required Materials.** The following are minimum but adequate materials requirements.
   a. Pencil or pen.
   b. A copy of the INSTRUCTIONS sheets (this and the next page) so you can refer to them while filling out the worksheets.
   c. Multiple copies of the RISK ANALYSIS worksheet. Each worksheet contains the information for one threat-asset pair.
   d. A site map, overhead imagery, and/or sketch of the site are important. If you are not planning on marking-up the map, bring overlay material.
   e. A camera (preferably digital). Ground level pictures can be very useful in reviewing and briefing your risk analysis work and in subsequent risk mitigation work.
   f. Something to measure approximate distances like spacing between tents/buildings/perimeter, or an ability to pace off approximate distances.
   g. Calculator to use in adding and multiplying small numbers.

4. **Process Overview.**
   a. If possible, start collecting information and filling out risk analysis sheets before arriving at the base.
   b. Determine likely threats against your assets.
   c. Build a site map if one is not available. As soon as possible, ensure the map actually displays what is on the ground or what is planned.
   d. Make a list of the threat types like VBIEDs and snipers, being careful to include the most important.
   e. Determine which assets appear to be important (called key assets early in the process, and called critical assets if they are determined to be high risk). Assets include people and property inside and outside the perimeter, and include items under direct control of the commander as well as other items such as critical infrastructure like power and water that are needed to accomplish the mission. Make a list.
   f. Determine threat-asset pairs; these are likely threat events/attacks that impact an asset. Some assets may face multiple types of threats (mortar and rocket and IED) using different threat COAs (VBIED at the entrance or loading dock). Some assets may not have any identified threats.
   g. Determine the vulnerabilities for each likely attack situation (the conditions that will contribute to the success of the terrorist attack) for each threat-asset pair. Vulnerabilities include incident response considerations.
   h. Determine the event likelihood for each threat-asset pair on a scale of 1 (negligible) to 9 (extreme).
   i. Estimate the projected consequences for each threat asset pair and the rating for each of the consequences. Also calculate the total consequences rating by adding the ratings for all risk factors.
   j. Determine risk for each threat-asset pair. (Risk = [event likelihood] X [consequences]).
   k. Sort the worksheets in order of risk score starting with the highest score. Assign the risk priority by numbering them 1, 2, 3, etc starting at the top of the sorted stack of worksheets.
   l. Use the risk analysis results to develop recommendations for the commander and data for the FP Annex to the OPORD.

5. Risk Analysis Worksheet Instructions

a. **SECURITY CLASSIFICATION Block.** Mark the classification and protect the worksheets accordingly.

b. **Sheet Number Block.** Enter a unique sheet number (1,2,3, etc.) at top right for each asset on your key asset list. Each sheet is used to describe a single threat-asset pair (a possible attack against some asset) and provide identification for the sheets. You now have 1 sheet for each asset.

c. **Asset Information Block.** Enter information for the asset of concern (i.e., name, type and number of personnel, equipment, etc in/at location x).

d. **Threat Information Block.** Identify the threats, particularly the threats tactics and weapons. Since each sheet must contain a single threat-asset pair, it may take several sheets to describe various types of threat attack concerns for a single asset. If you insert additional sheets for more threats to asset 1, enter 1a, 1b, etc in the sheet number block so all sheets related to asset 1 start with the number 1. If the asset information is the same as on another sheet, you can enter that other sheet number as a reference instead of duplicating the information. You may now have multiple sheets for some assets. You may have some sheets without a threat if none could be identified; set these aside and save them in case you identify threats later.

e. **Vulnerability Information Block.** For each sheet, list the reasons why the threat tactics with the weapon could be successful in causing loss of or damage to the asset. Visualize the threat movement to the attack location, and the attack operation. What enables the attacker? Ability to penetrate the entry control point? Get inside the facility with the asset? Fire mortars from areas with no patrols? No overhead cover? No sidewall protection? No standoff? High asset density? Also consider your incident response and consequence management capabilities.

f. **Event Likelihood Block.** Select the most appropriate likelihood for the event. This should be based on consideration of the asset, threat, and vulnerability information. If such attacks have occurred at the base or at others in the vicinity, or an interpretation of the intelligence assessment indicates that attacks are evolving in this direction, the threat likelihood should be on the high end of the scale.

g. **Consequences Blocks.** Enter projected consequences of the attack described above. Assume the attack is well-timed (i.e., meal time at the DFAC, or HQ is fully populated and has visitors, etc.). Enter the projected consequences **values** on the first line (number of fatalities and serious injuries, $ value to replace property and equipment, and degradation to the **base** mission [use the 1 - 9 rating scale as used for the event likelihood]). Then enter the level of concern **rating** for each attack consequence on the second line using the 1 - 9 rating scale. Repeat the mission degradation rating from the first to the second line.

h. **Total Consequences Score Block.** Add the 5 numbers on the rating line. Each number should be in the range 1 - 9, so the Total Score should be in the range 5 - 45.

i. **Risk Score Block.** Risk Score = (Event Likelihood Rating) X (Sum of Consequences Ratings). The result should be in the range 5 - 405. The larger the number, the greater the risk.

j. **Risk Priority Block.** When the risk analysis is finished, sort the sheets from highest-to-lowest risk score. The risk priority number (1,2,3, etc) runs from the sheet with highest- to the sheet with lowest-risk score. Enter the number in the risk priority block.

FIELD RISK ANALYSIS TOOL

Sheet No.	

Asset Information: What is the asset name, location, security zone, description?

Threat Information: What is the threat tactic and/or technique?

Vulnerability Information: Why is the asset susceptible to attack? (Include incident response shortfalls.)

Rating Scale – Use this for Event Likelihood and Consequences Ratings								
9 Extreme	8 Extreme -High	7 High	6 High-Medium	5 Medium	4 Medium -Low	3 Low	2 Low-Negligible	1 Negligible

Event Likelihood: What is the likelihood of the event occurring? Consider asset, threat, and vulnerability findings. Enter a rating from Rating Scale above.	**Event Likelihood Rating**	

Projected Consequences (Line 1: Estimate losses; Line 2: Select ratings from Rating Scale above)

	Fatalities	Serious Injuries	Property Damage	Equipment Damage	Mission Degradation		
Losses →							
Ratings →						Sum of Ratings	

Risk Score = (Event Likelihood) X (Sum of Consequences Ratings)	**Risk Score**	
	Risk Priority	

RISK MITIGATION

OVERVIEW

Like Risk Analysis, the COA Development process is best conducted as a team effort. The suggested team is part of the force protection working group (FPWG) and others directed by the JFOB commander. Operations leads the FPWG assisted by the FPO.

The planning process concludes with input to the FP Annex (see Chapter 14), the start or continuation of obtaining resources to implement the plan (see Chapter 12), and the implementation of the action plan. This includes input to the BDOC SOP.

Just as there is not a single design for laying out a JFOB, there is not a unique or single-solution COA for reducing risks. Different working groups taking different approaches can develop COA variants to accomplish the same goal. The reason is that the following tasks involve the imaginative use of engineering, science, and experience:

- Generating possible actions to reduce risk.
- Modifying actions to meet resource and operations constraints.
- Filtering COAs to reject actions that are losers and avoid unnecessary work (COA actions that don't provide sufficient benefits, require excessive resources such as funds or personnel or implementation time, etc.).

The commander has a major influence on COA development. That influence is exercised through guidance on the risks selected for mitigation, the relative importance attached to risk factors like fatalities and mission degradation, and the acceptability of the risk reduction (the benefit) and the projected residual risk that will still be present after a COA is implemented. The commander also approves allocation of resources to FP versus other uses and unfunded requirements. Operations constraints such as those imposed by the State Department, local authorities, HN, or the commander also influence acceptability of mitigation actions.

Some rules to use during the COA development process:

- Examine actions (i.e., improve the ECP) that will reduce many risks (i.e., attackers running the gates with a VBIED).
- Search for actions to resolve the highest priority risks.
- It is often necessary to crawl-walk-run your way to the objective risk reduction level since most actions (i.e., build the perimeter or emplace overhead cover on high occupancy areas) cannot be accomplished overnight.
- Some procedural actions (i.e., ensure the guards at the main gate have well defined and trained rules of engagement (ROEs) for potential attacker engagement) can be very effective and inexpensive.

- Benefit and cost data estimations are probably best made by engineer personnel, who have most experience in these specifics. This will help avoid excessive work on ideas that finally get rejected.
- Avoid unnecessary work as you go through the COA development process. Using the process, first make rough estimates (funds required, ability to support, projected benefit in reducing casualties, effect on mission degradation, etc). You might discover some risk mitigation ideas are losers, and any further effort to make the estimates more accurate or polish the actions into an acceptable form will not make them any more acceptable.
- Don't get distracted by easy-action solutions that don't provide much benefit.
- Don't over-design unless doing so involves little or no increase in resource requirements. Greater benefits can be gained using the resources elsewhere.
- Be innovative in making the cost of an action bearable (i.e., compare costs of relocate vs. renovate vs. new construction as different strategies for achieving the same result).
- Consider the risk mitigation procedures provided in successive chapters of this handbook. Some procedures such as good perimeter and entry control reduce the likelihood of attacks. Other procedures such as full-height sidewall protection, overhead cover, compartmentalization, and dispersion reduce the consequences when attacks occur.

The following are hypothetical examples of scenarios, vulnerabilities, and actions that could possibly mitigate the risks for the purpose of explaining the concepts. Note that it may not be possible to remove or reduce all vulnerabilities; many vulnerabilities are too difficult to fully cure for any of several reasons including cost, time, mission impact, and HN objection.

- Scenario 1.

  Attack. A 2-phase VBIED attack on main gate; first VBIED to kill, cause confusion, and distract at the gate; second VBIED to run the gate and attack the DFAC.

  Vulnerabilities. Confusion regarding ROE for such an event. Proximity of/lack of protection for pedestrian entrance, which will cause additional casualties. Lack of a counter surveillance capability (plan is available, but personnel not sufficiently trained). Insufficient DFAC standoff.

  Actions to Mitigate Risk. Develop ROE, and train and exercise them. Relocate the pedestrian entrance and shield it with a blast wall. Train and exercise the Counter Surveillance Plan and check that it is synchronized with the intelligence collection plan. Construct standoff for the DFAC.

- Scenario 2.

  Attack. A Katyusha is launched at the lightweight building living area.

Vulnerabilities. No sidewall blast/fragment protection for trailers in some areas. Insufficient sidewall blast/fragment protection height in some areas (insufficient height results in head/upper torso exposure). No counter-Katyushas capability. No overhead cover adequate for Katyushas in most areas.

Actions to Mitigate Risk. Improve estimate of most likely expedient launch areas and increase observation and random patrols. Emplace rocket screens to protect the DFAC, etc. and other high-population areas. Provide additional protection walls to reduce fragment effectiveness in areas selected on basis of risk priorities. Increase sidewall protection height. Construct Katyusha-detonating overhead cover in (at least) highest priority areas.

- Scenario 3.

  Attack. A homicide bomber with a body explosive or package IED detonates the IED in the DFAC. The attacker is disguised in U.S. or coalition force uniform.

  Vulnerabilities. Wide open areas with nothing to reduce blast and shrapnel effects except the bodies of personnel who are casualties. Inadequate access control to the DFAC.

  Actions to Mitigate Risk. Install blast and fragment protection materials in compartmentalization of the DFAC.

Special consideration should be given to not increasing the risk with an action intended to reduce risk. Some examples for purpose of illustration are as follows:

- An incorrectly constructed bunker/observation post/guard tower/etc. can collapse and cause casualties or fail to provide direct fire protection.
- An incorrectly designed standoff wall or blast wall can become fragments that dramatically increase fatalities in an IED attack.
- Window film on windows without a catch device can cause fatalities when fatalities would have been a low probability before the film was applied.

Risks can be reduced, often to the point they are negligible, but there can be situations where risks are not significantly reduced, and the commander must accept the risk (at least temporarily). Examples are the following:

- The vulnerability is inherently too difficult to solve (i.e.,, target is next to the road and standoff distance is not available, and you cannot evacuate the building; high elevation positions offer enemy mortar spotters a good view inside the JFOB, and there is no way to solve the problem except to move the JFOB).
- The resources are not available (i.e., the solution is tenable, but materials are not available).
- You are not willing to accept the mission degradation caused by the risk reduction measure (e.g., dispersing the targeted assets).

- Operational constraints make the action untenable (e.g., HN will not agree to the action).
- Implementation schedule forces you to adopt temporary, higher risk protection measures (e.g., the time to have a full military working dog (MWD) capability requires significantly less effective human search procedures for months).

Finally, there should be a quick blue/red look at each action.

- Blue look.
  - Is it feasible?
  - Is it supportable?
  - Are there special costs?
  - Are there benefits in addition to terrorist attack risk reduction?
  - Does the action result in substituting one risk for another?
- Red look.
  - What will be the terrorists' reaction when the increased protection measure is revealed, and what will the terrorists do in response?
  - Does the action increase the risk?
  - What reasonable countermeasures could be applied by the attacker?

JFOB HANDBOOK

The following chapters in this JFOB Handbook contain information that can be used as the basis for reducing risk.

This Handbook applies to a wide range of JFOB scenarios so COA development can range from using best practices for defense in a bare-base situation to tuning your protection capabilities when you fall onto a mature JFOB. The following are examples with broad risk reduction approaches for hypothetical scenarios. A real scenario will be some variation on the hypothetical one.

Scenario	Suggested Approach
New JFOB with no opportunity to perform a site survey. The site survey happens when the party/ advance party arrives on site. The JFOB site may be bare or contain facilities or structures you can modify or use as-is.	1. Apply the concepts of Chapter 5 Site Selection and Layout as best you can on-site. Consider site layout templates in Chapter 5 as a default, and modify them as needed. 2. Consider the threat and use concepts and designs from Chapters 6-11 to develop a JFOB with protection features against RAMs and IEDs in addition to the normal physical security and other protection considerations. 3. Modify the BDOC SOP (see Chapter 14) for your use. 4. Return to a risk analysis and COA development process to identify and mitigate risks as soon as the dynamic process of building the JFOB permits. Build the FP Annex (see Chapter 14).
New JFOB with an opportunity to perform a site survey, return to your peacetime location, and plan. The JFOB site may be bare or contain facilities or structures you can modify or use as-is.	1. Apply the concepts of Chapter 5 Site Selection and Layout. Using overhead imagery and a site survey, you have significant information for planning. An approximate site layout could be worked during the on-site survey. 2. Consider site layout templates in Chapter 5 as a default, and modify them as needed. 3. Consider the threat and use concepts and designs from Chapters 6-11 to develop a JFOB with protection features against RAMs and IEDs in addition to the normal physical security and other protection considerations you must consider. 4. Modify the BDOC SOP (see Chapter 14) for your use. 5. Return to a risk analysis and COA development process to identify and mitigate risks as soon as the dynamic process of building the JFOB permits. Build the FP Plan (see Chapter 14).
You are going to occupy an operating JFOB.	1. Apply Chapter 5. Collect all available information from the current JFOB occupants. Determine what the current occupants consider high risk and likely threat-attack situations, and start with this in your risk analysis and COA development. If the current occupants have a risk analysis, COA in-progress, FP Annex, etc., get copies. 2. Consider the threat, and use concepts and designs from Chapters 6-11 to improve the JFOB with protection features against RAMs and IEDs. 3. Modify the current occupant's BDOC SOP or formalize one (see Chapter 14) for your use. 4. Return to a review-and-improve risk analysis and COA development process to further identify and mitigate risks as soon as the dynamic process of moving into the JFOB permits.

Chapter 5

JFOB SITE SELECTION AND LAYOUT

Contents

INTRODUCTION

JFOB 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 (FP) measures should be consciously integrated into the planning, design, and construction of JFOBs. A JFOB 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 JFOB and will increase the JFOB'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 JFOB site location, design and layout.

FORCE PROTECTION PLANNING

Early identification of force protection and security requirements is essential to the JFOB 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 JFOB 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 JFOB 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 the Force Protection Working Group.

PLANNING AND DESIGN STAGES

Planners and designers can integrate force protection measures into three planning and design stages that support JFOB development:

- Site Selection. Site selection planning provides a framework to guide development of the JFOB. Consideration of force protection measures during the site selection stage may preclude the need for applying more stringent force protection measures to the JFOB at a later time. Site selection planning should make use of vegetation, topography, and natural barriers as protective measures.
- JFOB Layout and Design. During the JFOB layout and design stage, methods for integrating perimeter security, standoff, entry control points, vehicle barriers, fences, and security lighting to diminish potential threat to personnel and critical assets are addressed.
- JFOB Construction. The JFOB construction planning stage considers protective design measures for structures, including the structural hardening of walls, roofs, floors, and windows to reduce the vulnerability of these structures, thereby making them less inviting targets.

PLANNING FACTORS

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

- **Deter.** Do the location and layout of the JFOB present a hardened image to an aggressor, one that will discourage an attack?
- **Delay.** Do the location and layout of the JFOB 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 JFOB 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 against vehicle-borne improvised explosive devices (VBIEDs) and rockets,

artillery and mortars (RAMs) by allowing for use of natural barriers, standoff, dispersion, compartmentalization, clear fields of fire, etc.?

USCENTCOM STANDARDS AND REQUIREMENTS

U.S. Central Command (USCENTCOM) standards and requirements for JFOBs can be found in USCENTCOM Regulation 415-1 (dtd 01Dec 04) (Construction and Base Camp Development in the USCENTCOM Area of Responsibility (AOR) – "The Sand Book"). The regulation lays out the responsibilities of the Service component, combined joint task force (CJTF) and unit commanders in base camp development, construction, renovation, planning and design. The regulation requires that planners and designers consider force protection, environmental, safety and fire protection standards. Strict adherence to these requirements and those identified in Multinational Corps-Iraq (MNC-I) FRAGOs will provide the surest success in joint forward operations base (JFOB) site selection and layout.

USCENTCOM force protection construction standards apply to all locations controlled or used by U.S. personnel in the USCENTCOM AOR. These standards can be found in Appendix 2 (Antiterrorism Construction Standards) to Annex V to USCENTCOM OPORD 97-01B (Antiterrorism) (dtd 04 Jan 02). The threat tactic, severity of the attack, and desired level of protection are primary considerations in the selection of force protection and physical security measures. USCENTCOM standards provide stringent design guidance for mitigating the effects of specific aggressor tactics and for achieving defined levels of protection. These construction standards have specific requirements for such measures as standoff distance, perimeter barriers, and building construction. These minimum standards must be incorporated into the construction of all JFOBs, regardless of the identified threat. All Service component, CJTF, and unit commanders will annually conduct a systematic assessment of all their JFOBs and must either comply with standards, submit a plan to bring the facility into compliance, or submit a request for waiver to USCENTCOM, Joint Security Directorate.

SITE SELECTION CONSIDERATIONS

Sites for JFOBs are selected to facilitate the accomplishment of primary missions. Even so, force protection considerations must not be ignored. The location of a JFOB 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 JFOB. This analysis should consider the military aspects of a location from the standpoints of both the defenders and the enemy. Terrain analysis considerations include:

- Observation and fields of fire
- Cover and concealment
- Obstacles
- Key terrain

- Likely avenues of approach

In selecting a site, JFOB planners should do the following:

□ Threat: Identify and characterize threats to the JFOB. 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 JFOB and can assess the ability of the JFOB 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. Chapter 3 discusses threats and outlines a threat assessment process that can be used to determine the threat to JFOBs.

□ Political Considerations. Consider the relationship with the local public, including the following:

- *HN Political Climate.* Consider how the local situation influences JFOB location, design, or land use decisions. Politically unpopular decisions may actually attract acts of aggression.
- *Adjacent Landowners.* 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 JFOB.
- *Appearance.* Consider the local perception of the appearance of a proposed JFOB. For example, public perception of a "fortress" may be either desirable or undesirable.

□ JFOB Mission. Examine the JFOB's mission, planned facilities, tenant units/organizations and the JFOB's master planning requirements to identify requirements related to site selection. Mission requirements for the proposed JFOB 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:

- Existing facilities.
- Types of structures.
- Existing natural or manmade features.
- Types and quantity of indigenous construction materials.
- Available real estate and other infrastructure.

□ Dispersion and Standoff. Consider dispersion and standoff requirements, both for the JFOB and individual structures (see USCENTCOM Operation Order (OPORD) 97-01B (Appendix 2 to Annex V to "Antiterrorism Construction Standards").

□ Defense in Depth. 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.

- ☐ Perimeter Requirements. Assess perimeter security requirements (standoff, barriers, entry control points (ECPs), lighting, etc.), and select a site that will best accommodate these requirements.
- ☐ Parking Lots and Roads. Identify parking lot and road requirements that could impact security; i.e., how close vehicles will be allowed to protected assets.
- ☐ Occupancy Requirements. Determine space requirements and other occupancy related design constraints.
- ☐ Natural or Man-Made Vantage Points. Locate JFOBs away from natural or man-made vantage points Avoid selecting a site that places the JFOB adjacent to either of the following:
  - ○ Higher surrounding terrain or buildings that provide easy viewing of the JFOB.
  - ○ Vegetation, drainage channels, ditches, ridges, or culverts that can provide concealment.
- ☐ Potential Enemy Vantage Points. Situate the JFOB to limit, or preferably block, an attack by direct-line-of-sight weapons from potential vantage points. Options include:
  - ○ Use of natural or manmade obstructions, such as trees, fences, land forms, or buildings that obscure sight paths,
  - ○ Locating the facility at a high point, if possible, to force aggressors to fire up toward the target, and
  - ○ Placement of protective surfaces so they will be struck at an angle, thus reducing the effectiveness of the attack.
- ☐ Natural Terrain. 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.
- ☐ Enemy Hiding Places. Eliminate potential hiding places near a JFOB; select a site that provides an unobstructed view around a JFOB, one that can maintain clear zones.
- ☐ Uncontrolled Vehicle Access. Choose a JFOB site away from main thoroughfares and uncontrolled vehicle access.
- ☐ Access Roads. Minimize the number of access roads and entrances into a JFOB. Design entry roads to JFOBs and to individual buildings so that they do not provide direct or straight-line vehicular access to high-risk resources.
- ☐ Open Space. Maximize the distance between the perimeter fence and surrounding developed areas: provide as much open space (clear zone) as possible to the JFOB perimeter.

- □ Deliveries. Select a site that will accommodate off-site commercial and service delivery.
- □ Topographic Areas. Avoid low-lying topographic areas that can facilitate the effects of the possible use of biological and/or chemical weapons.

JFOB LAYOUT CONSIDERATIONS

Personnel concerned with JFOB layout and design and force protection/security measures must consider a multitude of issues, such as JFOB operational and functional issues, HN requirements, safety, and fire protection. In general, these concerns and constraints will be unique to a specific JFOB. 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 JFOB 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 JFOB. JFOB layout designers should plan for each of the following areas:

GENERAL REQUIREMENTS

- □ JFOB mission requirements (see Chapter 1).
- □ Tenant unit/organization mission and space requirements.
- □ Regulations. Ensure that all pertinent regulations are reviewed and considered. For example, USCENTCOM Regulation 415-1 (dtd 01Dec04) (Construction and Base Camp Development in the USCENTCOM AOR – "The Sand Book") and USCENTCOM OPORD 97-01B (Appendix 2 to Annex V to, "Antiterrorism Construction Standards") (dtd 04Jan02) provides specific guidance on JFOB construction and force protection requirements.
- □ Critical Assets. Identify assets to be protected and determine the level of protection needed against an identified threat.
- □ Procedural or Operational Considerations. Consider JFOB user requirements related to operations in heightened threat conditions. Examples include:
  - ○ *Deliveries.* Requirements related to how and where deliveries or pickups are to be made to the JFOB, i.e., how to monitor mail, supplies, materials, trash, service, and construction vehicles.
  - ○ *Restricted Areas.* Requirements concerning access to restricted areas within the JFOB.
  - ○ *Access Controls.* Requirements related to whom or what is to be controlled the degree of control, and where and when the controls apply, i.e., checks for identification of personnel, weapons, vehicles, and packages.

- *Mission and Functional Procedures.* Requirements related to the way the user will operate the JFOB, manage relationships between/among tenant organizations, develop work schedules, identify types of operations to be performed and tenant needs.

☐ Occupancy Requirements. Identify tenant unit/organization space requirements and other occupancy-related design constraints, taking into account the following factors:

- Available real estate and terrain.
- Existing natural or man-made features.
- Availability of existing facilities and types of structures.

☐ Dispersion and Standoff Requirements. Maximize the distance from occupied structures to the JFOB boundary (see USCENTCOM OPORD 97-01B (Appendix 2 to Annex V to, "Antiterrorism Construction Standards").

☐ HN security requirements, restrictions, sensitivities.

☐ Multinational force protection/security requirements.

☐ Tenant-unit force protection/security requirements and considerations.

☐ Financial Considerations. Consider funding limitations for force protection/security requirements.

☐ Construction Considerations. Assess the types and quantity of indigenous and other available construction materials, equipment, funding, labor, contractor support, and reverse-engineering considerations.

☐ Safety Considerations. Identify egress requirements and protective measures related to fire safety.

☐ Ammunition Storage. 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.

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

PERIMETER SECURITY

☐ 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 6.

☐ JFOB Design. Design the JFOB 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, 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 JFOB and entry roads that provide direct or straight-line vehicular access to the JFOB or to critical assets/high-value targets.

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

☐ Standoff Zone. Restrict parking within the standoff zone.

☐ Routes of Travel. Allow for the regulation and control of the direction of traffic on the JFOB, 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 ASSETS

☐ Asset Location. Locate critical assets in the interior of JFOBs, away from the perimeter.

☐ Visual Surveillance. 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 JFOB boundary.

☐ Defensible Space. 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.)

☐ Use of Available Space. 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.)

☐ Access Routes. Locate an asset so that it is not accessible to direct or straight-line vehicular access/vehicle approach routes.

- □ Vehicle Parking. Locate parking to obtain required standoff distance from critical assets/high value targets to minimize blast effects from potential VBIEDs.
- □ Exterior Signage. Minimize exterior signage or other indications of critical asset locations.
- □ Trash Receptacles. Locate trash receptacles as far from critical assets as possible.
- □ Vegetation. Remove dense vegetation near a critical asset that could screen covert activity.
- □ Separation Distance. Provide adequate standoff and separation distance between assets to minimize collateral damage (see USCENTCOM OPORD 97-01B (Appendix 2 to Annex V to, "Antiterrorism Construction Standards").
- □ Structures. Design structures that conceal assets, restrict access to assets, and eliminate hiding places.

UTILITIES

- □ Utility Access. Provide secure access to power/heat plants, gas mains, water supplies, and electrical service. Where possible, provide underground, concealed, and protected utilities.
- □ Utility Support. Provide redundant utility systems (particularly electrical services) to support site security, personnel safety, and rescue functions.
- □ Multiple Power Sources. 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.)
- □ Public Address System. Install a site-wide public address/mass notification system that extends from the interior to the exterior of structures/facilities.
- □ Perimeter Penetration. Secure all penetrations of the JFOB'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.
- □ Water Treatment and Storage. Protect water treatment plants and storage facilities by securing access points and maintaining routine water testing to help detect waterborne contaminants.
- □ Signage. Minimize signs identifying critical utility complexes, i.e., power plants and water treatment plants.
- □ Storage Tanks and Operational Facilities. 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.

- ☐ Communication Networks. Decentralize the JFOB's communications resources and conceal key network resources, such as network control centers, to withstand the effects of an attack.

OCCUPIED STRUCTURES

- ☐ Site. Locate high occupancy structures in the interior of the JFOB, away from the perimeter.
- ☐ Personnel. Avoid placing large numbers of personnel in one structure.
- ☐ Open Space. Maximize the distance between the perimeter fence and occupied structures, providing as much open space as possible inside the fence along the JFOB perimeter.
- ☐ Structural Hardening. Incorporate structural hardening techniques (tentage, temporary and permanent buildings, living areas, primary gathering facilities) in design and construction.
- ☐ Retrofit/Hardening Techniques. Consider the use of retrofit/hardening techniques (windows, walls, roofs, dispersion, compartmentalization) on existing facilities.
- ☐ Standoff Distance. Provide adequate standoff and separation distance between structures to minimize collateral damage (see USCENTCOM OPORD 97-01B (Appendix 2 to Annex V to, "Antiterrorism Construction Standards").
- ☐ Windows. Minimize window area in structures to reduce the risk of casualties from glass fragmentation and to restrict observation from outside.
- ☐ Safety Window Frames. Securely anchor window frames and exterior doors to prevent separation as a result of blast overpressure.
- ☐ Doors. Construct doors that open outward.
- ☐ Asset Concealment. Lay out structures to conceal assets, restrict access to assets, and eliminate hiding places.
- ☐ Pedestrian Traffic. Design pedestrian traffic flow within structures to provide unobstructed observation of people approaching controlled areas and occupied spaces.
- ☐ Trash Receptacles. Locate trash receptacles as far from occupied structures as possible.

COMMERCIAL AND SERVICE ACCESS

- ☐ Vehicle Delivery. Locate commercial and service vehicle delivery loading/off-load areas off-site, or designate an entry to the JFOB and offload/loading area that is distant from critical assets/high-risk resources and high-occupancy structures.

- □ Signage. Provide signage that clearly marks separate entrances for deliveries, visitors and employees.
- □ Driveways. Avoid having driveways within or under facilities.

REFERENCES

DoD O-2000.12-H. *DoD Antiterrorism Handbook*, February 2004.

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

MIL-HDBK-1013/14. Selection and Application of Vehicle Barriers, 1 February 1999.

Marine Corps Order P5530.14. Marine Corps Physical Security Program Manual, 21 December 2000.

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

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003.

UFC 4-012-01 (Draft). *Security Engineering: Entry Control Facilities/ Access Control Points*.

UG-2031-SHR. *User's Guide on Protection Against Terrorist Vehicle Bombs*, May 1998.

U.S. Air Force Entry Control Facilities Design Guide, 18 February 2003.

Chapter 6

PERIMETER SECURITY

Contents

INTRODUCTION

The perimeter security system often forms the first line of defense for the JFOB. The goal of perimeter security is to safeguard the JFOB mission by protecting personnel and property. This goal 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 manner so that JFOB security forces can achieve the following:

- Detect attempts to reconnoiter or attack the JFOB or interfere with the performance of JFOB missions/functions.
- Warn the JFOB that an attack is imminent or under way.
- Assess the size and intention of the enemy threat.
- Deny the enemy access to the JFOB and prevent it from degrading the JFOB's primary mission/function.
- Destroy, if possible, the attacking enemy's capability to threaten the JFOB.
- Delay and disrupt an attack, in the event the JFOB security forces lack the combat power to defeat the attacking enemy, to create conditions for

response or tactical combat forces to react and destroy the enemy force or to remove or deny base resources to the enemy.

The security elements that comprise the perimeter security system include:

- Standoff
- Physical barriers
- Access control
- Entry control points
- Security lighting
- Hardened fighting positions/towers/overwatch
- Intrusion detection and surveillance systems
- Security forces

STANDOFF

The best technique to reduce the risks and effects of an enemy attack, especially one involving explosives (VBIED, RAMs), is to keep the attack as far away from the JFOB and inhabited structures as possible (see Figure 6-1). Ideally, maximum standoff should be a primary consideration when personnel are deciding where to locate a JFOB. If distance is not possible, the next best solution is to maximize standoff for individual, inhabited structures. Regardless, even with adequate space, standoff must be coupled with appropriate operational security procedures 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. Standoff requirements for the central command (CENTCOM) area of responsibility (AOR) are identified in Appendix 2 “Antiterrorism Construction Standards” to Annex V to USCENTCOM OPORD 97-01B (Antiterrorism) (dtd 04Jan02). Additional information on standoff can be found in Chapter 8 (Protective Construction).

PHYSICAL BARRIERS

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

- Define the perimeter of the JFOB.
- Establish a physical and psychological deterrent to attackers and individuals from attempting unlawful or unauthorized entry.
- Optimize use of security forces.
- Enhance detection and apprehension opportunities by security forces.

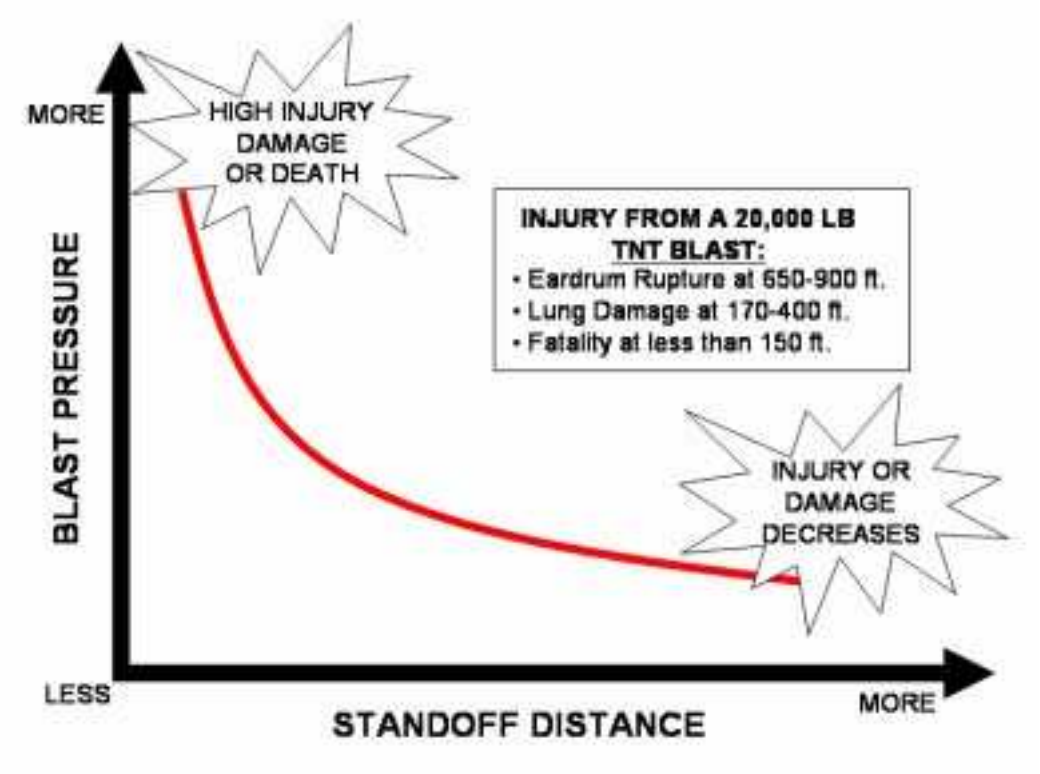


Figure 6-1. Importance of standoff

- 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.

Two major types of physical barriers should be considered:

- Natural (mountains, swamps, thick vegetation, rivers, bays, cliffs, etc.).
- Man-made (fences, walls, gates, vehicle barriers, etc.).

PHYSICAL BARRIERS BEST PRACTICES

☐ Barriers should be emplaced in concert with each other, the natural terrain, and any man-made obstructions.

☐ 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 JFOB.

☐ Combinations or layers of barriers should be separated by a minimum of 30 ft 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. These include concertina wire, multiple-strand razor or barbed wire, or other devices that inhibit enemy 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.
- ☐ Temporary walls or rigid barriers should be considered. They deny access and protect against high-speed vehicle penetrations. Types of materials for consideration include:
  - Concrete barriers (Jersey, Texas, Alaska, Bitberg barriers)
  - Concrete or sand-filled oil drums
  - Concrete bollards or planters
  - Steel or steel-reinforced concrete posts
  - Sand or water-filled plastic vehicle barriers
  - Earth-filled barriers (HESCO bastions, metal revetment)
- ☐ 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.
- ☐ 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 JFOBs or as a temporary serpentine in entry control points.
- ☐ Barriers installed in clear zones must be designed so that they do not provide terrorists with a protective hiding place or shield.
- ☐ Perimeter barriers should be kept under observation and patrolled frequently.
- ☐ 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.

- □ Barriers should be fully integrated to form a continuous obstacle around the JFOB, capable of stopping possible vehicle threats.
- □ 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.
- □ Barriers can be compromised through breaching (i.e., cutting a hole through a fence) or by nature (i.e., berms eroded by the wind and rain); therefore, barriers should be inspected and maintained at least weekly.
- □ Barriers at the perimeter can help conceal and shield JFOB activities from direct observation and surveillance.

Man-made perimeter barriers can assume a wide range of forms, to include fences, walls, ditches, berms, barricades, and vehicle barriers (active and passive). Perimeter barriers are further distinguished as either antipersonnel or antivehicular.

ANTIPERSONNEL BARRIERS

Antipersonnel barriers are designed to deter personnel on foot from entering a JFOB. 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 JFOB. 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 JFOB against infiltration by enemy personnel. 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. Fences offer delays of less than 1 min against low-level threats to as little as 3 to 8 sec against trained and dedicated high-level intruder teams. 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 (see Figure 6-2).

Figure 6-2. Metal mesh fence with razor wire and barbed wire outriggers

Chain Link and Metal Mesh Fence Best Practices

- □ 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 ft.
- □ 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 ft.
- □ 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 JFOB, 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 (MILITARY HANDBOOK DESIGN GUIDELINES FOR SECURITY FENCING, GATES, BARRIERS, AND GUARD FACILITIES).

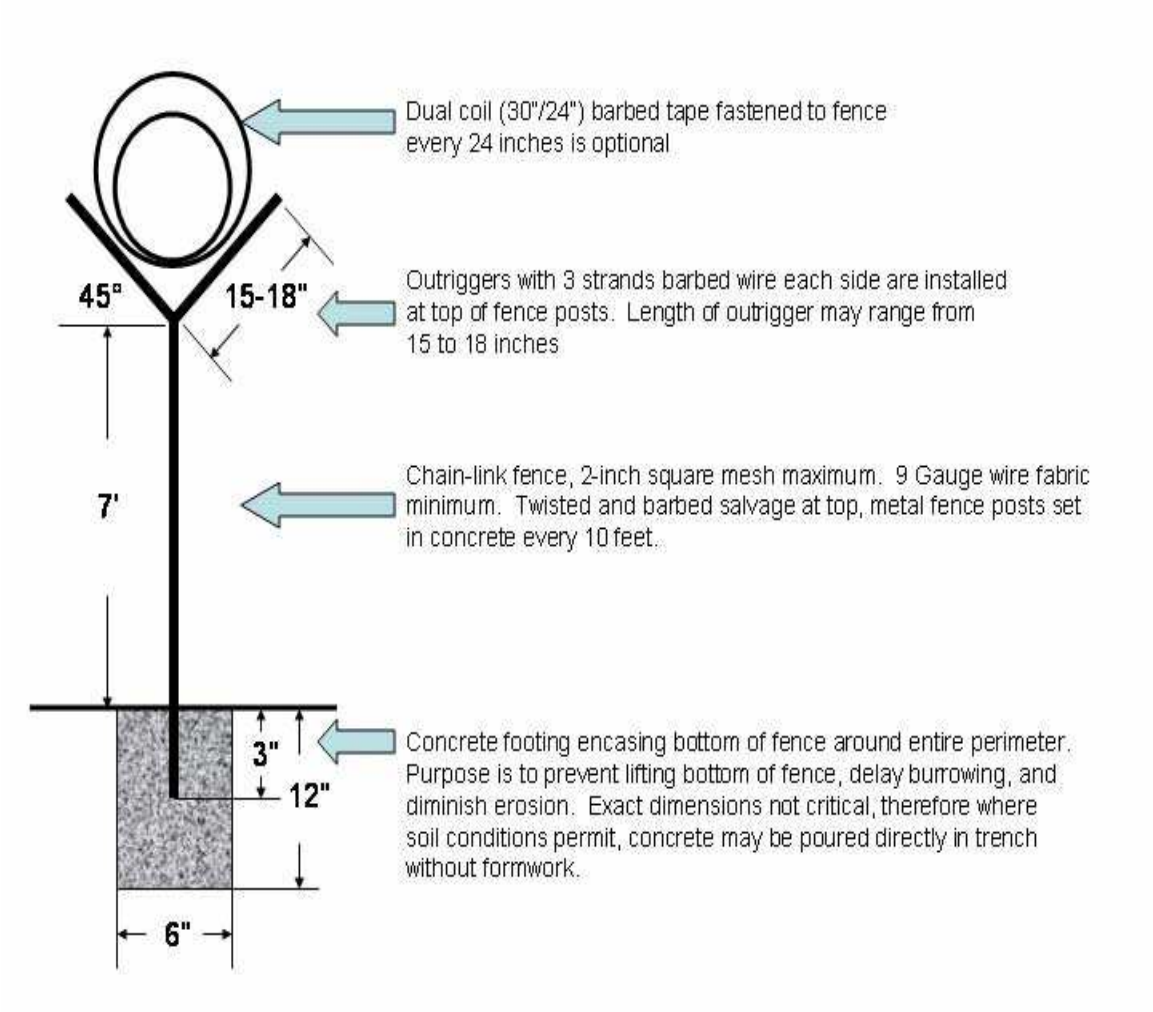


Figure 6-3. Diagram of Chain Link Fence

Triple-strand Concertina Fence. Triple-strand concertina fences are easy to set up and can be rapidly emplaced by unskilled labor. 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 (i.e., 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.

Instructions for Building a Triple-strand Concertina Fence

□ Approximate material and labor for a 300-m fence:

(160) Long pickets	(4) Short pickets	(3) 400-m reels, barbed wire
(59) Rolls of concertina	(317) Staples	(30) Man-hours

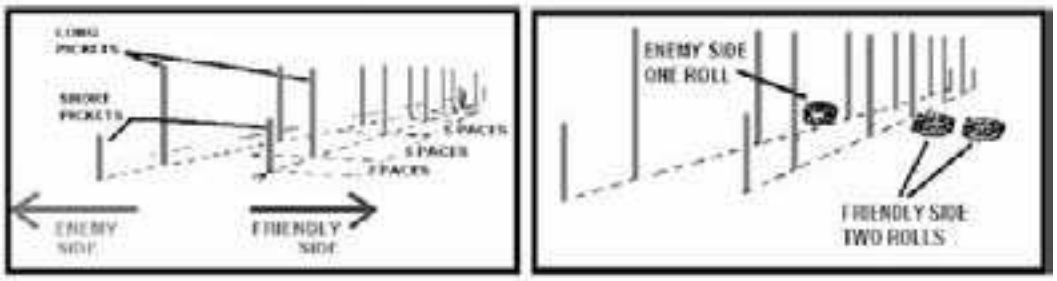
□ First, lay out and install the pickets from left to right, facing the enemy. Place the long pickets five paces apart and the short (anchor) pickets two paces from the end of each row of long pickets. Stagger the enemy side and friendly side picket rows three feet apart (see "Concertina Fence Stakes" below).

□ Second, lay out rolls of concertina. Place a roll in front of the third picket on the enemy side and two rolls to the rear of the third picket on the friendly side. Repeat this step every fourth picket thereafter (see "Concertina Fence Layout" below).

□ Install the front row (nearest the enemy) of concertina and horizontal wire. Place the concertina over the pickets. Install the rear row of concertina and horizontal wire.

□ Install the top row of concertina, and join the rear horizontal wire.

Concertina Fence Stakes



Concertina Fence Layout

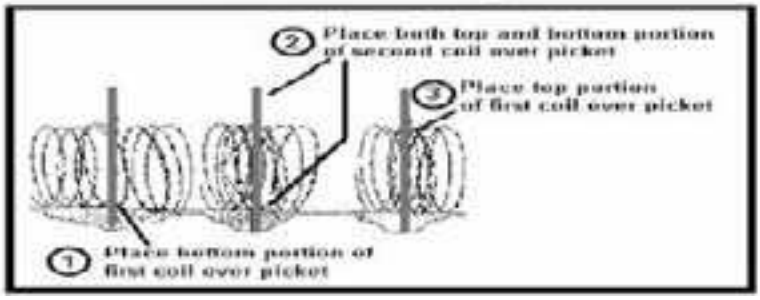


Figure 6-4a. Concertina fence

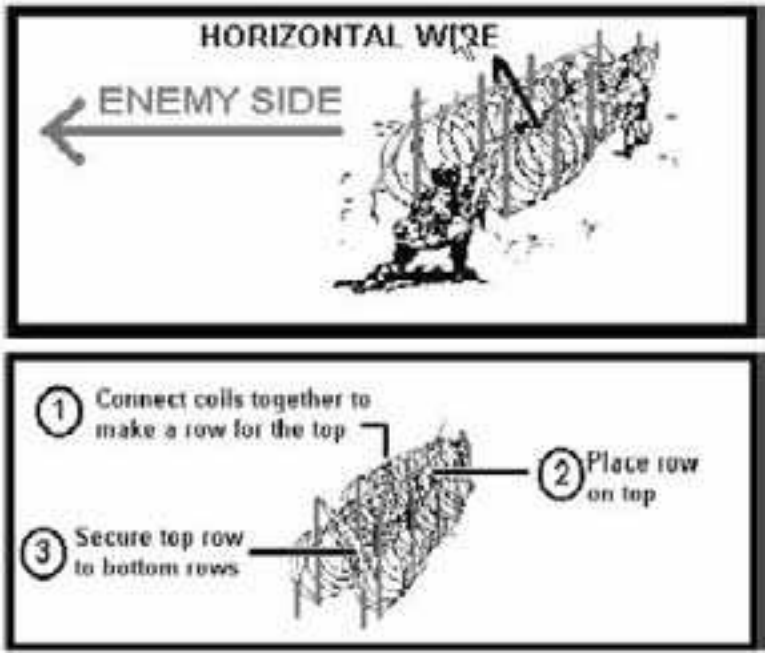


Figure 6-4b. Concertina fence

Concrete Walls. Concrete and concrete masonry unit (CMU) walls can be effective anti-personnel barriers and can also prevent observation of the JFOB, 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 ft 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.

Drainage Culverts and Utility Openings Under Fences. Special antipersonnel, protective measures must be designed for culverts, storm drains, sewers, air intakes, exhaust tunnels and utility openings that pass through cleared areas, traverse under or through security fences, or have a cross-sectional area of 96 in.^{2} (0.06 m^2) or greater with the smallest dimension being more than 6 in. (150 mm). Such openings and barrier penetrations should be protected by securely fastened grills, locked manhole covers, or other equivalent means that provide security penetration resistance of approximately 2 min. MIL-HDBK 1013/10 (DESIGN GUIDELINES FOR SECURITY FENCING, GATES, BARRIERS, AND GUARD FACILITIES) provides detailed design options.

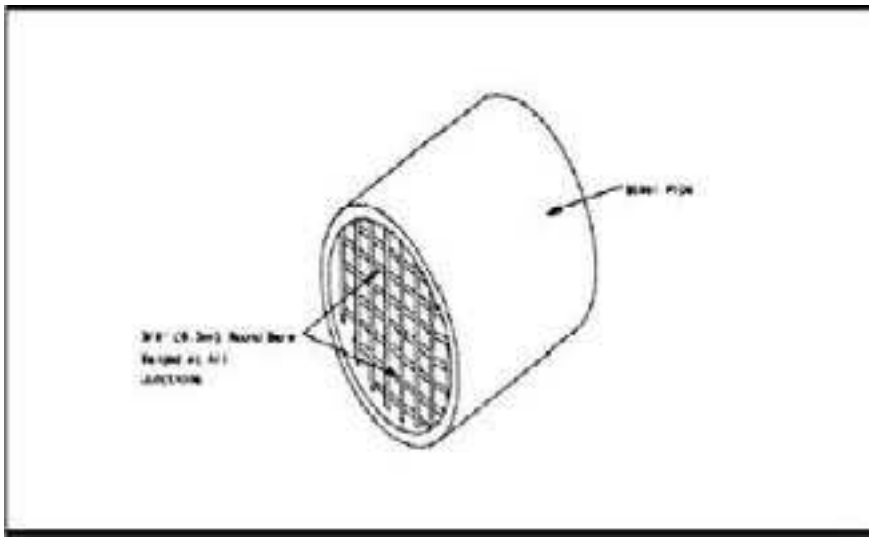


Figure 6-5. Steel culvert grill

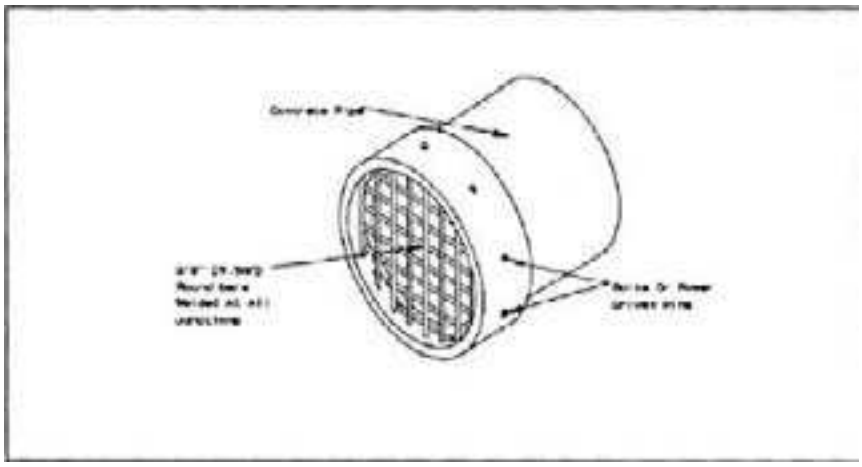


Figure 6-6. Concrete culvert grill

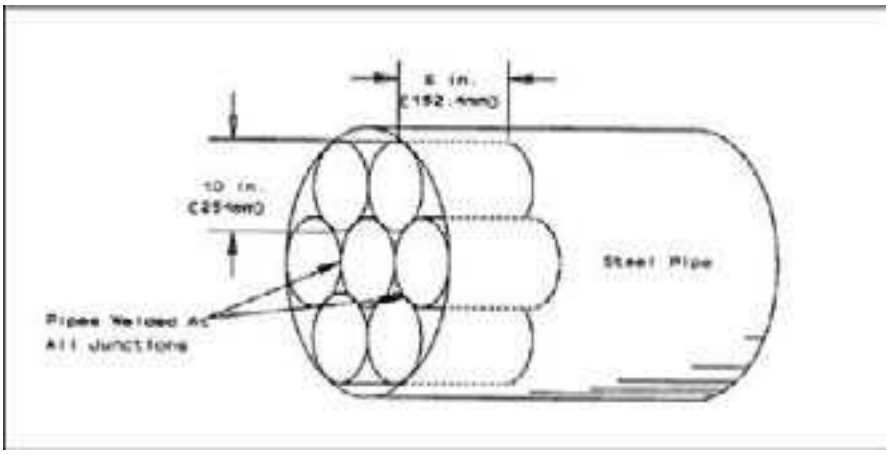


Figure 6-7. Large culvert with short honeycomb pipes

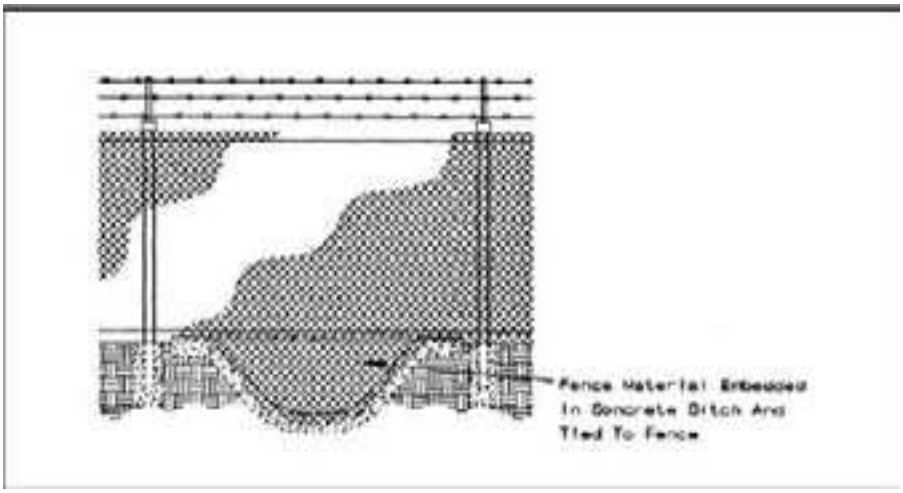


Figure 6-8. Swale crossing with ground stakes

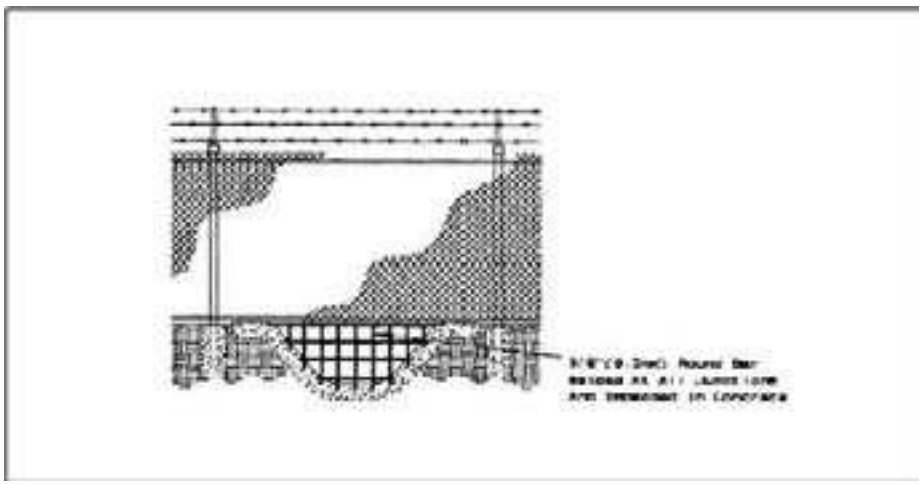


Figure 6-9. Bar grill embedded in concrete

ANTI-VEHICULAR BARRIERS

Anti-vehicular barriers are designed to stop vehicles at the perimeter of a JFOB. They also assist in establishing standoff distance from protected assets. When placing anti-vehicular 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. Typical anti-vehicular barriers for JFOBs include:

- Concrete barriers (Jersey, Texas, Alaska, Bitberg)
- Concrete blocks
- Cabled chain link fences
- Guardrails
- Reinforced concrete walls

- Berms and ditches
- Bollards
- Cabled steel hedgehogs
- Expedient barriers
- Earth-filled barriers (Hesco Bastions, metal revetments)

It is possible to breach anti-vehicular barriers, but breaching methods require considerable time and equipment. Anti-vehicular 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. MIL-HDBK-1013/14 (SELECTION AND APPLICATION OF VEHICLE BARRIERS) and UG-2031-SHR (USER'S GUIDE ON PROTECTION AGAINST TERRORIST VEHICLE BOMBS) provide vehicle barrier selection processes.

ANTI-VEHICULAR BARRIER DESIGN AND SELECTION CHECKLIST

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 JFOB?

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?

Concrete Barriers. Concrete barriers (Jersey, Texas, Alaska, Bitberg) are the most widely used anti-vehicular barriers (see Figure 6-10). 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 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 the USAF Force Protection Battlelab Vehicle Bomb Mitigation Guide). Soil-backed concrete barriers provide better protection against secondary debris hazards (see Figure 6-12). The smaller concrete barriers (Jerseys) are most effective when cabled together. 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 should be cabled together with at least a 3/4-in. aircraft cable. If the potential impact angle from a threat vehicle is expected to exceed 30 deg, then the selected concrete barriers should be anchored to a concrete foundation.

Figure 6-10. Cabled Concrete Barriers

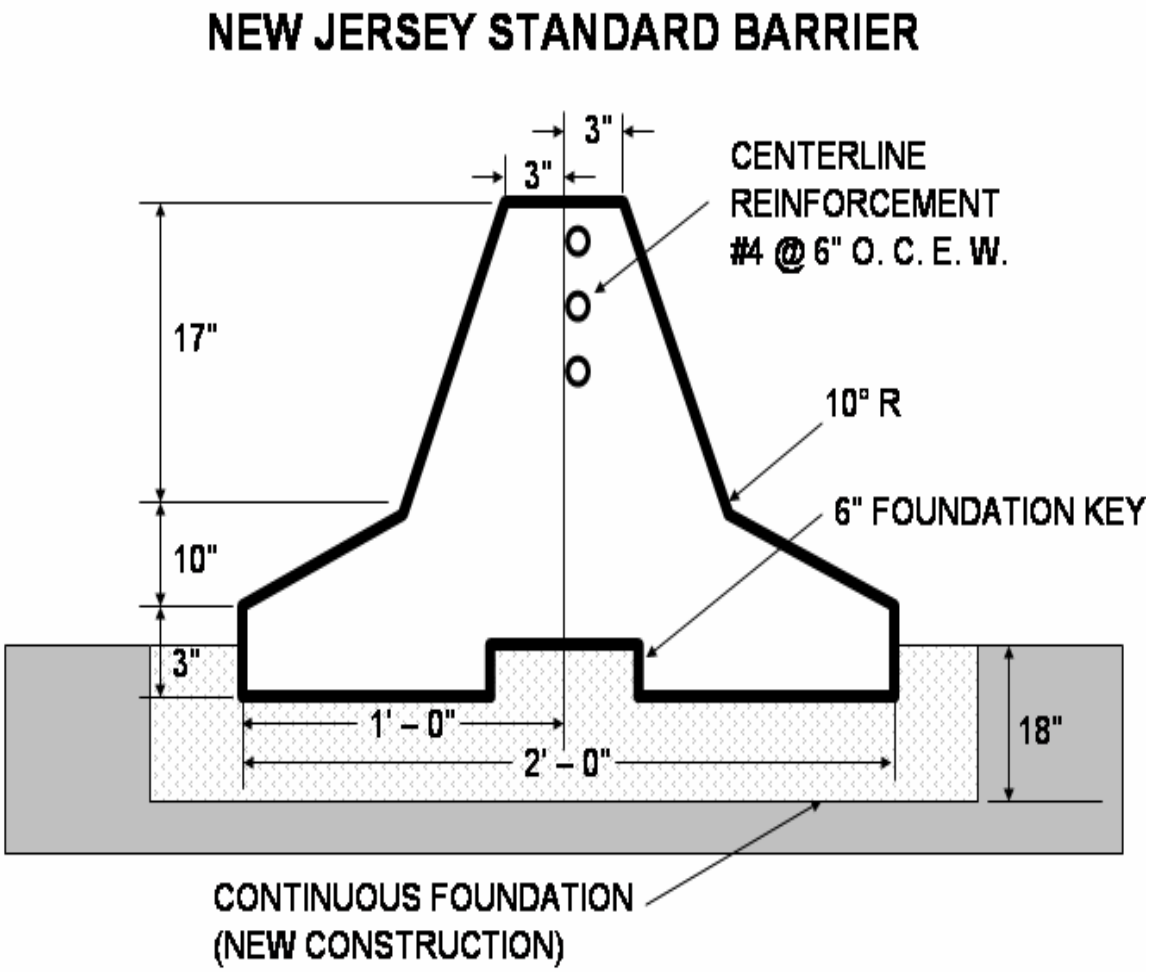


Figure 6-11. Concrete Barriers

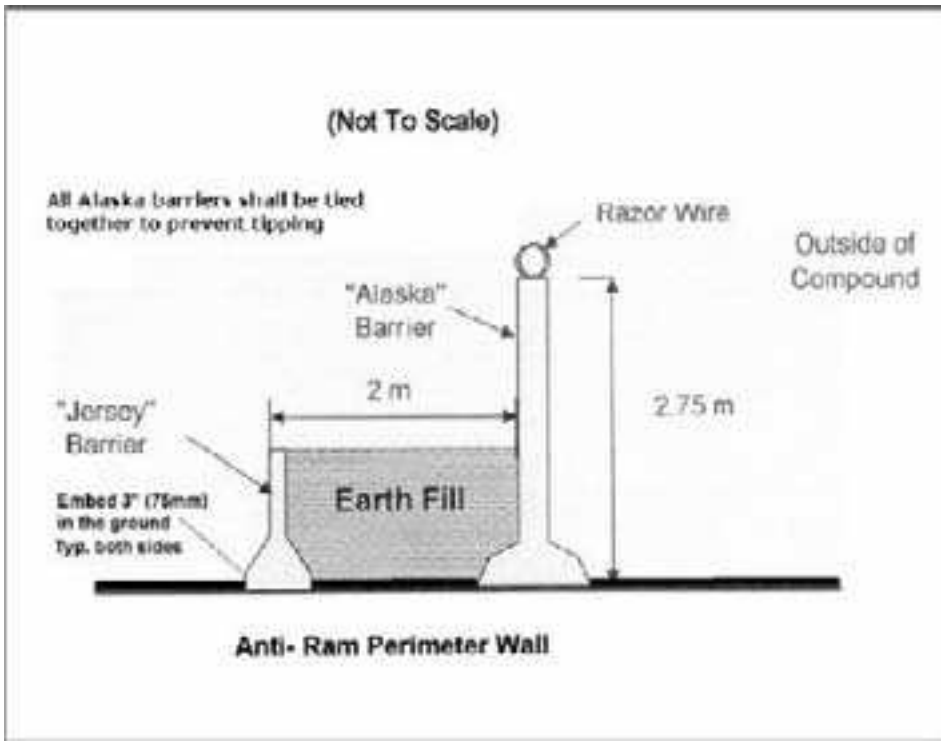


Figure 6-12. Soil-backed Concrete Barriers

Cabled Concrete Blocks. Like concrete barriers, non-reinforced concrete blocks can be used effectively to slow the speed of oncoming vehicles along the perimeter of a JFOB 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 pattern.

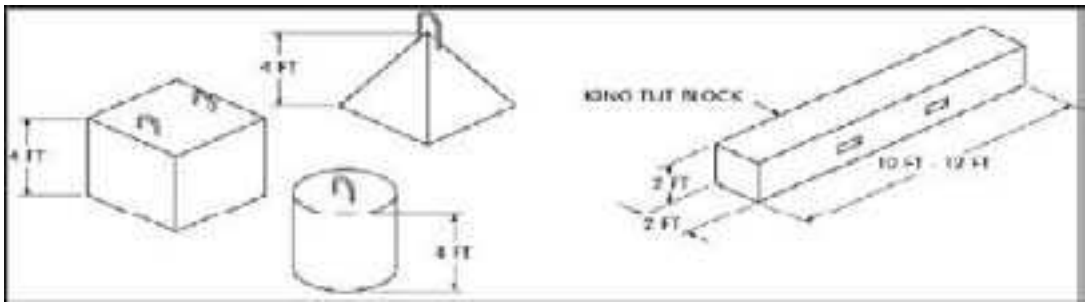
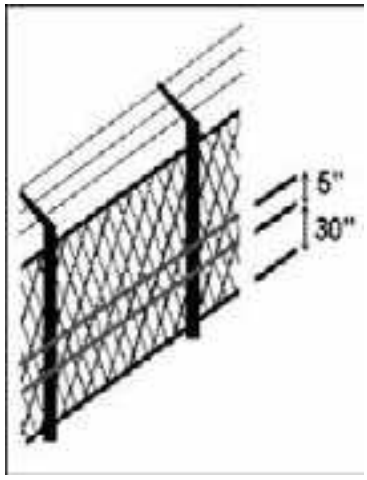


Figure 6-13. Types of Cabled Concrete Blocks

Cabled Reinforced Chain Link Fences. Chain link fences can be transformed into anti-vehicular barriers by reinforcing the existing fence line with steel cable. 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 anchored into a concrete deadman. Posts placed at 4-ft intervals further reinforce fences, making them better able to hinder vehicular 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).



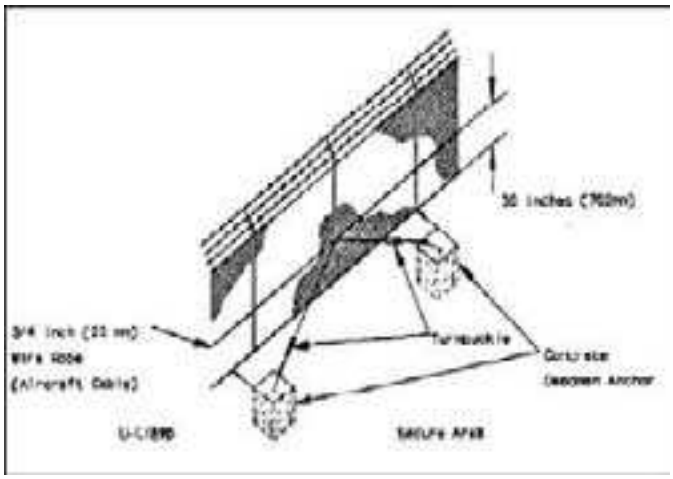


Figure 6-14 (left) and Figure 6-15 (right).

Guardrails. Standard highway guardrails installed on a JFOB perimeter can be effective vehicle barriers. Guardrails are specifically designed with an angled impact of less than 25 deg 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).

Guardrail Types and Dimensions

- Cable guardrail consists of H-beams [2-1/4 in. (5.7-cm) × 4.1 lb/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 anchored to a reinforced concrete deadman at 200-ft (61-m) intervals.
- W-beam guardrail 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).
- Box-beam guardrail 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).

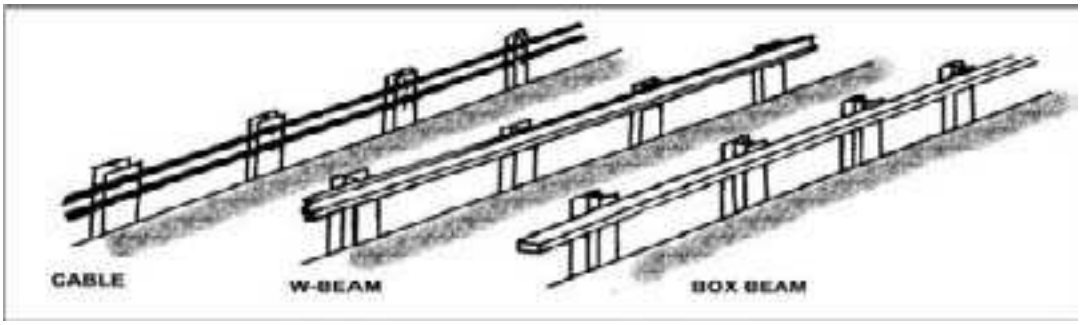


Figure 6-16. Guardrail types

Reinforced Concrete Walls. Concrete walls can be a costly, yet effective, low-profile anti-vehicular 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 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).

Berms and Ditches. Berms and ditches can be used to effectively stop vehicles from penetrating the JFOB 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. 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 JFOB 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 (0.6) to 4 ft (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.

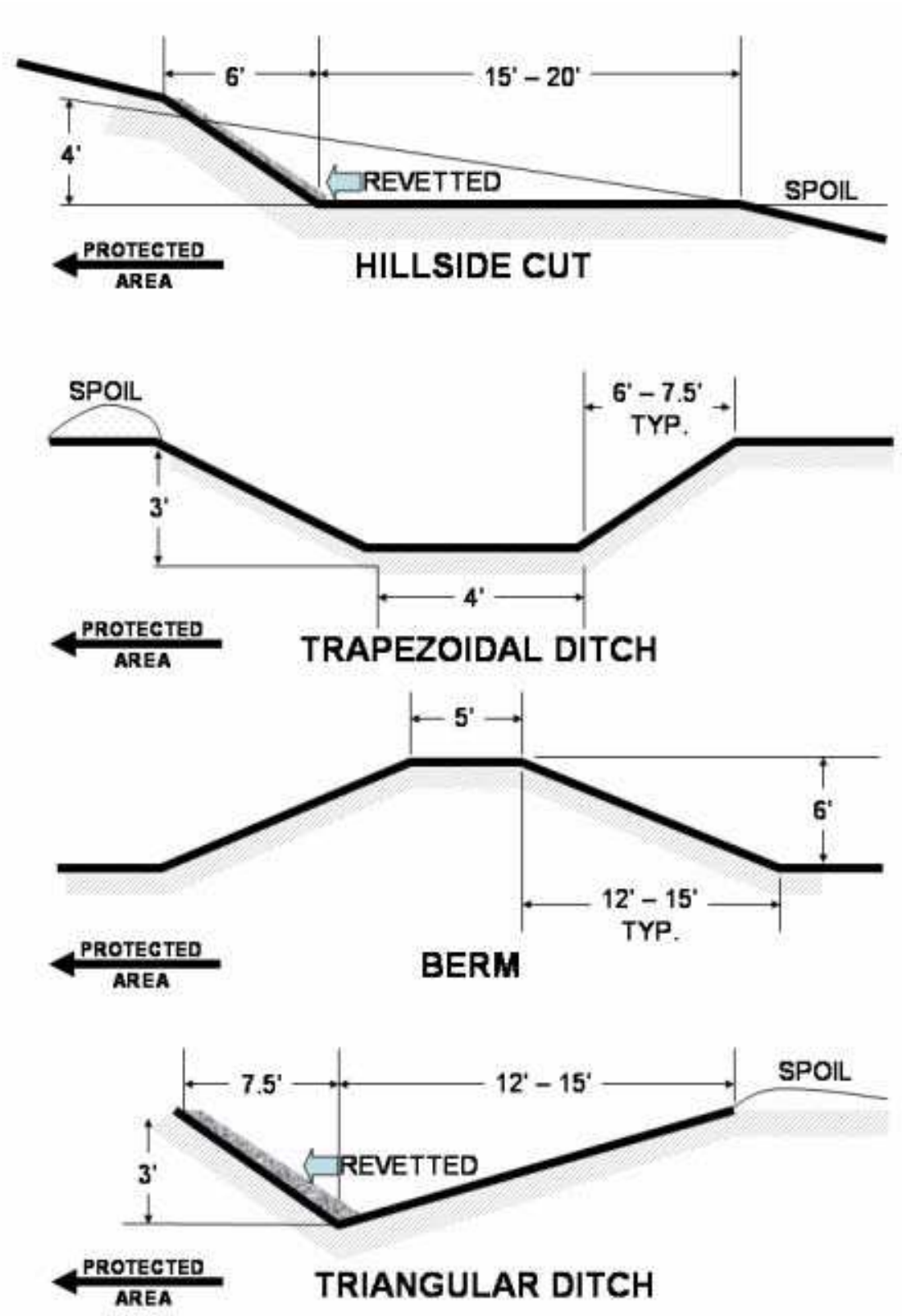
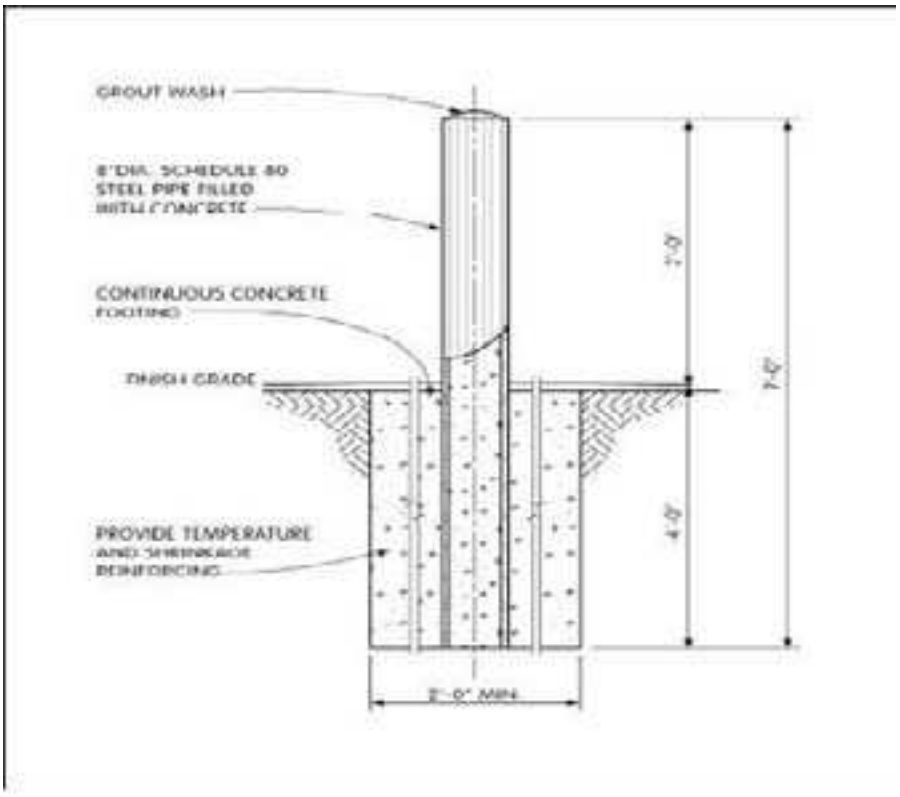


Figure 6-17. Berm and Ditch Designs



Scale: 1 foot = 0.3048 m

Figure 6-18. Bollard system

Cabled Steel Hedgehogs. Also known as star barriers, hedgehogs are designed to roll underneath a ramming vehicle and destroy the driveshaft and undercarriage. When cabled to adjacent jersey barriers, they can help stop a vehicle. To be effective, hedgehogs should be of sturdy construction and used on paved areas.

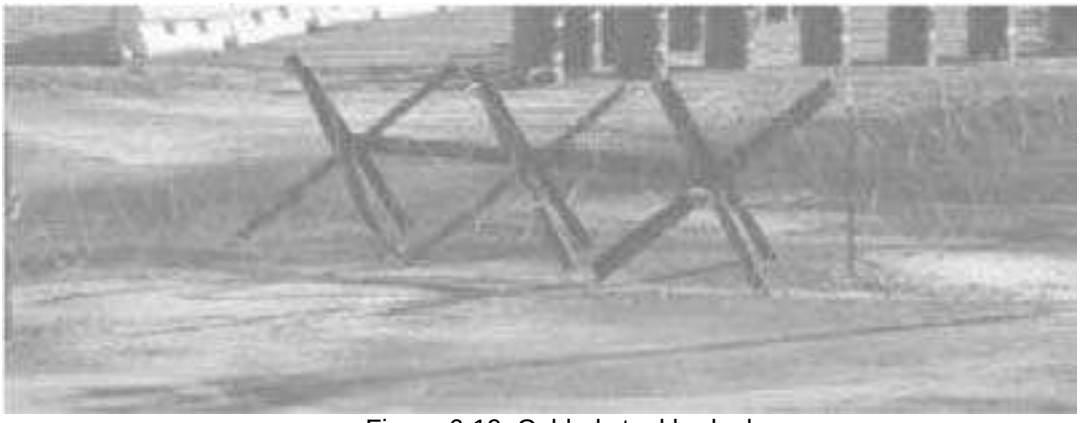


Figure 6-19. Cabled steel hedgehog

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

Examples of Expedient Barriers

- 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-vehicular barriers such as concrete barriers.
- Destroyed or captured enemy vehicles can also be used as expedient anti-vehicular 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. Buried equipment tires were tested 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 (2.4 m). They weighed 2,000 lb (909 kg) each.

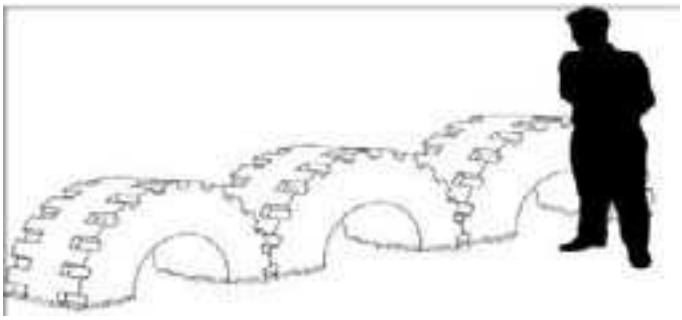


Figure 6-20. Barrier with heavy-equipment tires

Earth-Filled Barriers. Earth-filled barriers are typically employed at a JFOB 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, earth-filled barriers can also be effective as anti-vehicular barriers. Examples of earth-filled barriers include the HESCO bastion concertainers and metal revetments.

HESCO Bastion Concertainer. Concertainer geo-composite materials can be used to construct anti-vehicular barriers and are often favored because of their capability to minimize transportation weight and volume requirements, while optimizing the provided level of threat protection. The geo-composite material is composed of collapsible wire-mesh cells that are lined with a geo-textile fabric. The advantage of using this material is that during transport the geo-composite is collapsed and upon arrival at the final destination is expanded and filled. This quality allows the walls to be transported at only 5 percent of the as-constructed volume.

Figure 6-21. HESCO Bastion Concertainer

The concertainer wall sections consist of a series of large, linked, self-supporting cells constructed from geo-textile-lined wire-mesh panels. The wall cells are connected at the corners with spiral wire hinges that allow the wall sections to be expanded from a compact, folded-storage configuration. For deployment, the wall sections are expanded, positioned, and filled with available soil, sand, gravel, rock, concrete rubble, etc (the use of gravel, rock, or concrete should be minimized due to the fragmentation caused by an explosion). The wall sections can be connected to form longer walls, separated to form shorter sections, or stacked to increase wall height.

When utilized as an anti-vehicular barrier, the concertainer material 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 6-22 below that uses the Mil 1 size). Tests by the U.S. Air Force Battlelab showed that this design effectively stopped a 15,000-lb truck traveling at 30 mph.

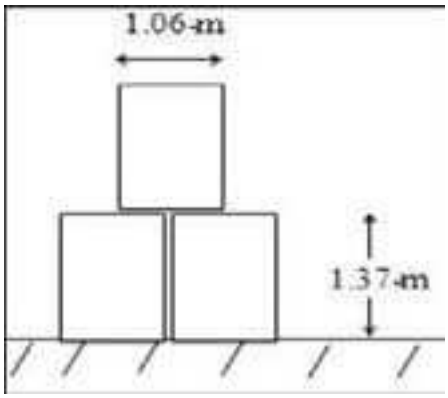


Figure 6-22. Anti-vehicular Barrier

Since the concertainer ranges in sizes, anti-vehicular barriers can be constructed to mitigate larger threats. Large-sized concertainers, such as 7 ft 3 in. high × 7 ft wide, when constructed as indicated above, provide a significant anti-vehicular barrier. More information on HESCO bastion concertainers can be found in Chapter 8 (Protective Construction).

Metal Revetment. Metal revetment materials can also be used to construct anti-vehicular barriers. Like the concertainer, 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 during transport the metal material can be collapsed and stacked and upon arrival at the final destination expanded and filled. More information on metal revetments can be found in Chapter 8 (Protective Construction).

Figure 6-23. Metal revetment walls

ACCESS CONTROL

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

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

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

In order to maintain adequate security throughout the JFOB, or within a facility, activity, critical asset or unit located on the JFOB, without unduly interfering

with day to day operations, it is necessary to permit personnel to move about. On the other hand, access control procedures should ensure that critical assets remain protected. To be effective, access control procedures should be designed to increase the amount of time needed to gain access to the JFOB 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 egress from the JFOB. These procedures aid in containing and resolving the incident as well as in the apprehension of the perpetrators.

PERSONNEL ACCESS CONTROL PROCEDURES

The objective of a personnel access control system is to establish control pertinent to the JFOB or a protected critical asset. Regardless of the type of measures used, a policy that clearly defines authority and identifies the criteria for access should be established. This policy should cover visitors, vendors, contracted workers (maintenance and support personnel), HN, police, and armed forces, etc. The policy must also clearly define the types of identification to be presented by personnel to verify authority and criteria for access. For example, if a badge system is used, the policy should contain a complete description of acceptable badges. Personnel access control procedures must also define personnel search procedures and methods. To maintain positive control over personnel access to the JFOB and associated critical assets, security personnel can implement several access control measures, including:

- Access control lists
- Pass and badge system
- Exchange-pass system
- Escort system

Access control Lists. Admission to a JFOB, as well as to critical assets, should be granted only to persons whose names appear on an access control list. Personnel desiring access should be positively identified prior to granting access. Access control lists are essential to security. They should contain names of only those individuals specifically authorized access to a JFOB 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. Admission of persons other than those on the authorized access list should be approved by the JFOB commander or designated representative.

Pass-and-Badge System. If the number of personnel requiring access to the JFOB exceeds a number that can be recognized personally by security personnel for the JFOB, a pass-and-badge identification system should be considered. 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 the home address, the specific work location address and telephone number, security 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 JFOB. This system involves exchanging one or more identification media (such as badges or passes) for another separate type of identifier (such as badges or passes). This system is particularly useful in controlling visitors. The process of exchanging passes is a personal one, permitting security personnel an opportunity to examine closely all persons before they enter and exit the JFOB.

Escort System. Escorting is an effective method to control visiting personnel or contracted workers within a JFOB. The escort must remain with the visitor at all times while he/she is within the JFOB. If local written policy determines that an individual does not require an escort within the area, the individual must meet all the entry requirements for unescorted access. Escorts should be military personnel assigned or attached to the JFOB. A major objective in escorting visitors around a JFOB is to ensure that all material brought into the JFOB by the visitor is searched for contraband or explosives and that no packages or other materials are left behind when the visitor departs.

CONTRACT WORKER/VENDOR ACCESS CONTROL PROCEDURES

Contract workers/vendors may be used to operate dining facilities, collect trash, perform custodial services, and maintain utility systems on the JFOB. Procedures must be established to screen the background of these personnel and control their access on JFOBs. 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 JFOB. The following are key elements to a contract worker/vendor access control plan:

- Background investigation
- Control
- Contracted worker/vendor uniforms
- Control officer
- Parking
- Packages

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 JFOB. 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 JFOBs 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 JFOB. 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 at the ECP to the JFOB should have a photograph book of authorized contracted workers/vendors.

Sample procedures for controlling contracted workers'/vendors' access onto a JFOB are listed below:

- □ The contracted workers/vendors arrive for work at a designated ECP.
- □ 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.
- □ If the contracted worker/vendor has authorization for unescorted access, he is issued his photographic badge and allowed to proceed to the search area.
- □ 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.
- □ Once the escort arrives the contracted worker/vendor is allowed to proceed to the search area.
- □ If a contracted worker/vendor is not authorized onto the JFOB, the individual is detained and HN security forces are contacted.
- □ All badges are collected as contracted workers/vendors leave the base.

□ All badges are reconciled daily to ensure that all contracted workers/vendors have left the base and returned their badges.

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 movement. 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. JFOBs 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 JFOB and ECP that protective standoff is maintained.

PACKAGES

The type of packages/bags that contracted workers/vendors are allowed to bring onto a JFOB must be restricted. Security personnel must ensure that contracted workers/vendors leave the JFOB 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.

MATERIEL CONTROL PROCEDURES

The first line of defense against aggressors that might use materiel and supply deliveries as a means of attack is to implement off-site delivery and transfer points. In determining the location of these points, security personnel must consider protective standoff distance. If off-site delivery/transfer points are

impossible, procedures must be established that ensure the maximum level of protection for JFOB inhabitants. Best practices for material-access control include the following:

- □ Specific procedures that describe how to control incoming deliveries should be established. These procedures should explain access requirements, search procedures and any special control measures.
- □ If possible, commercial, service and delivery vehicles should have a designated ECP into the JFOB, preferably at a safe standoff distance from critical assets and inhabited structures.
- □ If deliveries must be conducted on the JFOB, then these deliveries should be accomplished away from inhabited areas and at a safe standoff distance.
- □ Delivery routes through the JFOB should located away from inhabited structures and critical assets.
- □ Specific instructions for outgoing commercial vehicles should also be established.
- □ Search procedures for commercial vehicles should follow the vehicle search procedures located in the following section that discusses vehicle control procedures.

Unified Facilities Criteria (UFC) 4-012-01 *Security Engineering: Entry Control Facilities/Access Control Points* discusses different types of equipment, such as the Mobile Search Advanced X-Ray Portable Inspection System and the Mobile Vehicle and Cargo Inspection System (VACIS) – Gamma Ray Imaging System that can be used to search commercial vehicles.

VEHICLE ACCESS CONTROL PROCEDURES

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. The ECP section of this chapter discusses in detail the design concepts and considerations for 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, military working dogs (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.).

VEHICLE SEARCH PROCEDURES

Specific procedures for vehicle searches should be established for each JFOB based on the JFOB 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.

Elements of a Detailed Vehicle Search

- 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 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.

- 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 JFOB. 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 JFOB. The following procedures can be used as general guidance when establishing guidelines for conducting detailed vehicle searches:

□ 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 the driver and passenger holding area where they 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 (i.e., gas in washer fluid reservoir), air filter replaced with wires or explosives, new components in engine, and extraneous components (i.e., 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 reenter vehicle and proceed through ECP.

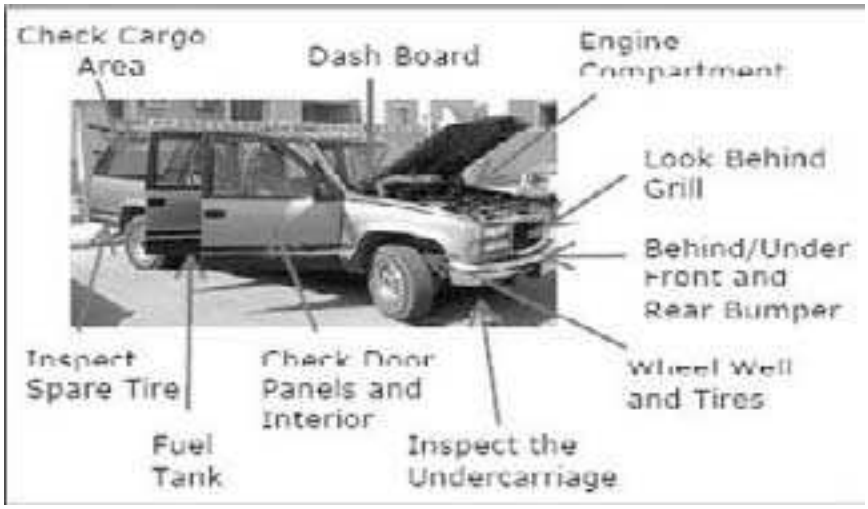


Figure 6-24. General vehicle search areas

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 (e.g., hood, trunk, passenger doors, glove box, or even a package). Searchers should complete one search technique before starting another one.

Explosive Detector Dog (EDD) Searches. The search techniques provided below were derived from the USAF Force Protection Battlelab Vehicle Bomb Mitigation Guide (Sept 2002).

Although specific EDD search procedures will vary according to local JFOB policy, individual MWD handler preference, and the unique abilities of individual canines, the typical approach follows five general steps:

□ 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).

□ The EDD team (the handler and the dog) proceeds directly to the downwind side of the vehicle.

Figure 6-25. EDD searches

□ 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.

□ The dog is directed to search all opened compartments, vehicle seats, and floorboard.

□ The dog is directed to search any on-board packages and parcels.

Search Techniques for the External Portion of a Vehicle

□ 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, the presence of new weld marks or new bolts/screws.
- ☐ Be sure all connections are properly made (e.g., 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.

Search Techniques for the Engine Compartment of a Vehicle

- ☐ 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.
- ☐ Inspect the insulation on the firewall, hood, etc. for rips, tears, bulges, etc. and any subsequent repairs.
- ☐ Look for additional wires running from the hoodlight or the absence of a bulb in the hoodlight socket.

Search Techniques for the Trunk of a Vehicle

- ☐ Take a minute to observe everything within view; then begin at the edge and inspect inward.
- ☐ Pay attention to packages/devices (e.g., alarm clocks, iron or PVC pipe) that look out of place. Inspect items normally found in a trunk (e.g., 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 (e.g., spare tire well, jack/tool storage).

- ☐ 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.

Search Techniques for the Passenger Compartment of a Vehicle

- ☐ Take a minute to observe everything within view; then start at the floor and work up. Pay close attention to packages/devices (e.g., 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 (e.g., extra switches with no label as to their function, 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.

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 EDD and off loaded 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.

Search vehicle from the terrorist's perspective; consider and imagine where the terrorist would hide an explosive device or quantity of explosives?

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 the following:

- ☐ Establishing transfer stations – transferring the cargo from the "dirty" vehicle outside the perimeter to bladders, or "clean" vehicles inside the perimeter, never letting the vehicles get near the assets being protected.
- ☐ Individually searching each vehicle before cargo is loaded at the origin and then escorting the delivery vehicle to the JFOB.

□ Physically inspecting the entire vehicle again at the JFOB with search personnel and MWDs.

ENTRY CONTROL POINTS (ECP)

During Operation Iraqi Freedom, ECPs have been attacked with VBIEDs. VBIED attacks have also been coupled with dedicated assaults in order to gain the assault force access into the JFOB. In the future, attacks may include suicide bombers wearing IED vests. Properly designed ECPs can help defend against these types of attacks. However, ECPs must remain functional and an essential aspect of the JFOB access control system regardless of the level of threat.

Figure 6-26. VBIED attack at ECP

This section provides general design concepts and considerations for ECPs. The guidance provided must be adapted to the specific needs of each JFOB. The information provided is intended to assist in determining JFOB-specific tactics, techniques, and procedures (TTPs) for ECPs. The guidance provided closely models that found in UFC 4-012-01 "Security Engineering: Entry Control Facilities/Access Control Points." Where differences occur the UFC guidance should govern.

As indicated in the UFC, the term ECP is synonymous with the terms entry control facility or access control point (ACP) that often are used in some Service-specific publications. ECPs serve as the entry point for all personnel, visitors, and vehicles to the JFOB. The objective of the ECP is to prevent unauthorized personnel and vehicle access and maximize vehicular traffic flow.

Design Threat. Currently, the recommended minimal design threat for ECPs in Iraq and Afghanistan should be based on the following threat level and specific threat tactics:

- **HIGH Threat Level** – conditions under which Anti-U.S. forces are operationally active and use large casualty producing attacks as their preferred method of operation; there is a substantial DoD presence, and the operating environment favors the attacker.
- **VBIED** – a tactic that allows the enemy to target ECP personnel and/or breach the ECP so that an assault force obtains access through the ECP to attack a target inside the site.

- **Suicide Bomber –** an individual that targets ECP personnel and/or attempts to gain access through the ECP in order to attack a target inside the site.

ECP Functional Zones. ECPs for a JFOB should be subdivided into four functional zones, each encompassing specific functions and operations. These zones are as follows:

- Approach Zone
- Access control Zone
- Response Zone
- Safety Zone

The diagram in Figure 6-27 is an example of the functional zones and design concepts that should be incorporated into an ECP located in an expeditionary HIGH threat environment. The diagram also depicts different types of materials (see Legend) that can be used for construction. For illustration purposes, this example can be considered a multi-purpose ECP since several types of entry control operations are combined in one location.

Approach Zone. The approach zone (see Figure 6-27) is the initial interface between the off-site road network (public highways) and the JFOB. 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 threat personnel/vehicles, including those attempting entry through the outbound lanes of traffic.

Access control Zone. The access control zone (see Figure 6-27) 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 JFOB. This zone defines the end of the ECP. The response zone should be designed so security personnel can carry out the following functions:

- □ Have time to react to a threat, operate the final denial barriers, and close the gate, if necessary.
- □ Monitor overwatch for the entire ECF.
- □ Define the JFOB 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 (i.e., expected weight of the explosive charge) and the JFOB 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.

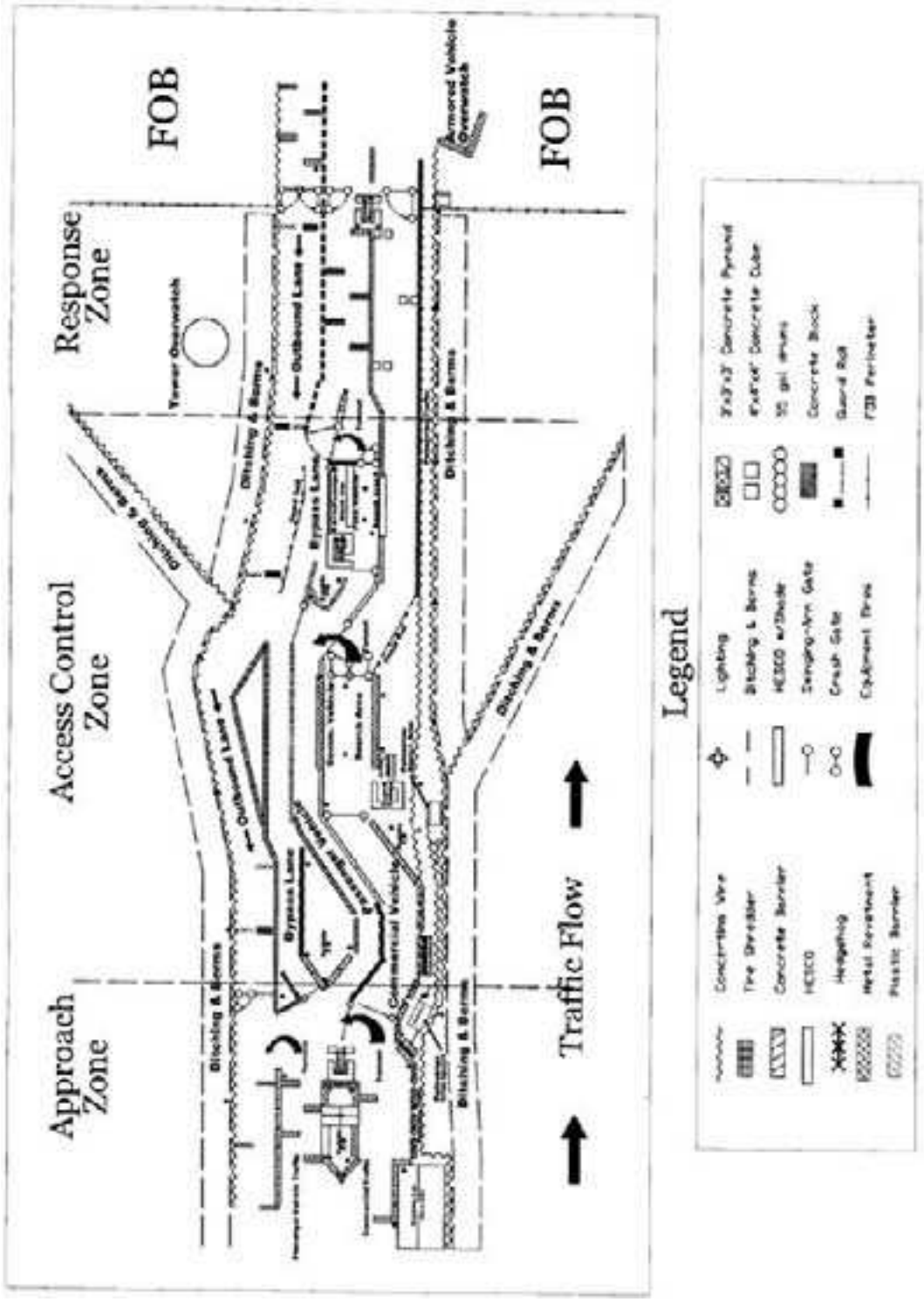


Figure 6-27. Example of functional zones, design concepts, and types of construction materials

ECP Design Concepts and Considerations. The design of the ECP should not detract from the JFOB's mission and operations. The following design concepts should be consistent with all ECPs:

□ Security. The JFOB perimeter is the first line of defense. The ECP, as an integral part of the JFOB perimeter, is essential to a defense in depth strategy

and as a legal line of demarcation. The first priority of an ECP is to maintain perimeter security. The ECP must be designed to 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 JFOB security personnel. Security personnel safety includes provisions for personal protection against attack and errant drivers. Special consideration must be given to climate, location, and orientation.

□ Capacity. The ECP must maximize vehicular traffic flow to eliminate undue delays that would affect JFOB 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 JFOB's commitment to the protection and safety of personnel.

The design guidelines that follow are concepts that should be common to all ECPs:

□ Site selection for a new ECP begins with an extensive evaluation of:

- 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 can have a significant impact on the suitability of a potential ECP site. Flat terrain with a gentle rise in elevation up to the gatehouse is generally preferred. This rise in elevation allows for a clear view of arriving vehicles, which helps entry-control personnel monitor potential threats.

□ ECP spatial requirements vary, depending on the type of ECP, traffic demand, and essential security measures. The design of the ECP should take

into consideration the ECP's intended function, anticipated usage, and type of access. ECP categories include:

- Primary (open continuously 24/7)
- Secondary (regular hours, closed at times (truck – delivery gate)
- Pedestrian access (hours vary)

□ The type of access 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 JFOB, to include:

- Threat
- Mission of the JFOB
- Operations conducted on the JFOB
- Number of security personnel available to enforce access control

□ The preferred type of access for an ECP in a high threat environment is one that limits all pedestrian and vehicle access to mission-essential personnel only. For example: Allow no access to truck/commercial delivery vehicles; instead, establish a centralized off-site inspection/delivery point that is separate from the primary ECP, and allow no access to passenger vehicles; require an off-site parking area.

□ The ECP design should anticipate increased traffic volume and should support the employment of required FPCON measures and RAMs, as outlined in the JFOB Force Protection Plan.

□ The number of ECPs should be kept to a minimum. However, a large JFOB should consider one ECP for truck/commercial vehicle inspection and access only, one ECP for pedestrian access, one for military vehicle access, etc. Limiting the number of functions to be conducted at each ECP and the amount of usage reduces the infrastructure and manpower requirements.

□ A major factor in determining the type of ECP should be the size of vehicles requiring entry. At least one ECP should be designed to accommodate large and/or oversized vehicles (military vehicles) and another for normal sized vehicle traffic. Where possible, a tertiary gate should be planned for contingencies and for emergency vehicular and pedestrian egress.

□ When possible truck/commercial and passenger vehicle traffic should be segregated and compartmentalized, and separate search areas should be constructed for each. The reasons for segregating these vehicles, if possible, include the following:

- The effectiveness of most speed management techniques/barriers for passenger vehicles decreases if trucks/commercial vehicles must use the same lanes (distances between barriers must be increased and lanes widened for larger vehicles).
- Search requirements for trucks/commercial vehicles and passenger vehicles differ significantly.

- Separate search areas help avoid congestion and improve efficiency of searches during 100% inspections.

□ To accommodate oversized, atypical vehicles, such as military vehicles and equipment, the ECP design may require modifications to lane widths, size of inspection areas, spacing of barriers, and other potential obstructions:

- The minimum lane widths for an ECP should be 3.0 m (10 ft).
- The preferred lane width is 3.6 m (12 ft).
- Lanes approaching the gate should be 3.6 m (12 ft) wide, plus another 0.61 m (2 ft) 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 roadway should be designed with the required turning radius to allow a single movement for the vehicle to be rejected or redirected. Where possible, the ECP should incorporate the turning radii outlined in the Policy on Geometric Design of Highways and Streets by the American Association of State Highway and Transportation Officials (AASHTO WB-15m (WB-50)). The radius of a corner or turning lane depends on the largest vehicle expected to use the lane and the average turning speeds, which should be quite low for an ECP. Other factors to consider include the available right of way, the angle of the intersection, and pedestrian activity. The following minimum inside radii should be used:

- Locations serving only passenger vehicles: 4.57 m (15 ft) to 9.14 m (30 ft); preferred is 6.1 m (20 ft)
- Corners where RVs, SUVs, or similar vehicles turn: 10.67 m (35 ft)
- Intersections where large trucks (WB-50), including semi-trailers, (WB-67) turn: 15.24 m (50 ft)
- Turnarounds for large trucks: 19.81 m (65 ft)

□ 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. Inspection and search areas should have sufficient area to safely move vehicles from the lanes of traffic to conduct thorough vehicle inspections.

- The minimum width should be 5.5 m (18 ft) to facilitate the safe inspection of vehicles.
- The length of a pull-off area or inspection area should be a minimum of 12.2 m (40 ft) or the length required to support the largest vehicle expected at the ECP, whichever is larger.
- As a minimum, the JFOB should provide the following inspection areas:
  - For standard vehicles: 4.5 × 7.2 m (15 ft × 25 ft) inspection bays that can be enclosed, if necessary, to protect inspection equipment in the event of bad weather.

- For commercial vehicles: 5.5 × 24.4 m (18 ft × 80 ft) × 5.4 m (17 ft 6 in.) high inspection bays that can be enclosed to protect inspection equipment in the event of bad weather.

Access control section of Chapter 6 provides personnel and vehicle inspection techniques.

□ ECPs should have a dedicated right-of-way protected from encroachment by buildings, trees, and other objects. The ECP should not be located near restricted/clear zones and identified critical or vulnerable assets or near congested areas, housing, schools, and commercial areas, both on and off-site, to avoid interference with pedestrians, parked cars, and driveways.

□ Entry roads to JFOBs and to individual buildings should be designed so that they do not provide direct or straight-line vehicular access to high-risk assets.

□ Parking areas should be located away from high-risk JFOBs and critical assets to minimize blast effects from potential VBIEDs.

□ Signs identifying high-risk JFOBs and critical assets should be kept to a minimum.

□ ECPs should provide full containment and control of vehicles. 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. Vehicle containment can be achieved through a combination of passive and active vehicle barrier systems. Active barriers require some action, either by personnel, equipment, or both, to prevent entry of a vehicle. Passive barriers require no action once in place and are normally used to direct and channel the flow of traffic.

□ The selection of passive and active anti-vehicle barriers should be based on their capacity to stop threat vehicles. Other considerations include:

- o Barriers should have a limited profile in order to minimize cover and concealment positions for aggressors.
- o Barriers should encompass a contiguous perimeter around the ECP, with the final denial barriers completing the containment.
- o Barriers should be arranged to ensure that a vehicle does not circumvent the ECP once the vehicle has entered the approach zone.
- o Barriers should complement the employment of other physical and procedural security requirements.

□ Containment may also be accomplished with natural or constructed barriers:

- o 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 (see Figure 6-13).
- o 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 the search area should force the driver to ram through a gate or barrier, clearly demonstrating hostile intent to the overwatch.
- Anti-vehicular barriers must not obstruct fields of vision or fields of fire for the overwatch or backup security forces.

□ 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 vehicular traffic and ensure pedestrian walkways are integrated into the existing site layout. Pedestrian access control considerations include:

- 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.
- 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 (i.e., 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 (see Security Lighting section of this chapter). Factors that should be considered in this design include:

- Power requirements for future traffic control devices, identification equipment, and other devices associated with potential automation of the ECP.
- An alternate electrical power source. 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.

□ The ECP should be provided with multiple, redundant lighting to ensure that the loss of a single light does not seriously degrade the total lighting available for security personnel. Guidelines for lighting include:

- The approach and response zones require typical roadway lighting. Roadway lighting should provide enough intensity so that vehicles, pedestrians, security personnel, islands, signage, and other hazards are visible.
- The lighting should not be directed in the driver's eyes, and it should not backlight security personnel or important signage.
- In the access control zone the lighting should illuminate the exterior and interior of a vehicle to facilitate identification of the occupants and the vehicle contents.

- □ Additional key concepts that should be incorporated into an ECP design include:
  - o Layered defense
  - o Nonlinear design
  - o Maximized protection for ECP personnel (multiple guardhouses)
  - o Maximized standoff
  - o Traffic and pedestrian segregation and channeling
  - o Multiple vehicle turn around/rejection areas
  - o Vehicle speed management/reduction through the use of serpentines and vehicle barriers
  - o Segregated search areas with line-of-sight denial from possible external surveillance
  - o Overwatch positions (hardened fighting positions)
  - o Hardened perimeter gate access (final denial barrier)
- □ Concepts that should be incorporated into ECP exit–point design include:
  - o 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 JFOB by going against the flow of exiting vehicle traffic.
  - o An active barrier should be used to maintain positive control over an exit lane and to prevent someone from entering the JFOB through the exit.
  - o The active barrier should be bounded by measures, such as serpentines and speed bumps/tables, that slow vehicle traffic from both outside and inside the installation before it reaches the active barrier.
  - o 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.

DESIGNING THE SEARCH AREAS

- □ 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 JFOB. Personnel who do not need to drive into the JFOB 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 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, tall concrete barriers (Texas, Alaska, Bitberg), or earth-filled barriers (HESCO bastion and metal revetment) should be placed around the search pit to protect nearby personnel from fragmentation should a bomb-laden vehicle explode while being searched. Soil-backed concrete barriers provide better protection against secondary debris hazards.

□ 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 JFOB.

□ 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.

□ Shade. In order to maximize the effectiveness of security personnel and MWDs, the search area should have overhead protection from the sun.

□ 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 fans and dog shoes.

□ 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, such as x-rays that utilize backscatter or transmission imaging, which can be used at ECPs to augment bomb detection capabilities. 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.

OVERWATCH

The overwatch for an ECP is a manned position that provides observation and has the ability to employ deadly force against vehicles and attackers that attempt to bypass, ram, or otherwise run through an ECP. Overwatch planning considerations include:

- The overwatch should be equipped with a weapon that can stop a vehicle by disabling it or killing the driver. This weapon should be no smaller than an M60, M240G, or other type of medium machine gun. Other weapons likely to stop a vehicle include the M-2 .50 caliber heavy machine gun, the MK19 40 mm machine gun, and the AT-4.
- The overwatch should be planned and designed with the same considerations as those used against an ambush; Fix the enemy in place so you can kill him.
  - 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.
- 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 and HN buildings and personnel possibly in the fan.
- 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.

Figure 6-28. M60 Overwatch

- □ Rules of engagement criteria should be defined and readily available for the overwatch position.
- □ The overwatch weapon system should require minimal traversing and elevation (T&E) adjustments to continually bring fire on the kill zone.
- □ All overwatch positions should be equipped with 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.
- □ 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.
- □ In determining a location for the overwatch, security forces should consider the following:
  - o Can the overwatch clearly observe the ECP and its barriers?
  - o Is the overwatch able to clearly determine the circumstances under which he is authorized to employ his weapon?
  - o Is the overwatch able to engage a hostile vehicle while it is at least 100 m away?
  - o 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?
  - o 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?
  - o Can the overwatch employ his weapon 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 sec?
  - o How much distance does the overwatch have to engage the target vehicle?
  - o Can the weapon bring enfilade fire to bear on the hostile vehicle?

Anti-Vehicular Barrier Design. Anti-vehicular 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 be effective, anti-vehicular barriers at the ECP should be a combination of active and passive barriers that are integrated with the surrounding perimeter barrier system. Active barriers alone are less likely to stop a moving vehicle than their passive (static) counterparts; however, when properly integrated with passive barriers, they can effectively stop vehicles. Active barriers that can be easily opened and closed can help maintain positive control of the traffic flow

through the ECP. Anti-vehicular barriers should be used to control traffic flow into the search area and through the entrance and exit lanes.

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
- □ Nonlinear lane designs
- □ Serpentine layout of lanes with anti-vehicular barriers, such as concrete barriers (Jersey, Alaska), concrete blocks, earth-filled barriers (HESCOs, metal revetment), and cabled steel hedgehogs. The tighter the serpentine or "S" turns, the more the vehicle must slow down (see Figures 6-29, 6-30, and 6-31).

Speed bumps and tables 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.

The most effective design is one that uses a combination or combinations of the above speed management techniques (see Figure 6-27).

Serpentine Pattern for Anti-vehicular Barriers. Due to centrifugal force, it is difficult for a threat vehicle to drive fast on a curve unless the road surface is banked. When centrifugal force is great enough, the tires of the threat vehicle will overcome the road friction and start to skid. The threat vehicle may also overturn if its center of gravity is too high. Therefore, when constructing an anti-vehicular barrier system for a JFOB ECP, security forces should consider a serpentine pattern. The following table and diagram depict recommended distances between barriers as well as an example of a serpentine layout.

MOVING VEHICLE – SPEED CONTROL OBSTACLES

- "S" curves
- 90 degree bends
- Traffic Circles
- Speed bumps
- Serpentines

Separation Distance (D)* for Barriers to Reduce Speed on a Straight Path in Feet (m)

Achievable Speed of Vehicle on a Curve in mph (kph) → / Road Width in ft (m) ↓	20 (32)	30 (48)	40 (64)	50 (80)	60 (97)
20 (6.2)	28 (8.5)	43 (13.1)	58 (17.7)	73 (22.2)	87 (26.5)
30 (9.3)	40 (12.2)	63 (19.2)	86 (26.2)	108 (32.9)	130 (39.6)
40 (12.4)	47 (14.3)	77 (23.5)	106 (32.3)	134 (40.8)	161 (49.1)
50 (15.3)	51 (15.5)	87 (26.5)	122 (37.2)	155 (47.2)	187 (57.0)
60 (18.3)	54 (16.5)	96 (29.2)	135 (41.1)	172 (52.4)	209 (63.7)

*Based on f=1.0

Figure 6-29. Separation distance for barriers to reduce speed on a straight path

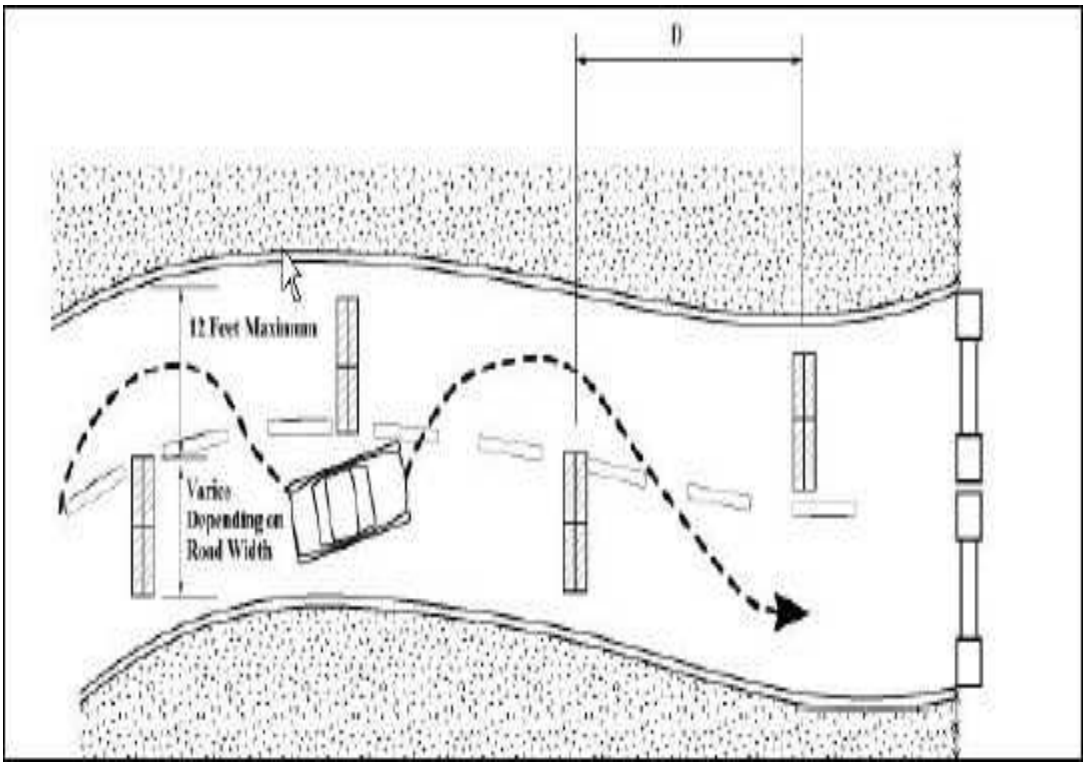


Figure 6-30. Concrete barrier/block serpentine layout to reduce speed

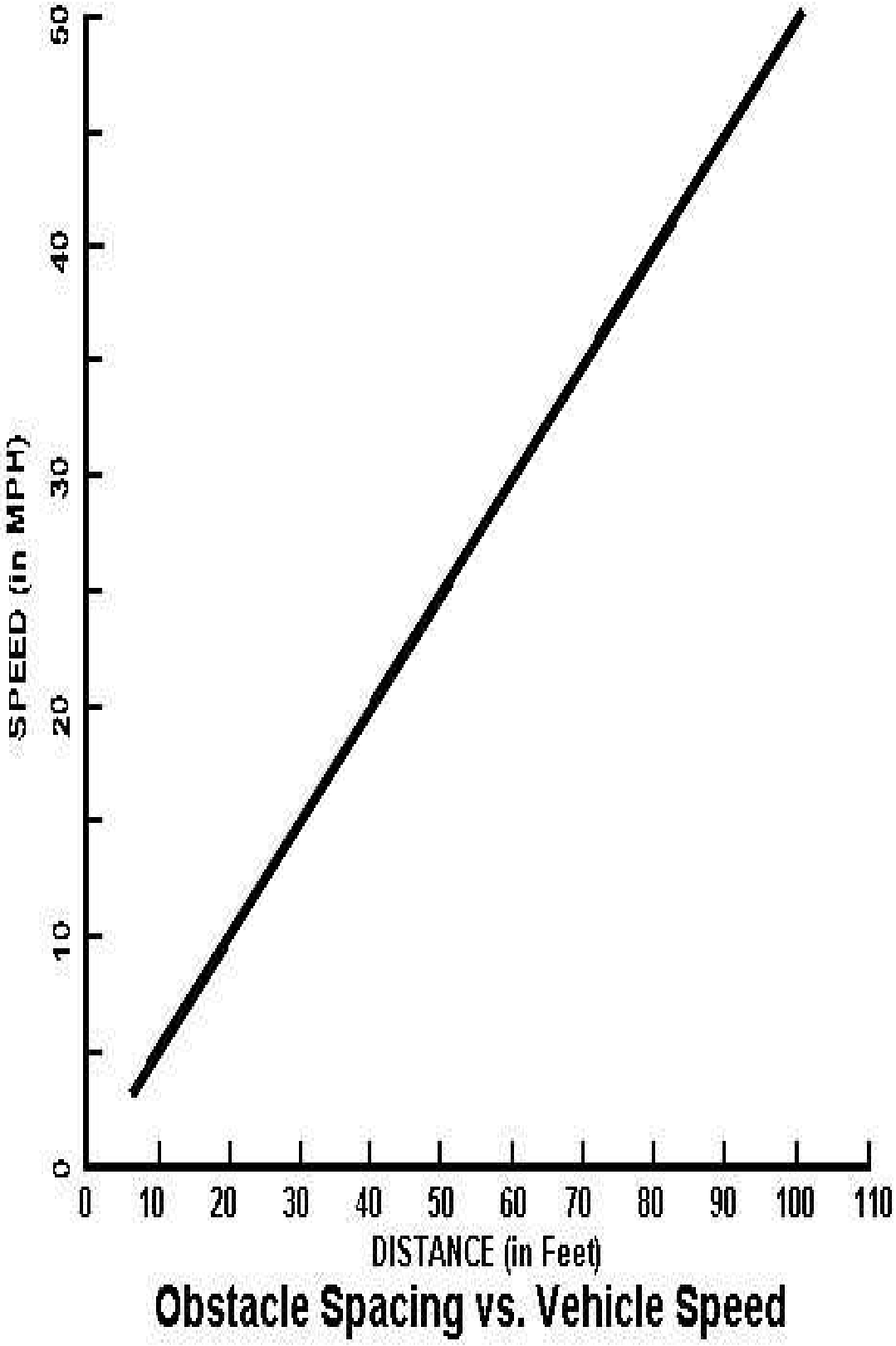


Figure 6-31. Moving vehicle – speed control obstacles (From TM 5-853-2)

ECP Barrier Types and Selection Considerations. A DETAILED DESCRIPTION OF MATERIALS THAT CAN BE CONSIDERED FOR USE IN ECPS IS INCLUDED IN THE PHYSICAL BARRIER SECTION OF CHAPTER 6. TYPES OF MATERIALS INCLUDE THE FOLLOWING:

- □ Concrete barriers (Jersey, Texas, Alaska, Bitberg)
- □ Concrete blocks
- □ Cabled chain link fences
- □ Guardrails
- □ Reinforced concrete walls
- □ Berms and ditches
- □ Earth-filled barriers (HESCO bastions, metal revetments)
- □ Bollards
- □ Cabled Steel Hedgehogs
- □ Expedient barriers (steel pipe, destroyed or captured enemy vehicles, construction or military vehicles, buried heavy equipment tires, tire shredders)

In selecting barrier materials, security personnel should consider the following:

- □ What is the purpose for the barrier? Antipersonnel or anti-vehicular?
- □ If anti-vehicular, what is the counter-mobility capability of the barrier?
- □ Does the barrier have blast-mitigation capability?
- □ If a blast occurs, will the barrier create secondary fragmentation?
- □ Can the barrier be easily moved to accommodate changes (operational, capacity, FPCON) to the ECP?
- □ Is materiel handling equipment (MHE) available to place and move barriers?
- □ Can the barrier be anchored together?
- □ Can the barrier accommodate additional security measures (concertina top-guard, intrusion detection system, lighting, etc.)?

ECP Gates. The ECP typically ends at the JFOB perimeter. The ECP should have a gate or final denial barrier, enabling the ECP to be closed at the JFOB 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.

Personnel Gates. Personnel gates should be designed to permit only one person to approach security personnel at any time. For pedestrian use, single swing gates should be considered as the second alternative to turnstile gates.

Operational and security personnel requirements should be considered to determine the best type of personnel gate for a JFOB. Examples of personnel gates include single swing gates, double swing gates and turnstile gates.

Single Swing Gates. Swing gates should be designed with a minimum 4ft-(1.2m) wide opening by 8ft (2.4m) high plus 1ft (305mm) of three strands of barbed wire on top. The gate opening shall not exceed 14ft (4.3m). Gate frames shall be constructed from 2in. (51mm) (outer diameter) rails or 2in. square members welded in all corners.

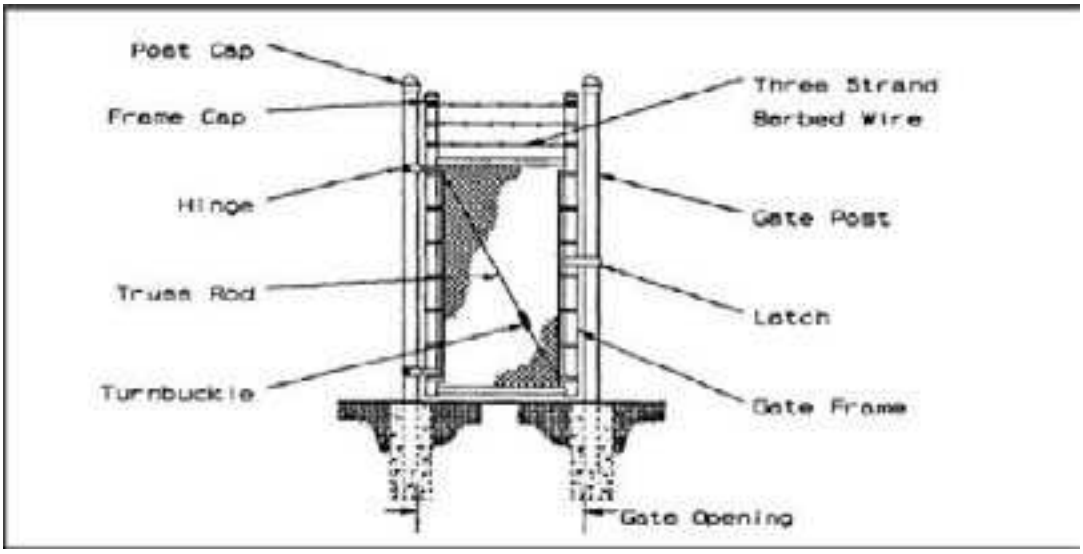


Figure 6-32. Single swing gate

Double Swing Gates. Double swing gate construction is identical to that of single swing gates.

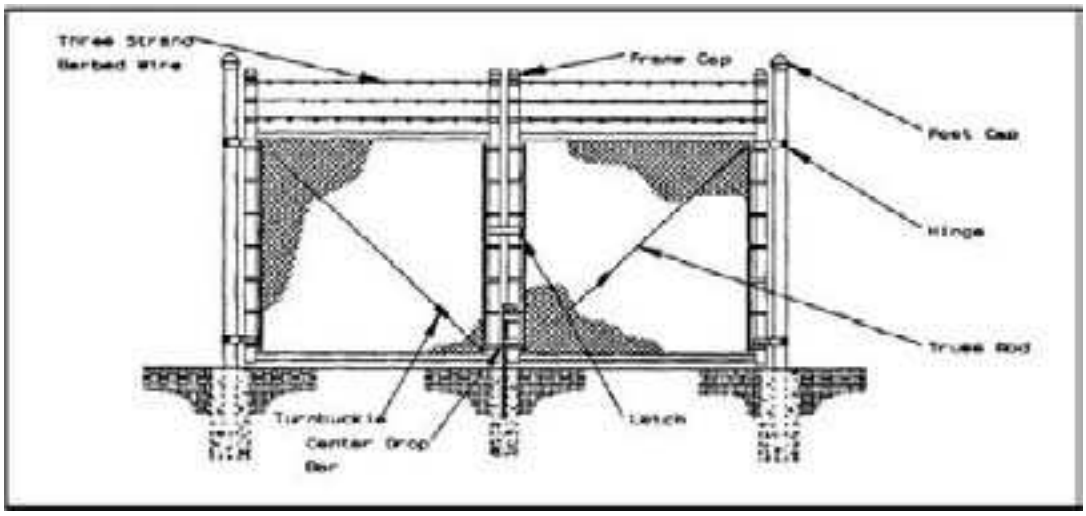


Figure 6-33. Double swing gate

Turnstile (Rotational) Gates. Turnstile gates 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 1-1/2in. diameter, 14 gauge (38mm) overall exterior height is 91in. (2.3m) with a pedestrian walk-through height of 84in. (2.1m).

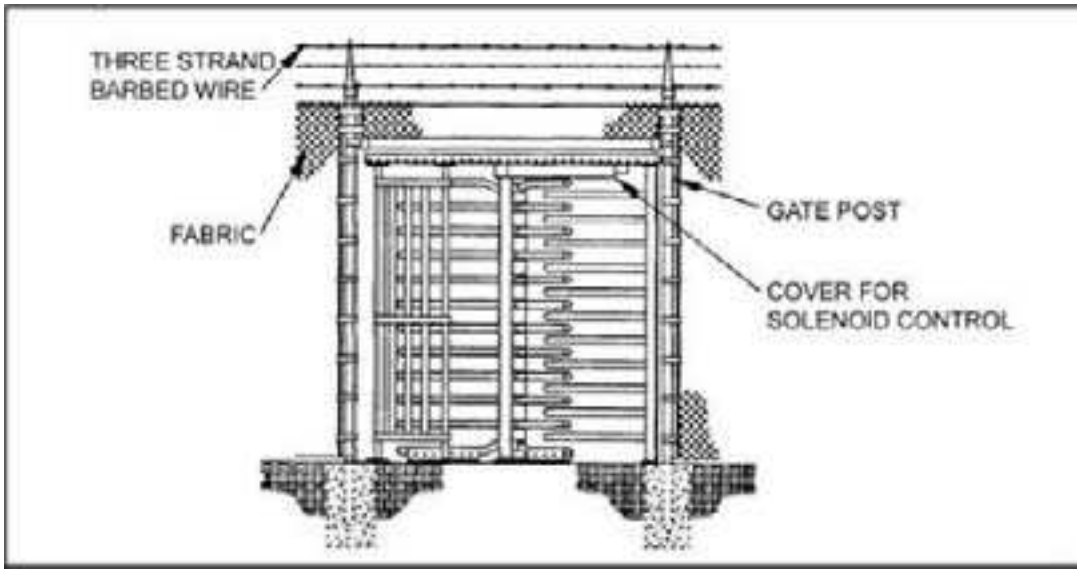


Figure 6-34. Turnstile (rotational) gates

Anti-Vehicular Gates. The expeditionary nature of the JFOB will require expedient and effective anti-vehicular gates. The selection of anti-vehicular gates should be based on an analysis of daily peak vehicular traffic, the operational access control requirements for the JFOB, operating cycle time, and the estimated speed of vehicles as they approach the gate. During operation, anti-vehicular gates should limit opening sizes when possible to decrease open/close cycle time. The ECP design discussed earlier in this section, if implemented, should slow vehicles to less than 10 mph. If this speed is accomplished, then lower impact gates, such as the drop-arm gates, can be used.

Cabled Crash Beam and Drop-Arm Barriers. This is the most commonly used active barrier at JFOBs. 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 Jersey barrier system. The crash beam is raised only to allow authorized entry.

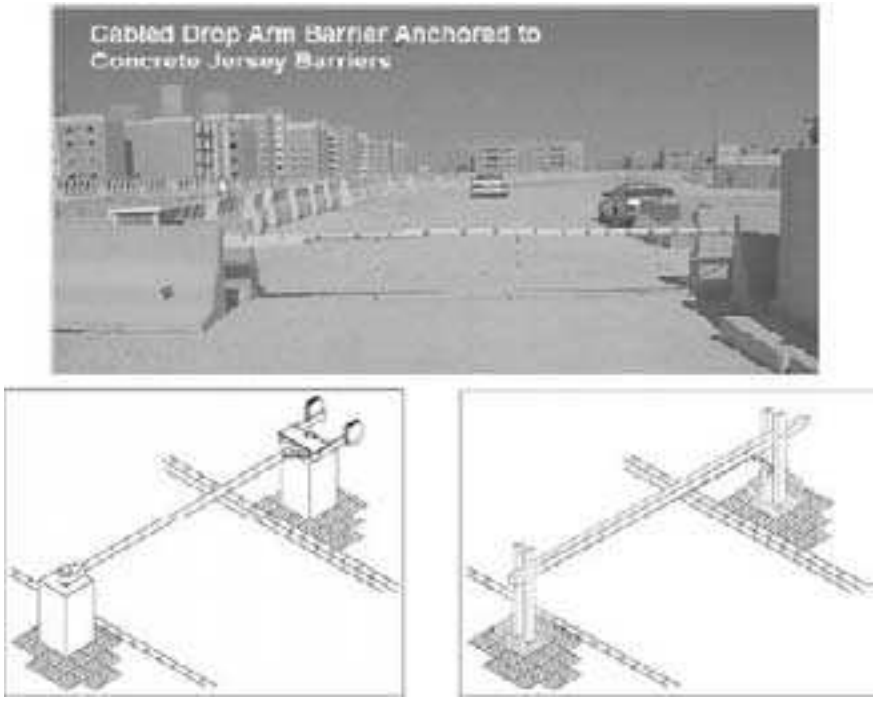


Figure 6-35. Drop-arm type barriers

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 be anchored to adjacent barriers.

Tire Shredders/Puncture Strips. Although tire shredders/puncture strips will not stop a vehicle, they may help cause a vehicle to lose control when combined with other obstacles. 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. 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. 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.

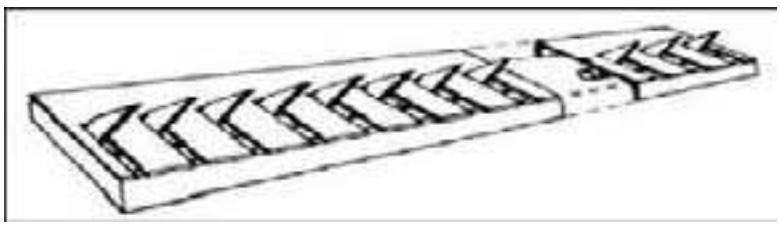


Figure 6-36. Tire shredder (puncture strip)

Cabled-Reinforced Chain Link Fence Gates. If cable-reinforced chain link fence gates are used to secure a JFOB, then wheel-supported or cantilever sliding gates are the best selection for vehicle security. 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.

The locking mechanism and the hinges on the chain link fence gate are the weakest components of the gate system. These areas can be reinforced by combining chain and wire rope (cable) to form a barrier across the opening. Once the chain and wire rope have been installed, the energy of a vehicle crash attempt is transferred from the gate through wire rope links to the side gate posts and further to the fence cable reinforcement system and deadman concrete anchors.

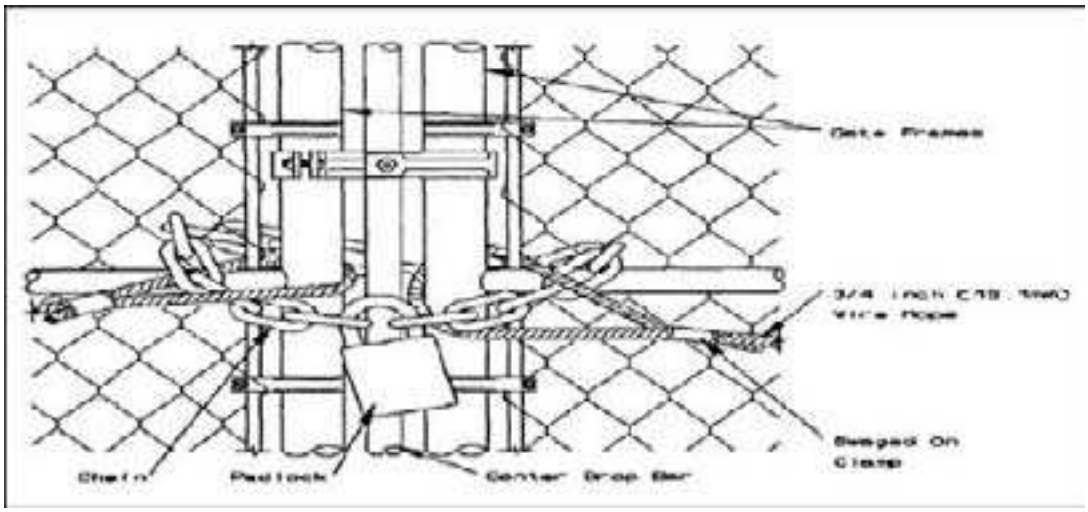


Figure 6-37. Locking mechanism for chain link fence gate

There is no generic or standard solution for hardening the various configurations of sliding gates; however, a 3/4in. (19.1mm) wire rope (cable) can be attached along the length of a sliding gate. The cable ends are then looped securely around the gate frame uprights at each end and affixed to deadman concrete anchors. The end of the fence reinforcement cable system should be looped around the terminal posts on each side of the gate opening. All cable ends should be looped and terminated with either three wire rope clamps or hydraulically swaged wire rope fittings.

Higher Impact Gate Designs. Higher impact gate designs should be installed in the ECP if the speed of approaching vehicles is expected to be greater. The USAF Force Protection Battlelab successfully tested the following design and stopped a 15,000-lb truck traveling at 50 mph.

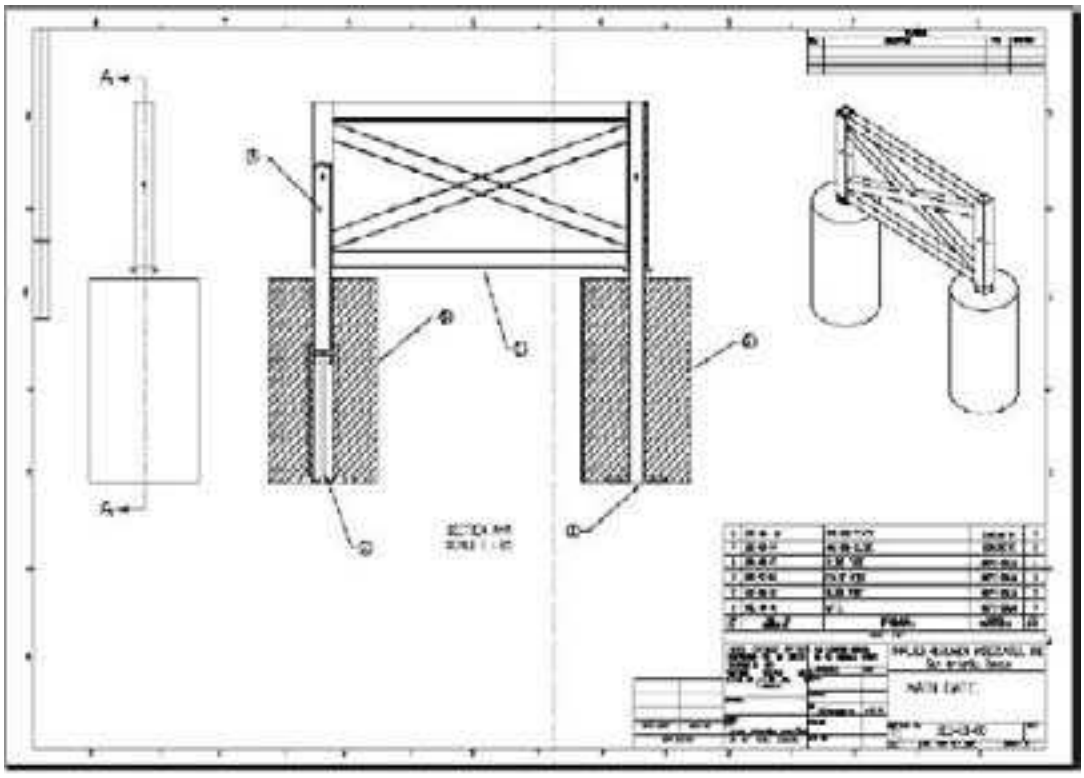


Figure 6-38. Gate design for higher impact

Personnel Access Control Point. The U.S. Army Corps of Engineers – Protective Design Center (PDC) has developed a personnel access control point that addresses the high threat environment in Iraq and Afghanistan and is capable of detecting explosives on persons or in hand baggage. The following charts summarize this design:

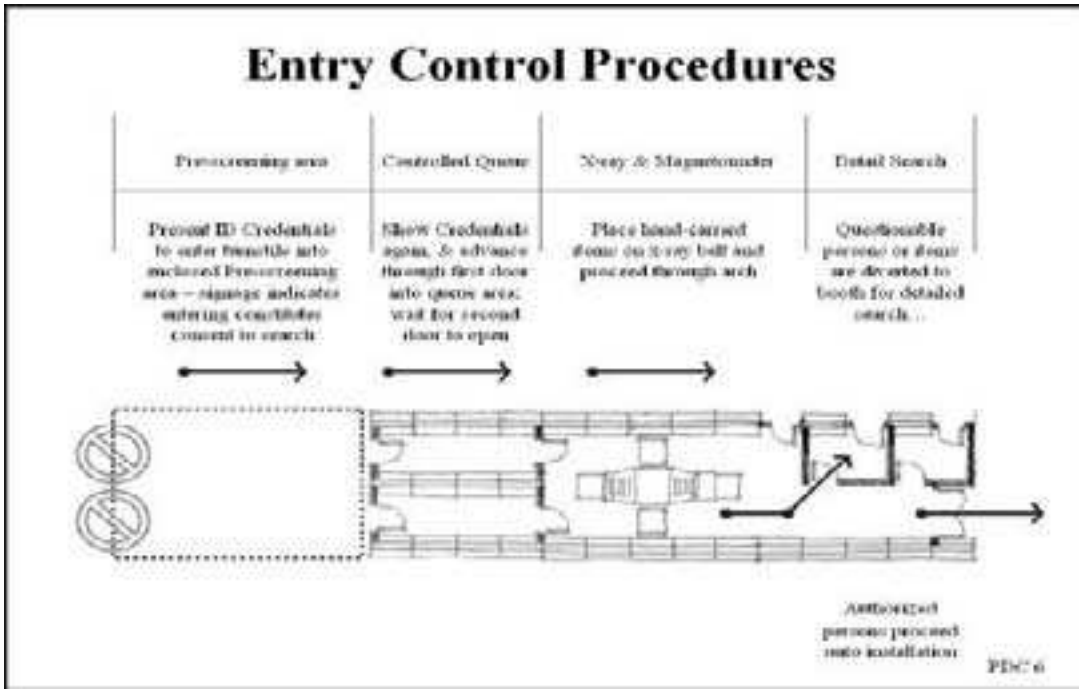


Figure 6-39. Entry control procedures

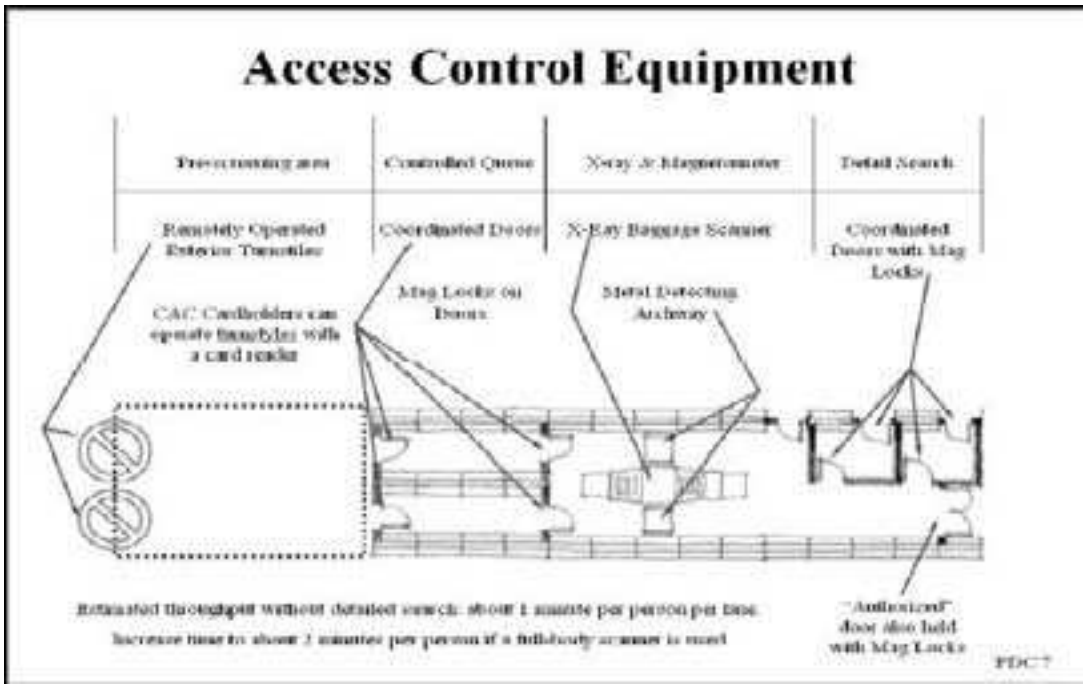


Figure 6-40. Access control equipment

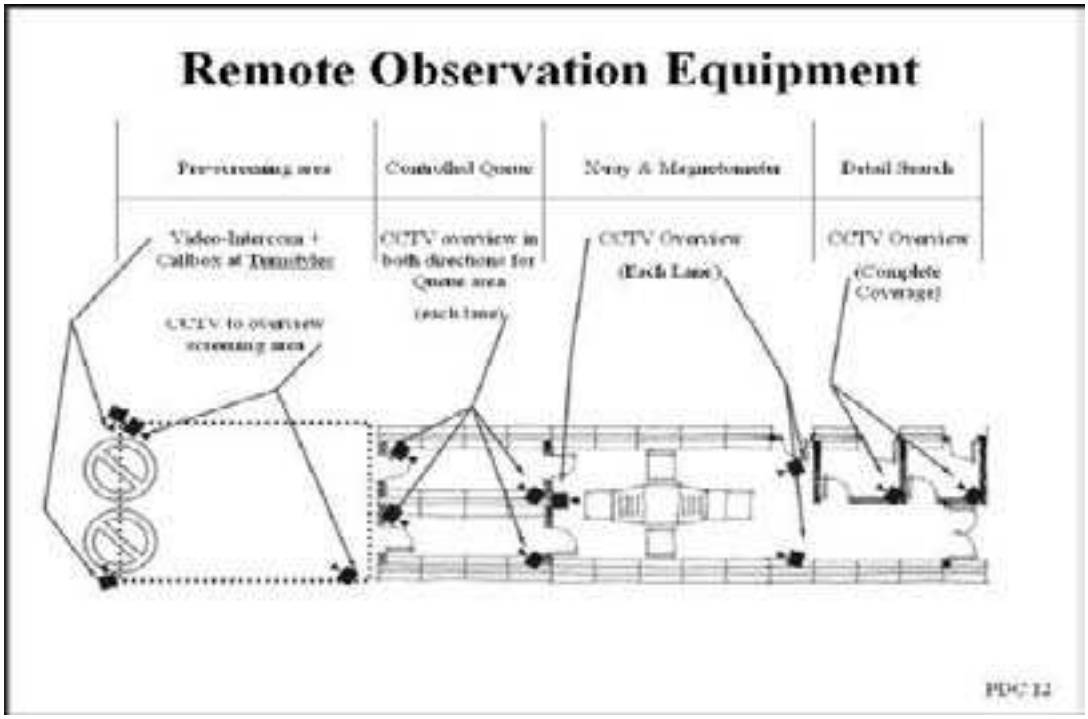


Figure 6-41. Remote observation equipment

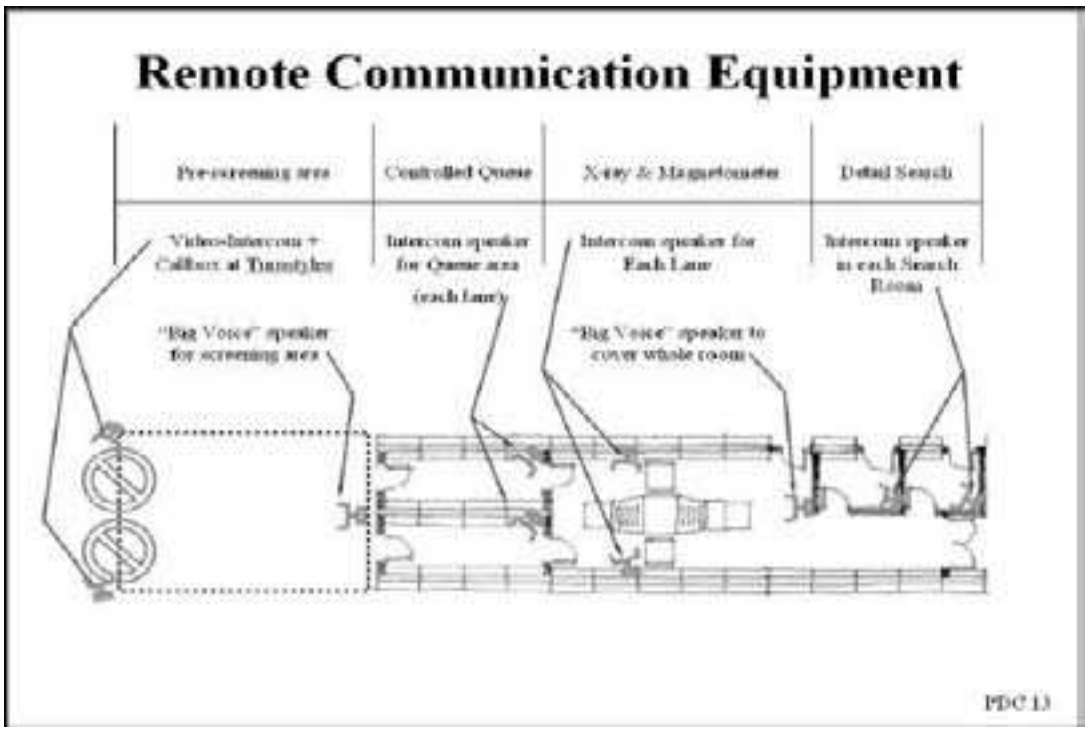


Figure 6-42. Remote communication equipment

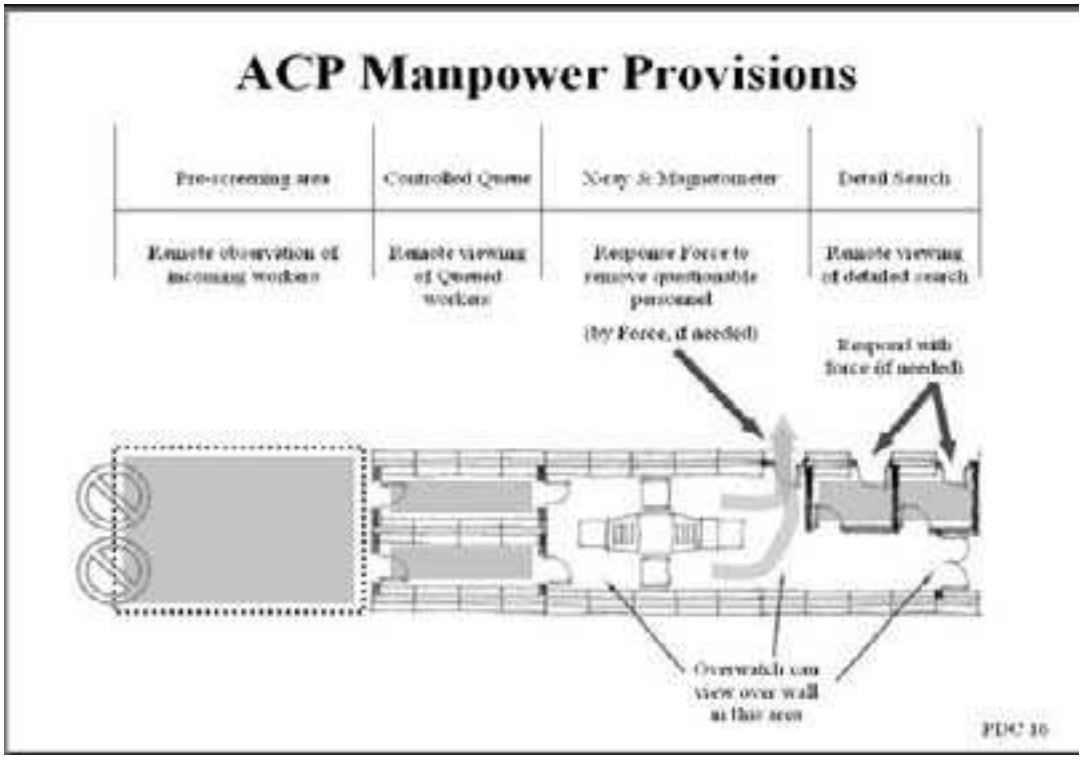


Figure 6-43. ACP manpower provisions

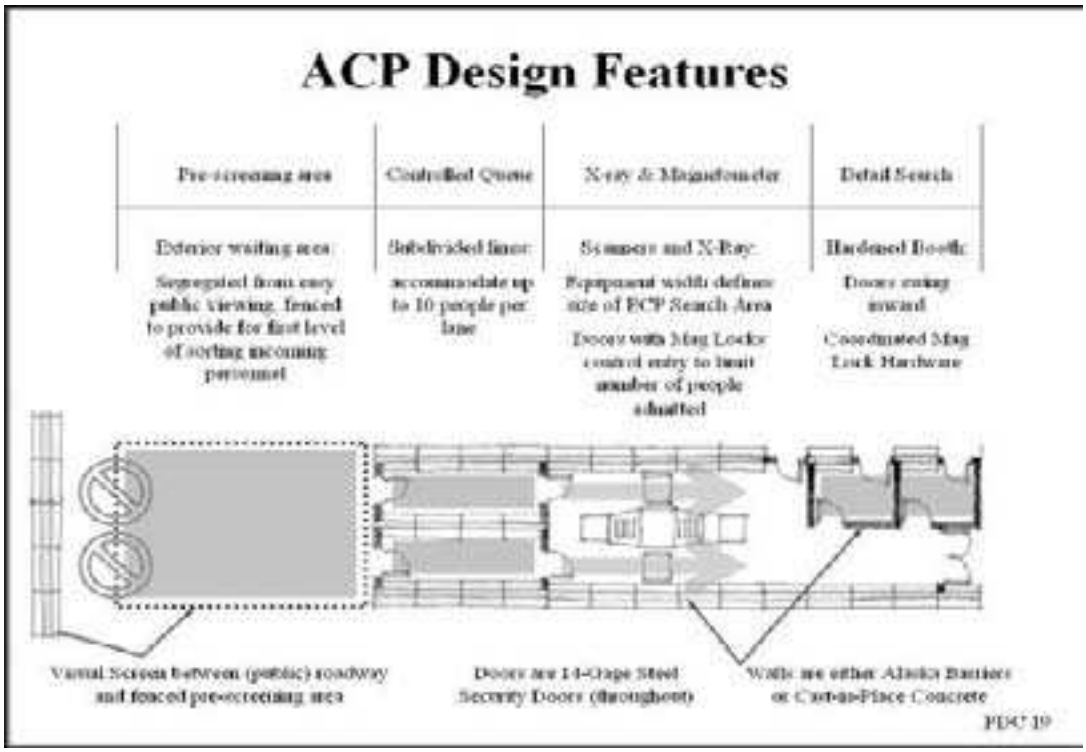


Figure 6-44. ACP design features

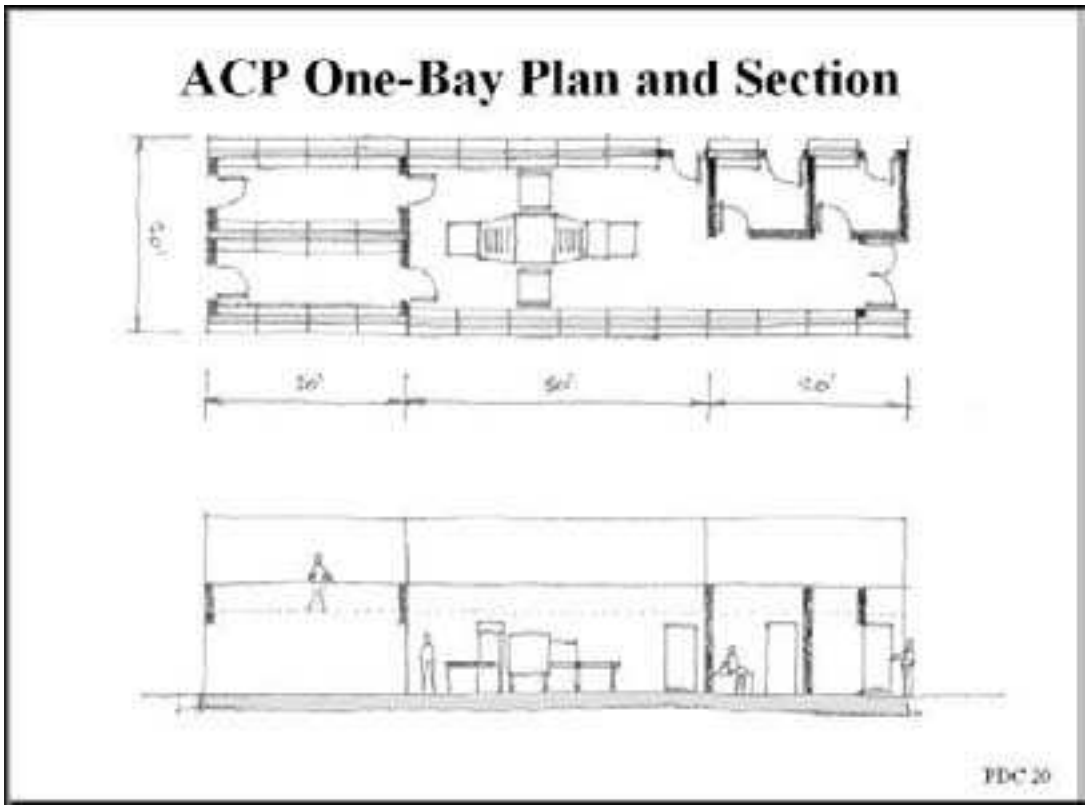


Figure 6-45. ACP one-bay plan and section

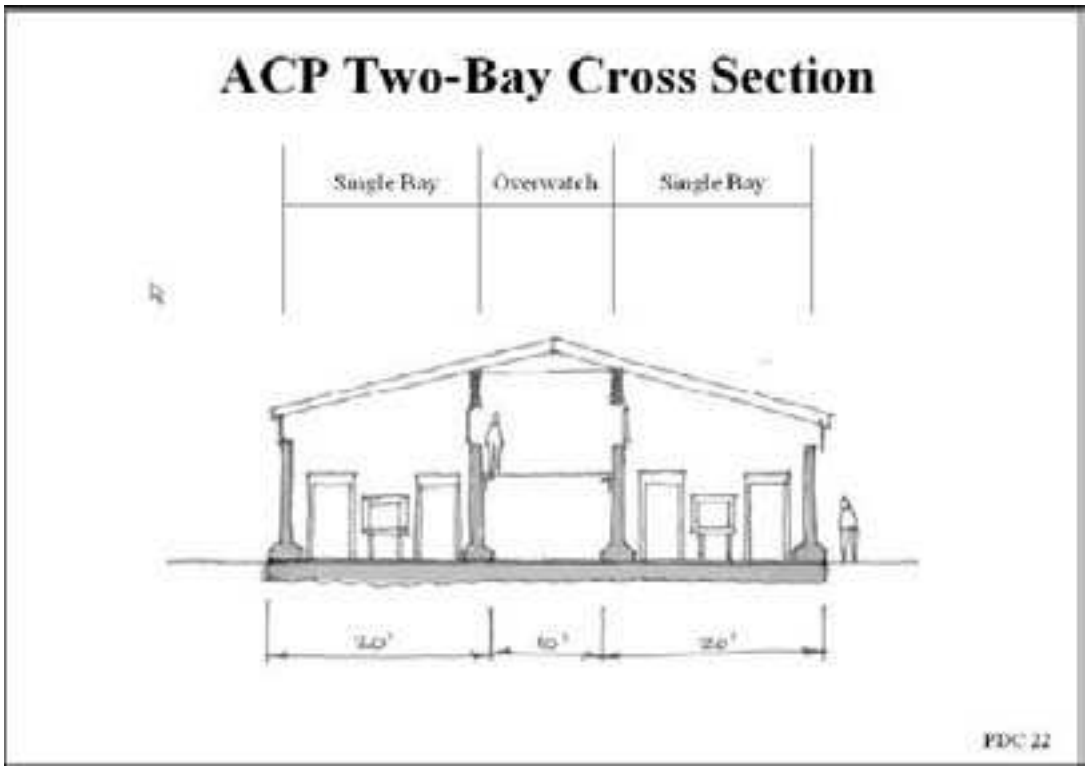


Figure 6-46. ACP two-bay cross section

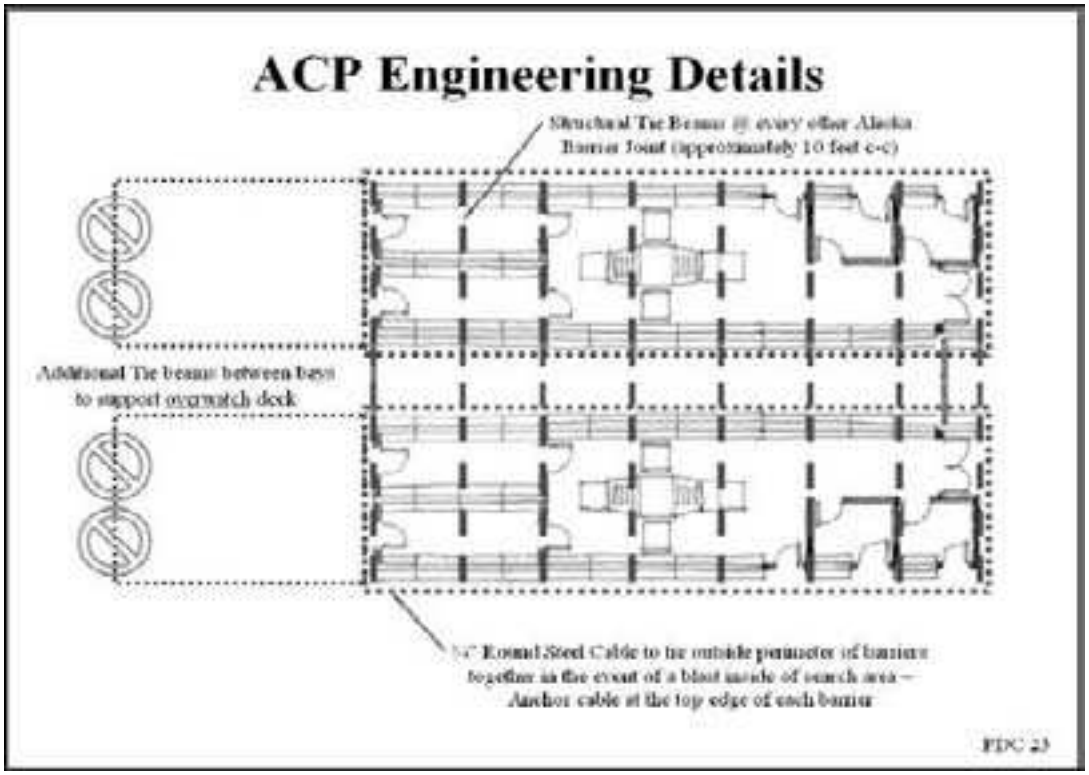


Figure 6-47. ACP engineering details

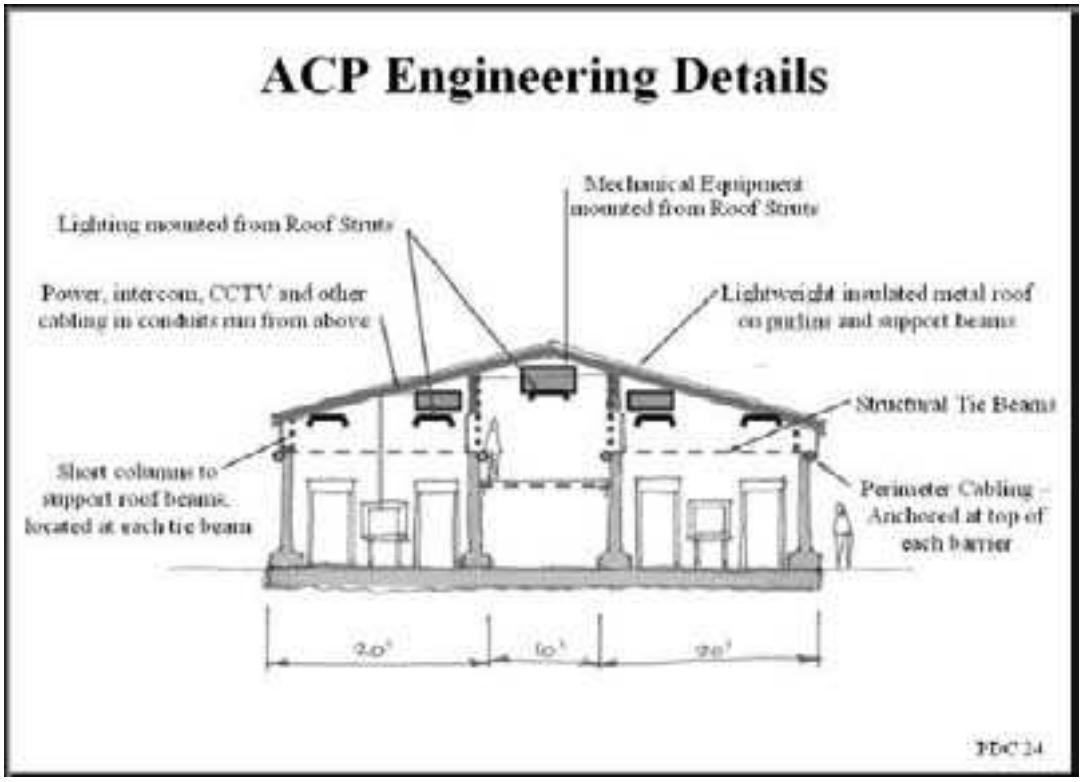


Figure 6-48. ACP engineering details cross-section

SECURITY LIGHTING

Light discipline will determine the type of lighting utilized for JFOB perimeter security and at ECPs. JFOB commanders may choose to enforce strict light discipline; if so, the type of lighting used on the perimeter and at the ECP may be limited. Regardless, protective lighting should enable security force personnel to observe activities around or inside the JFOB without disclosing their presence. Adequate lighting for all approaches to a JFOB not only discourages attempted unauthorized entry but also reveals persons within the area. Security lighting accomplishes the following:

- Aids threat detection, assessment, and interdiction
- Serves as a deterrent
- Increases the effectiveness of the security force and electronic security systems by increasing visibility range during periods of darkness or by illuminating an area where natural light is insufficient.

Lighting should not be used alone. Lighting should supplement other measures such as fixed security posts or patrols, fences, and alarms.

Requirements for protective lighting at a JFOB will be determined by

- Asset(s) and area(s) to be protected
- JFOB layout
- Terrain
- Weather conditions
- Security requirements

The overall goal is to provide the proper environment for personnel to perform duties, such as identification of badges and personnel at gates, inspection of unusual or suspicious circumstances, etc. Where lighting is impractical, additional compensating measures must be instituted. The remainder of this section discusses lighting concepts, standard types of lighting, and related lighting issues for guardhouses and ECPs.

Security Lighting 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 illumination 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.

Security Lighting Best Practices

To be effective, installed security lighting should accomplish the following:

- □ Provide adequate illumination or compensating measures to discourage or detect attempts to enter the JFOB 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 (i.e., CCTV) 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.

Types of Perimeter Lighting

- □ Continuous Lighting. Continuous lighting is the most common protective lighting system. It consists of a series of fixed lights arranged to flood a given area continuously with overlapping cones of light during the hours of darkness. Two primary methods of continuous lighting are glare projection and controlled lighting. This type of lighting may not be desirable for JFOBs where light discipline is a must, as continuous lighting could help attackers pinpoint the location of the JFOB.
- □ Glare Lighting. Glare lighting is installed 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 the guard by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter.

- Standby Lighting. Standby lighting is similar to continuous lighting. However, this lighting is not continuously lighted but is either automatically or manually turned on only when suspicious activity is detected or suspected by the security force or intrusion detection systems. This type of lighting may be very effective in high-threat environments like a JFOB.
- Emergency Lighting. Emergency lighting may duplicate any or all of the above systems. Its use is limited to times of emergencies that render the normal system inoperative. It depends on alternative power sources, such as installed or portable generators or batteries.
- Motion-Activated Lighting. Motion-activated lighting can be very effective in deterring intruders as it is turned on by the intruder's movement into a protected area.

Lighting Considerations for Guardhouses. Exterior lighting for sentry booths and guardhouses should be designed to minimize exposure of security personnel. "Glare protection" lighting is directed at the gate while the guardhouse remains in the shadows. The interior lighting in the guardhouse should be diffused lighting designed to aid night vision and provide additional security to the occupants. Night light units with a red lens enhance the occupant's night time vision. Guardhouses should have a standby power source.

Lighting Considerations for ECPs. Within the ECP, the lighting requirements vary, depending on the type of zone and light discipline restrictions. Unified Facilities Criteria (UFC) 4-012-01 "Security Engineering: Entry Control Facilities/Access Control Points" provides specific details and requirements concerning security lighting at ECPs and recommends foot-candle capabilities.

- Approach and Response Zone Lighting. The approach and response zones require typical roadway lighting. The roadway lighting should provide enough intensity so that pedestrians, security personnel, islands, signage, and other hazards are visible. The lighting should not be directed in the driver's eyes and should not backlight important signage or security personnel. Transitional lighting is necessary on approaches to the ECP so that drivers are not blinded during arrival and departure.
- Access Control Zone Lighting. In the access control zone, area lighting provided in the vicinity of the search facilities should be at a higher level to facilitate identification and inspection procedures. The lighting should illuminate the exterior and interior of a vehicle. In addition to good vertical illumination, additional task lighting may be necessary for adequate identification of vehicle occupants and contents. Such lighting should be directed across the roadway; it will then illuminate the roadway in front of the guardhouse, the driver, and the security personnel. Lighting may also be mounted at or below pavement level to facilitate under-vehicle inspection.
- Restrike or Restart Capability. Another important consideration in the design of JFOB ECP lighting is the restart, or restrike, time for the selected lamps. Restart occurs when a lamp experiences a loss of power and there is a delay

before backup power restores power to the lamp and triggers the subsequent restrike or restart of the lamp. As an example, high intensity discharge (HID) lamps are more energy conserving than incandescent lamps; however, they require several minutes to warm up and restart after power is interrupted. This warm-up period could be 15 to 20 minutes, an unsatisfactory delay for high-threat security operations. The selection of light sources, especially in the access control zone, should include an evaluation of restart or restrike time. It may be necessary to provide lamps and auxiliary equipment with rapid startup and restrike to ensure minimal adequate lighting in the event of a power interruption.

□ General Requirements. The ECP should be provided with multiple, redundant lighting to ensure that the loss of a single luminary does not seriously degrade the total lighting available for security personnel. The lighting at the ECP should be designed as controlled lighting to increase traffic safety. Glare projection, or glare lighting, should be avoided where a safety hazard would be created.

HARDENED FIGHTING POSITIONS / TOWERS / OVERWATCH

Hardened fighting positions. Chapter 8 provides designs and detailed instructions for using HESCO bastion and metal revetment materials to construct hardened fighting positions for perimeter security.

Guard Towers and Overwatch. Design of guard towers and overwatch positions must begin with a physical site study, including terrain analysis, and an analysis of security requirements. Based on this data, basic design considerations include:

□ Accommodations for the maximum number of personnel required in the guard tower(s)/overwatch to meet security requirements.

□ Required number of guard towers/overwatch.

□ Installation requirements for electronic and communications equipment, including location in the guard tower/overwatch, for optimum use by security personnel.

□ Requirement for and location of gun ports. 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 (i.e., night vision scopes).

□ 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.

- ☐ The location and height of the guard tower/overwatch that best suits a particular JFOB, 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.
- ☐ Placement of towers/overwatch inside the perimeter of the JFOB with at least a 30ft (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. A 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. 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 150mph (241.4km/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.

Pre-cast Concrete Pipe Guard Tower. This type of tower is constructed of eight precast elements. 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 as follows:

- ☐ The rectangular footing is placed on the ground.
- ☐ The bottom pipe section is placed on the base.
- ☐ The next pipe section is placed the same way.
- ☐ A floor section is then placed on the pipe section.
- ☐ The next pipe section is placed.
- ☐ A floor section is then placed on the pipe section.
- ☐ The cab section is placed.
- ☐ The roof section is placed.

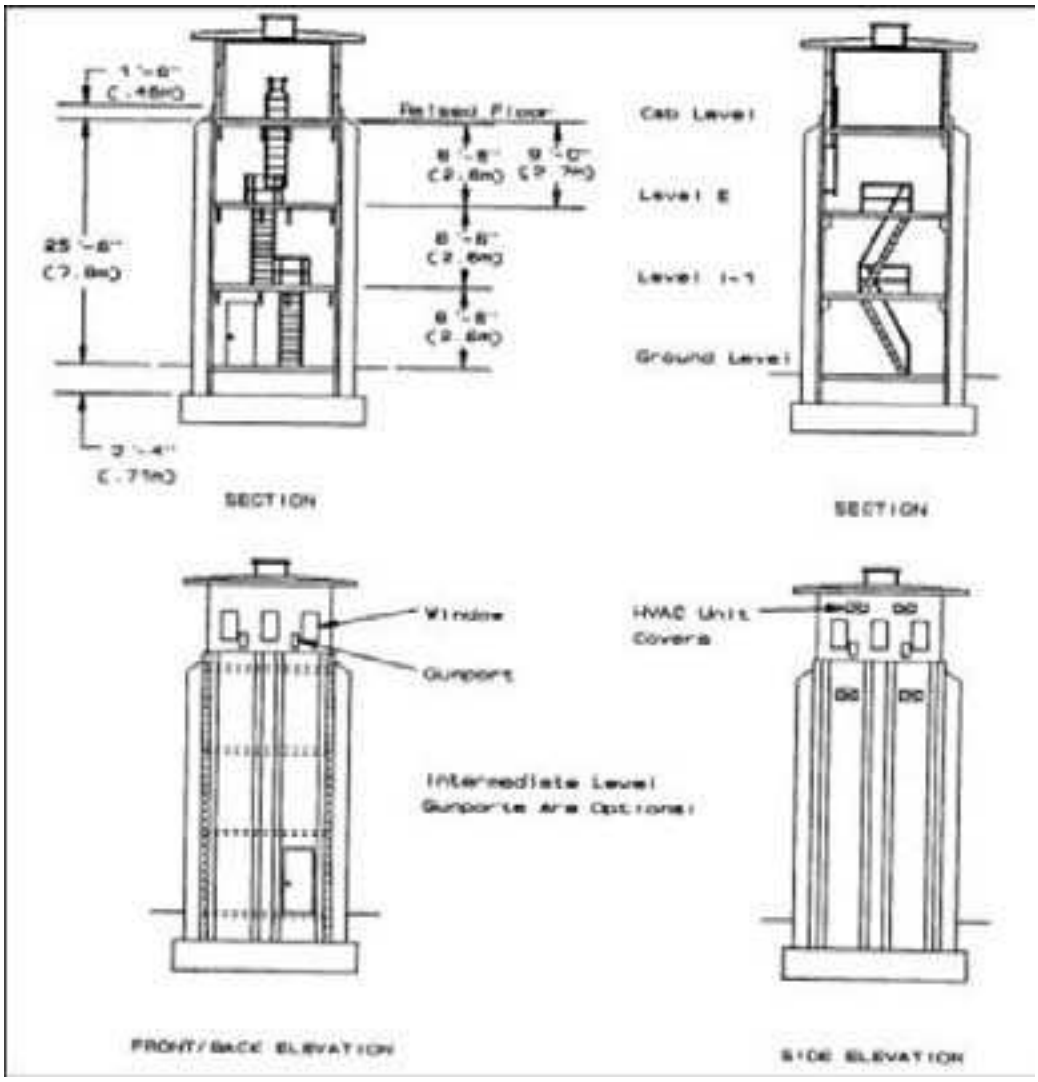


Figure 6-49. Pipe guard tower – construction view

Base slab: 200mm thick, 4000mm by 4000mm with four lifting hooks

Base segment: 300mm thick, 2000mm outside diameter, 2000mm high.

Base Segment Door: door opening is 800mm by 1800mm.

Floor segment: At elevations 6000mm and 8000mm there are floor segments 2000mm diameter and 200mm thick. Each has an opening for the ladder and operable steel cover plates for the openings.

Top Segment: 6-window openings 500mm by 600mm, 1250mm from floor.

Roof segment: 3000mm diameter, 300mm thick domed roof for drainage.

Interior ladder: Steel vertical ladder in segments welded to embedded plates in walls.

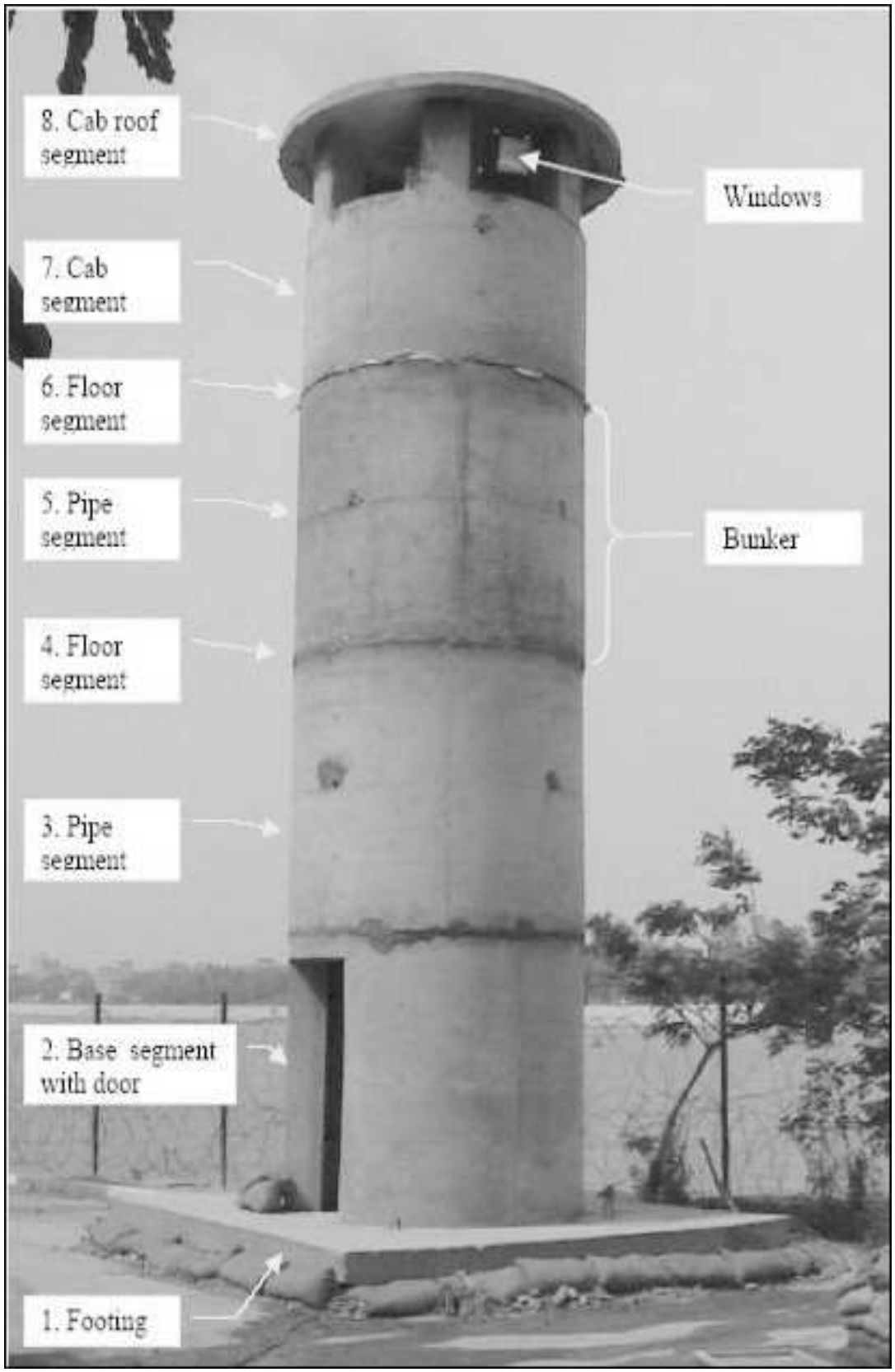


Figure 6-50. Precast concrete pipe guard tower

Camp Bondsteel, Kosovo Design

The following design was used extensively during the Kosovo campaign.

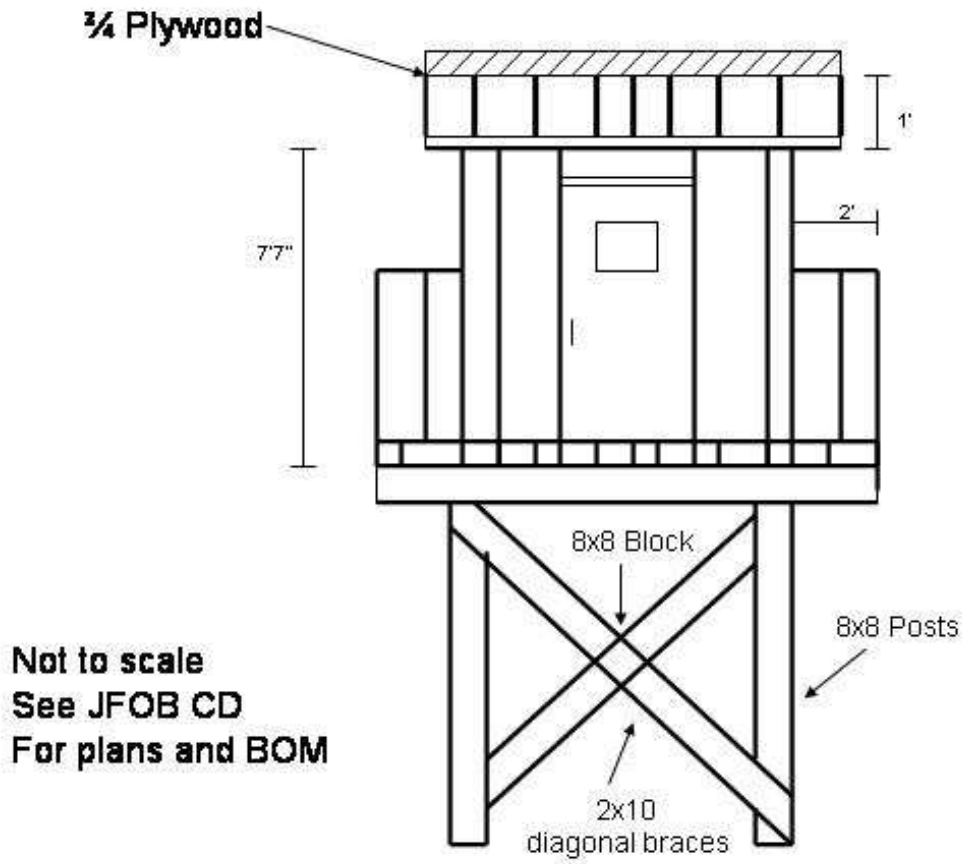


Figure 6-51. Perimeter guard tower example

INTRUSION DETECTION (IDS) AND SURVEILLANCE SYSTEMS

The function of perimeter IDS is to detect a threat and initiate a response by security personnel. Relying on perimeter IDS involves inherent risks. In high-threat environments like those for JFOBs in Iraq and Afghanistan, security personnel cannot rely solely on IDS. Rather, IDS should be an essential part of an integrated and layered approach to JFOB force protection.

OBJECTIVES OF IDS AND SURVEILLANCE SYSTEMS

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.

IDS AND SURVEILLANCE SYSTEMS FUNCTIONAL REQUIREMENTS.

Regardless of the type of system used to perform intrusion detection or surveillance, certain functions must be achieved by the system(s):

- Threat Detection. The earlier that threats are detected and the greater the distance that they are detected, the greater the opportunities to protect JFOB personnel, assets, and materiel. A wide variety of systems can be used to detect the presence of activity at a distance from the JFOB. However, several factors can influence system performance:
  - Seasonal and/or ambient weather conditions.
  - The type of background against which systems are attempting to operate. For example, motion detection systems work well in remote environments but can suffer data overload in an urban environment.
  - Environmental and/or geographical locations where the systems are placed, for example key terrain (hills, ditches, roads) or on fixed man made barriers (fences, walls, barriers).
  - The number and variety of systems used.
- Threat Annunciation. The threat detected by the security system must be reported to a central information processing center from which security forces can be dispatched. This annunciation capability should have redundancy.
- Threat Assessment and Classification. Once data is received in the information processing center, the detected data must be assessed and classified to determine whether the alarm is real or false and whether the intrusion is hostile or benign. CCTV can assist in the assessment of IDS.

Once assessed, the system should help classify intruders. Normally, this task is accomplished via human intervention and direct observation of the intruder with aid of CCTV, a night vision device, an infrared imaging device, or human interrogation.

- Threat Delay. Perimeter physical barriers coupled with IDS can effectively delay intruders. Delay has two purposes: facilitate definitive threat classification and assessment and facilitate response by security forces.
- Threat Response. Responding security forces assess the on-scene situation, and, if necessary, the on-scene commander can request additional assistance. Response to threats begins immediately upon detection and is designed to
  - Stop further intrusion by the threat at the greatest distance possible from protected assets.
  - Slow the rate of advance toward the protected asset(s).
  - Facilitate the evacuation of the protected asset(s) to safe areas.
  - Secure the protected area and contain the threat.
  - Prevent additional hostile resources from arriving.

IDS Selection Considerations. The requirement for an IDS must be identified and determined during the site selection and JFOB layout planning process (see Chapter 5). The IDS required cannot be completely identified until the proposed JFOB layout plan has been developed. A perimeter IDS designed to provide detection along a long perimeter may result in high system costs for installation, operation and maintenance. Regardless, the standard for selection of an IDS should be optimal performance achievable in local environmental conditions, such as soil, topography, weather, and other factors. These factors can adversely affect performance or increase false alarm (an alarm without a known cause) rates. Therefore, to ensure an effective system is selected, the performance parameters of the system should be primary concerns, including:

- Completeness of coverage
- False and nuisance alarm rates
- Probability of detection
- Zone at which the alarm occurred
- Delay time

If the delay time is too low, then the time available for effective security force response may not be adequate. The relationship between perimeter sensor location, delay times, and security force response times must be carefully examined.

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) and Security Technology Decision Tree Tool (STDTT) to assist in the selection

of IDS and surveillance systems. These tools can be found in Chapter 15 (Tools) of this handbook.

TYPES OF IDS. Several types of sensors (microwave, passive/active infrared, seismic, magnetic) are used throughout the USCENTCOM AOR. While sensors are NOT by themselves a layer of defense, they can greatly improve the effectiveness of security personnel. Types of IDS sensors include the following:

- Passive Infrared. Passive infrared (PIR), also known as thermal infrared, alarms are generated by a change of thermal radiance within the detection zone. Daytime nuisance alarms can be activated by backgrounds having a variety of materials that are alternately sunlit and shaded due to intermittent cloud cover. The likelihood of daytime nuisance alarms is low on overcast days or when the IDS's detection zone is shaded.

- Active Infrared. An active infrared IDS detects a target when the pulsed infrared beam that transmits across the detection zone is interrupted. The beams are not visible to the eye. Multiple beams are arrayed vertically to provide line-of-sight detection to the height desired. Their vertical spacing defines the detection pattern. The distance of the detection zone can vary from 300 to 1200 feet.

- Microwave Radar. There are two types of microwave radar sensors: bistatic systems that have separate transmitter and receiver units and monostatic systems that combine the transmit and receive functions in one unit. These sensors generate an alarm when the receiver detects a change in the microwave field. The change can be caused by microwaves scattering off an intruder. Nuisance alarms can be triggered by site conditions, such as reflections from metal objects or water or heavy rain or snow. Also, vegetation and piled sand can shield a crawling intruder from detection.

- Near-Infrared Beambreak**.** Near-infrared beambreak sensors are active systems that alarm when a near-infrared beam (between transmitter and receiver units) is interrupted for a certain duration. Beambreak 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. To ensure detection of a crawling intruder, the detection zone should be level, with no elevated areas to shield the intruder or hollows to conceal him.

- 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. They detect a fence disturbance mechanically by the following means:
  - Lost contact when a mass is bounced off a support
  - Electrically by a friction-generated charge transfer between the inner and outer portions of a cable attached to the fence (triboelectric)
  - A charge transfer generated in a dielectric within a sensor cable subjected to mechanical stress (piezoelectric)

  - A relative motion between a conductor and a charge-storing dielectric (electret)
  - Optically by changes in the pattern of standing waves of light in optical fiber cables attached to the fence.

- Changes in fence motion depend on how well the fence posts are anchored in the soil and how stiff the fence panels are. The stronger the fence, the less likely the incidence nuisance alarms caused by wind loading.

- 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 array of wires (parallel to the ground) with additional wires on angled outriggers. Only a few centimeters of vertical clearance separates two wires or separates the bottom wire and either the ground surface or the top of a wall or fence. An intruder cannot pass his body through the gap without deflecting one or two adjacent wires.

- 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 (~ 5 to 9cm) depth. The cable is generally laid in a serpentine pattern to give dense coverage. Sand, gravel, and wet or loose soil are favorable burial mediums for ground motion IDS. Wind-induced motion of surface objects whose motion couples into the ground is the primary cause of weather related nuisance alarms.

- 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. The two cables may be placed in separate trenches or they may be encased together and laid in a single trench. Burial depth is typically shallow. The electromagnetic field extends above the ground surface, establishing a volumetric detection zone. Wet soil in the detection zone may be a persistent condition because of poor drainage, or it may occur temporarily during after rainfall. The correct location will eliminate this problem. Nuisance alarms can be caused by the motion of surface water or metallic objects.

- Seismic. Seismic sensors detect ground motion. Their detection range is greater for a moving vehicle than for a moving person. Seismic sensors are omni-directional, which generally renders them inappropriate for situations where legitimate activity is ongoing near the area being monitored for intruders. In such situations the seismic sensor does not discriminate between ground motion generated by the legitimate activity and ground motion generated by an approaching intruder. Seismic sensors are best used in remote areas where human or vehicle generated ground motion is the exception.

- Acoustic. Acoustic sensors are not used to detect personnel. They detect vehicles on the basis of the noise generated by the vehicle. An acoustic

sensor (microphone) typically is used in conjunction with a ground motion sensor (geophone). The sensor package reacts first to the geophone signal as an indication of intruder activity, and then, if certain criteria are met, it analyzes the acoustic signal to confirm that a vehicle is operating nearby. If the acoustic sensor activates only after ground motion criteria are met, then weather conditions that impede ground motion can prevent or reduce the likelihood of acoustic detections.

- Magnetic. Magnetic sensors detect movement of ferrous metal. They have a short detection range; the actual detection range depends on how much ferrous metal is carried by a person or vehicle moving past the sensor. Personnel, lacking metal objects, would not be expected to activate a magnetic sensor. Consequently, magnetic sensors are most effective when used in conjunction with another type of IDS that has the potential of discriminating between alarms caused by human activity and those caused by wildlife.

- 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. The extent of the sensor's detection zone is determined by the length of wire in use. The IDS must be manually reset after each break of the wire; there is no detection capability from the time the wire is broken by an intruder until the IDS is reset.

- Electrostatic Field/Capacitance. This sensor class includes electric field and capacitance systems. These sensors consist of a vertical array of horizontal wires that are free-standing or mounted to a chain link fence. The wires detect an intruder (as he approaches the wire array or extends part of his body between a pair of wires) by sensing his disturbance of the electrostatic field between the wires and the ground. The intruder does not have to contact the wires. Vegetation that extends into the electrostatic field, moving water, and wind induced motion of the wire arrays are potential causes of nuisance alarms.

- CCTV. Though not as effective as direct observation, CCTV is often used to augment security forces when 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. Standard video motion detection (VMD), which relies on changes in pixel gray scale to detect intruder activity, is subject to numerous nuisance alarms caused by moving shadows, wind-blown vegetation, and birds

and animals. AVS equipment is more likely than general VMD equipment to generate an acceptably low number of nuisance alarms. Detection capability with VMD and AVS can be diminished by sand storms that decrease visibility and visual contrast, and high levels of direct or reflected solar radiation that may saturate the camera detector. Several types of cameras can be used as part of AVS:

- Black/White Camera. All black and white cameras (also known as monotone cameras) can be used with visible and near-infrared illumination. Black and white video is less informative than color video in describing an intruder.

- Color Camera. Color cameras are suitable for use with visible illumination only, not with near-infrared illumination. Color cameras require a higher light level to produce video of the same quality as that of a comparable black and white. Color video is more informative than black and white video or thermal infrared video in describing an intruder. Color video monitors and color video recording devices also must be used if the advantage of color video in describing an intruder is to be realized.

- Day/Night Camera. Day/night cameras are a means of having the advantages of a color camera during daylight hours and a black-and-white camera with near-infrared illumination for use at night. The day/night camera may be a system of two cameras, or it may be a single camera with filters that automatically change with daytime and nighttime illumination. Some day/night cameras have a built-in near-infrared illuminator for nighttime use. The illuminator and black-and-white camera can be set to switch on and off automatically, according to ambient light level.

- Thermal Camera. Thermal infrared cameras define video scenes by thermal contrast (temperature differences among objects in the camera's field of view), rather than visual contrast, which is the basis of color and black and white camera imagery. Thermal cameras do not require illumination for nighttime operation. Thermal imagery is less informative than color video in describing an intruder.

EXAMPLE OF IDS AND SURVEILLANCE SYSTEMS

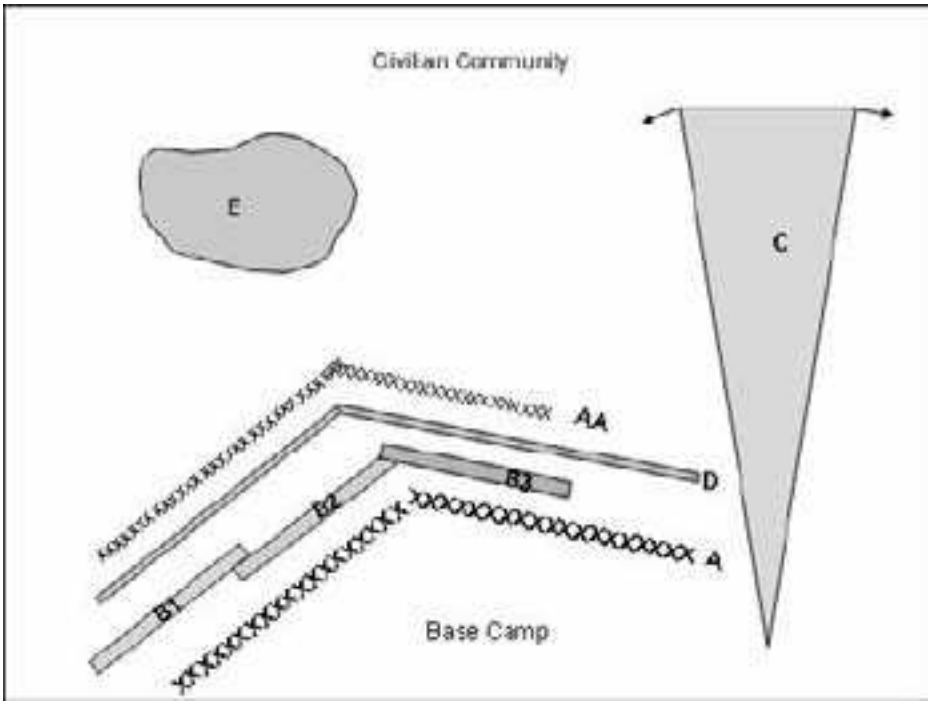


Figure 6-52. Diagram of intrusion detection system

- Object A in Figure 6-52 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 AA shows a second chain-link fence that, with object A, 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 A in the figure could be replaced with a taut-wire system. Options include:
    - Full height taut-wire system (ground to 8ft 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.

INFORMATION ON SOURCES OF TECHNOLOGY

The following organizations have produced manuals and guides to assist in the selection and employment of IDS and surveillance systems. These documents and selection tools can be found in Chapter 15 (Tools) or on the attached CD.

- *Weather Vulnerability Assessment Tool (WVAT) and Security Technology Decision Tree Tool (STDTT)*: U.S. Army Engineer Research and Development Center, Cold Regions Research and Engineering Laboratory (CRREL)

- *Security Equipment Resource Guide*; DoD Physical Security Equipment Action Group (PSEAG)

- *Perimeter Security Sensor Technologies Handbook*; Defense Advanced Research Projects Agency (DARPA)

- *Handbooks of Intrusion Detection Sensors and Access Control Technologies*; SPAWAR Systems Center Charleston

REFERENCES

DoD O-2000.12-H. *DoD Antiterrorism Handbook*, February 2004.

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

MIL-HDBK-1013/14, Selection and Application of Vehicle Barriers, 1 February 1999.

Marine Corps Order P5530.14. Marine Corps Physical Security Program Manual, 21 December 2000.

Physical Security Equipment Action Group (PSEAG) Security Equipment and Resources Guide, April 2001.

TM 5-853-2/AFMAN 32-1071 Vol. 2. *Security Engineering Concept Design*, 12 May 1994

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

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003.

UFC 4-012-01 (Draft). *Security Engineering: Entry Control Facilities/ Access Control Points*.

UG-2031-SHR. *User's Guide on Protection Against Terrorist Vehicle Bombs*, May 1998.

U.S. Air Force Entry Control Facilities Design Guide, 18 February 2003.

U.S. Air Force Handbook 10-2401. Force Protection Battlelab Vehicle Bomb Mitigation Guide, July 2004.

Chapter 7

INTERNAL SECURITY

Contents

INTRODUCTION

The perimeter security discussion (Chapter 6) was presented prior to a discussion of internal security in order to indicate the focus of effort and priority of work for force protection operations. Whether establishing a new JFOB or falling in on an already existing JFOB, military leaders should focus initially on establishing or reassessing force protection measures at the perimeter of the base. Once these measures are adequate, attention can be directed to internal security procedures. Internal security consists of those measures used to protect personnel or assets located on the interior of the base. Regardless of the type of measure implemented, a force protection team approach should be used to develop internal security procedures and manage the overall JFOB force protection mission.

UNITY OF COMMAND

The JFOB commander is responsible for base force protection and security operations. In this capacity, the JFOB commander should use all available assets within the perimeter to create the required level of security. Accordingly, the JFOB commander may, for purposes of base force protection and security, exercise temporary operational control (OPCON) or tactical control (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 JFOB 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 JFOB 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 JFOB's force protection mission. A senior commander, in this case the JFOB commander, will provide the authority to bring the various units together to accomplish the mission. JFOB command relationships should be established early, ideally prior to the units' occupying the JFOB. In addition, the JFOB commander should define areas of responsibility not only for units occupying the JFOB but also for the surrounding area that has direct influence on the security of the JFOB.

COORDINATION AND COOPERATION

Critical to the success of the JFOB force protection mission is the need for coordination and cooperation among the units tasked with supporting the JFOB. 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 JFOB operations officer, force protection officer, and the force protection working group should take the lead in orchestrating the coordination and cooperation effort.

FORCE PROTECTION TEAM

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

JFOB OPERATIONS OFFICER

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

JFOB FORCE PROTECTION OFFICER

The JFOB 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 JFOB 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 JFOB force protection working group in designing, developing and implementing force protection, antiterrorism and physical security policies and procedures

JFOB FORCE PROTECTION WORKING GROUP

Early during the occupation of a JFOB, a JFOB force protection working group should be established and activated. The working group is ideally suited for developing the JFOB 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 Ordinance Disposal (EOD)
- Communications
- Public Affairs
- Resource Management (Comptroller)
- Legal
- External Security Forces (Tactical Combat Force (TCF))
- Host Nation (HN) (as appropriate)

Figure 7-1. Working group organizational chart

BASE DEFENSE OPERATIONS CENTER (BDOC)

The BDOC is a command and control facility established by the JFOB commander to serve as the focal point for base defense, force protection and security operations. The BDOC coordinates area security operations with the base cluster operations center (BCOC) (if established), which is responsible for security missions within the base cluster, and oversees and coordinates the efforts of the force protection working group through the JFOB force protection officer. As such, the BDOC should be comprised of many of the same elements found in the JFOB force protection working group. However, depending upon the combination of forces located at each particular base, the combination of representatives will vary. Essential members of the BDOC include representatives from the following units:

- Operations
- Intelligence/Counterintelligence
- Communications
- Maneuver Units
- Fire Support
- Aviation Units

Multi-service units, multinational units, HN, and interagency organizations that are directly involved in JFOB force protection and security should also be represented.

SECURITY FORCE

In conjunction with the physical security measures employed on the perimeter, the first line of defense against hostile acts on a JFOB is the security force. The security force constitutes one of the most important elements of the JFOB's force protection mission. Security forces consist of personnel specifically organized, trained, and equipped to provide security functions for the entire JFOB. 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 JFOB 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 JFOB, the JFOB commander must address several factors critical to the security force:

- Threat for the JFOB
- Size and location of the JFOB
- Geographic characteristics of the JFOB
- JFOB 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 JFOB
- Criticality of assets being protected

In all instances, the security force, regardless of size, should meet the requirement for a reaction force capability.

Since no two JFOBs 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 and, as a minimum, the following:

Security Force Considerations

□ What commander or staff has overall responsibility for the JFOB'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 JFOB?
- ☐ 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 JFOB?
- ☐ Have security force orders/standing operation procedures (SOP) been developed
- ☐ Is there a review process for ensuring currency, 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 JFOB maintain an organized and equipped Quick Reaction Force (QRF)?
- ☐ Does the QRF receive adequate training?
- ☐ Are there sufficient on-board, active duty military 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 nonessential 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?

SECURITY POST REQUIREMENTS AND CONSIDERATIONS

The specific post requirements and operating procedures for the JFOB should be established with the help of JFOB operational and security force personnel.

Security force personnel are normally deployed throughout the JFOB in various operating configurations that include the following:

Entry Control Points (ECP)/Gates. Due to the heavy manpower requirement associated with ECPs/Gates (see Chapter 6), these posts should be limited to the minimum number required to permit expeditious flow of traffic in and out of the JFOB. Operating hours for each ECP/Gate determine manning requirements. Accordingly, JFOBs 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 JFOB, 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 JFOB unpredictable, while making it easier to maintain observation over a large area. However, because of their continuous mobile nature, roving patrols cannot provide continuous observation of a specific area. Consequently, someone attempting to infiltrate a JFOB 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 JFOB 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. Unless the JFOB has the manpower to do so, full-time posts for visitor escorts manned by security force personnel should not be established.

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 JFOB 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 JFOB 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 (e.g., 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 JFOB 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. The following types of equipment may be employed in support of the security mission:

- 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 JFOB commander. The use and possession of privately owned weapons by military personnel in the performance of assigned duties should be strictly prohibited.

- Additionally, machine guns, grenade launchers, etc. can be issued for use if security force personnel have received required weapons training.
- 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 JFOB 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 JFOB and the specific requirements of the security force. See chapter 10 for additional specifications regarding communications requirements.

RESPONSE FORCES

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

- Deterrence. The presence of response forces is a visible, tangible reminder of the response that would meet an intruder who attacks a JFOB.
- 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.
- 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.

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 (i.e., M-16A2s, M203s, M-2s, M60s, M240Gs, M249s, Mk 19s) and equipment (i.e., night vision device (NVDs), spotlights, radios). Response times for QRFs range from 5 to 15 min.

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.

RULES OF ENGAGEMENT (ROE) AND USE OF FORCE

DoD defines 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. 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:

- Actions a soldier may take without consulting a higher authority, unless explicitly forbidden
- 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 U.S. Central Command (USCENTCOM) Commander, 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.

JFOB ROE CONSIDERATIONS

Prior to drafting ROE for JFOB force protection, commanders should first review USCENTCOM, Combined Force Land Component Commander (CFLCC) and any other higher echelon ROE and guidance.

In addition to the security force standing orders, personnel involved in the JFOB 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.

ROE considerations include:

- 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:
  - The need to use force effectively to accomplish the mission objectives
  - The need to avoid unnecessary force.
- 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.

ROE KEY POINTS

- Soldiers 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 with the threat.
- 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, soldiers 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.

ACCESS CONTROL

Access control is primarily designed to restrict persons from areas where they do not belong. An access control system for a restricted area that protects a critical asset, for example HQ buildings, can be designed to facilitate surveillance, control, and segregation of personnel. Depending on the functions to be accomplished, access control points can be designed either to be closed during nonduty hours or to be subject to surveillance and control for all-hours entry.

Depending on the threat, the asset to be protected, and the availability of protection and security forces, access control points can be established as a series of checkpoints. The greater the value of the protected asset, the larger the number of checkpoints that must be passed before access is granted. For a detailed discussion of access control procedures see Chapter 6.

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 DoD O-2000.12-H (DoD Antiterrorism Handbook).

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

RANDOM ANTITERRORISM MEASURES (RAMS)

RAMs change the security atmosphere surrounding a JFOB. When implemented in a truly random fashion, RAMs alter the external appearance or security "signature" of a JFOB so that insurgents conducting surveillance cannot identify force protection patterns. RAMs present the insurgents with an ambiguous security profile for the JFOB. The impact of RAMs is difficult to measure, but

such programs introduce uncertainty for planners and organizers of insurgent attacks.

RAMs provide the JFOB 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 JFOB personnel and force protection/security personnel.
- RAMs reduce adverse operational impacts and unplanned economic costs when enhanced force protection (FP) 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.

PURPOSES OF RAMS

- RAMs can be used as a tool to test which measures have higher costs to a JFOB 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 JFOB 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?”

RAM CONSIDERATIONS

RAMs are part of a proactive and dynamic force protection program. JFOB commanders should consider the following factors when developing and implementing RAMs:

- 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 JFOB 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 JFOB vulnerabilities.
- RAMs should be conducted both internally to the JFOB and externally in coordination with local HN authorities.
- RAMs should be compatible and coordinated with current JFOB surveillance detection and security measures.

MASS NOTIFICATION AND WARNING

Mass notification is the capability to provide real-time information to all JFOB 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.

JFOB IMPLEMENTATION

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 JFOB 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.

TYPES OF MASS NOTIFICATION SYSTEMS

Autonomous Control Unit. An autonomous control unit is used to monitor and control the notification appliance network and provide consoles for local operation. Using a console, personnel can initiate, in a building, the delivery of pre-recorded voice messages, provide live voice messages and instructions, and initiate visual strobe and (optional) textual 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 (optional) is provided on the base, 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.

Notification Appliance Network. A notification appliance network consists of audio speakers located to provide intelligible instructions in and around the building.

- **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 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 intelligible. If a base-wide control system for mass notification (optional) is provided on the base, an interface to the Giant Voice system may improve the functionality of both systems.

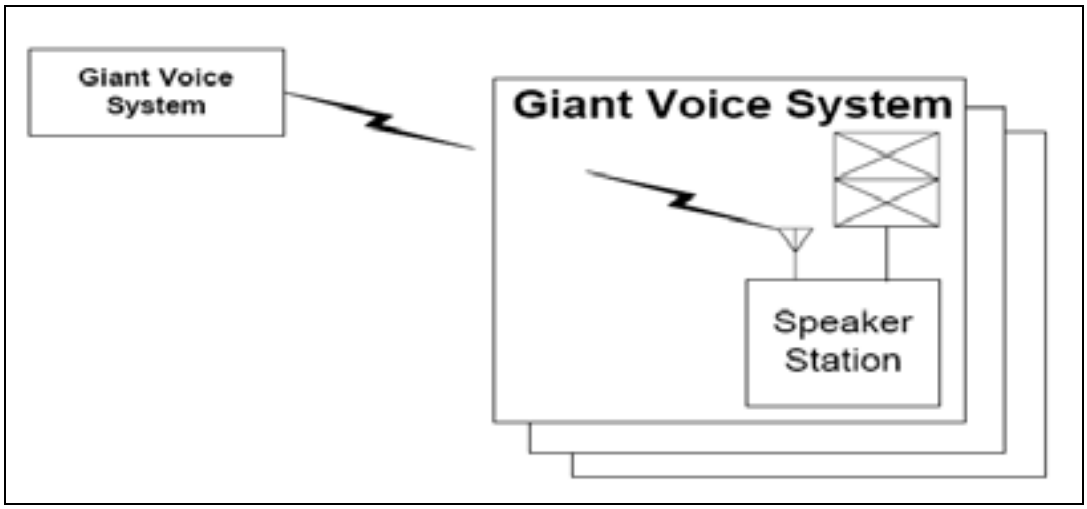


Figure 7-2. Giant Voice System

- **Exterior Based Alert Warning System (AWS)** The following outdoor alert warning system is being examined by DoD and federal agencies. Information on the product was extracted from vendor documents. Commanders are reminded that the list contained herein is not all-inclusive; other systems are available, and surveys should be conducted before the acquisition process is initiated.

Figure 7-3. Outdoor alert warning system

Whelen of Chester, CT, provides 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 ft throughout 360 deg of coverage. Ten different models ranging in size from a one-cell speaker to a ten-cell speaker configuration allow the user to customize his personnel alerting solution to the requirements of the command. Included as part of the electronic siren package are six standard warning tones (i.e., wail, alert, hi/lo, attack, air horn, and whoop), a pre-recorded message capability, (capable of storing up to 16 pre-recorded digital voice messages) and a real time public address voice capability.

Regardless of speaker configuration, the Whelen system is capable of operation at full output on battery power for 30 min without any alternating current (AC) power connection. It can accept solar panels and wind generators in order to charge the battery back-up system (i.e., does not rely on AC power for battery back-up charging), and performs a silent diagnostic self-test which can be reported back to the command and control location.

Command and control of an installation's electronic siren package is accomplished through an encoder/decoder keyboard capable of being programmed to select a single siren, a group of sirens, or all sirens for immediate activation upon depressing any one of 60 programmable "hot keys." Additional command and control features include a ten-digit Dual Tone Multi-Frequency protocol code to provide security from false activation. Sirens may be activated through either RF or hardwire means.

A site survey is required in order to determine the cost for equipping a site with the 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.

REFERENCES

DoD O-2000.12-H. *DoD Antiterrorism Handbook*, February 2004.

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

Marine Corps Order P5530.14. *Marine Corps Physical Security Program Manual*, 21 December 2000.

Physical Security Equipment Action Group (PSEAG) Security Equipment and Resources Guide, April 2001.

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

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003.

UFC 4-012-01 (Draft). *Security Engineering: Entry Control Facilities/ Access Control Points*.

U.S. Air Force Entry Control Facilities Design Guide, 18 February 2003.

Chapter 8

PROTECTIVE CONSTRUCTION

Contents

INTRODUCTION

One of the elements in an integrated, layered, defense-in-depth plan for the JFOB is the use of structures that are designed to protect personnel and other assets from the effects of threat weapons (in this case, vehicle-borne improvised explosive devices (VBIEDs) and rockets. artillery, and mortars (RAMs)). This chapter groups these structures as follows:

- ***Sidewall Protection and Revetments***. Walls or barriers designed to stop fragments and reduce blast effects from near-miss impacts of RAM rounds. Revetments are used to provide full-height sidewall protection and to form a wall around open stores of critical equipment or material assets. Some revetment designs can also function as vehicle barriers (see Chapter 6).
- ***Compartmentalization***. A series of interconnected walls designed to divide large areas of high occupancy into smaller protected areas so as to limit casualties from impacts of RAM rounds.
- ***Overhead Cover***. A structure designed to provide protection from the direct impact of incoming RAMs. The concept consists of a pre-detonation layer that activates the incoming round's fuse, causing it to detonate, and a shielding layer that stops the fragments and reduces the blast effects.
- ***Personnel and Equipment Bunkers***. Purpose-built structures designed to withstand both near miss and direct hits of RAMs

- ***Hardened Fighting and Observation Positions***. Similar to personnel and equipment bunkers except they have apertures for returning or initiating fire.
- ***Use of Existing Structures***. Depending on construction type and standoff, existing structures can provide protection against VBIEDS and RAMs. If required, there are retrofit construction techniques for increasing protection.

Protection from VBIEDs and RAMs should be considered during the JFOB planning/layout stage rather than trying to include it after the JFOB is occupied. However, this may not be practical due to constraints on available resources (lack of time, manpower, materials, equipment, funds, etc.)

If the desired level of protection from VBIEDs and RAMs cannot be provided during the expeditionary and initial stage of the JFOB, at a minimum, a plan should be established for implementing and increasing levels of protection as the JFOB evolves. To the extent plausible, locations in which personnel routinely work eat, or sleep 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 JFOB. The axiom, continue to improve the position for as long as it is occupied, remains valid. The following priority of effort should be considered:

□ Provide perimeter fighting positions. Provide personnel bunkers at various locations throughout the JFOB for temporary protection if given sufficient warning.
□ Where available use existing buildings for protection from VBIEDs and near-miss RAMs after ensuring:
  - Sufficient standoff to perimeter is available.
  - Windows are removed and/or openings boarded over.
  - Walls are a minimum of 8-in.-thick concrete masonry units (providing a low level of protection from fragments).
□ Provide full height sidewall protection for all billeting, high occupancy and other critical facilities, such as the dining facility (DFAC) and Base Defense Operations Center (BDOC).
□ Compartmentalize large area, high occupancy facilities (such as DFACs).
□ Provide overhead cover incorporating pre-detonation and shielding layers for billeting areas, high-occupancy and other critical facilities.
□ Provide bunkers and revetments for protection of critical equipment.

SIDEWALL PROTECTION AND REVETMENTS

Revetments are simply walls designed to provide protection from the blast and fragment effects from near-miss RAMs. 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. The primary uses of revetments on the JFOB are

- As walls and vehicle barriers along the JFOB perimeter and at entry control points (ECPs).

- As a means of providing full-height sidewall protection for soft-sided structures such as tents and trailers (see Figure 8-1)
- As free-standing walls to protect mission-critical equipment (weapons storage, helicopters, fuel bladders, etc.)

Figure 8-1. Example of providing full-height sidewall protection

SANDBAGS

Description: Sandbagging is 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 freestanding 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.

Pertinent Data:

1 bag (4 in. × 8 in. × 16 in.) = 0.3 cu ft (0.011 cu yd) of sand

100 bags = 1.1 cu yd of sand

12 bags = A wall 1 ft high by 4 ft long

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.

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 8-2. 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.

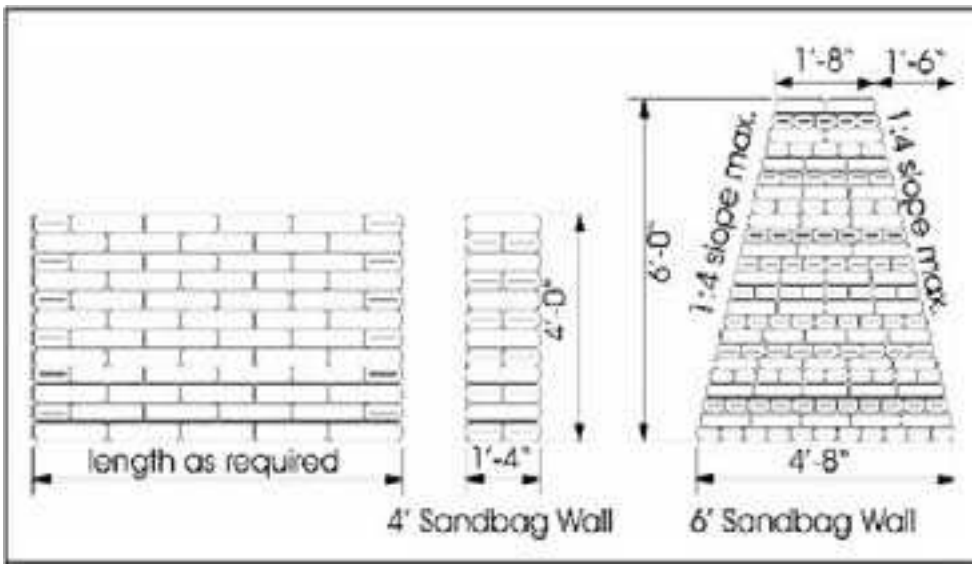


Figure 8-2. Freestanding sandbag revetment details

Performance against Weapons Effects: Numerous tests have shown that a minimum of two layers (app. 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.

HESCO BASTION CONCERTAINER® REVETMENT

Description: Hesco Bastion Concertainer® is the brand name for a commonly used revetment used in Iraq and referred to as "Hesco." The Hesco wall sections consist of a series of large, linked, self supporting cells. 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. To deploy, the wall sections are expanded, positioned, and filled. The wall sections can be connected to form longer walls, separated to form shorter sections, or stacked to increase wall height.

Pertinent Data: Hescos come in nine sizes and two colors, all of which have NSNs (see Table 8-1).

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. Fabric material used as a liner is UV sensitive and will degrade over time. Also, note that Hesco "look-alikes" have been encountered in Iraq and often provide limited performance and accelerated degradation.

Table 8-1. Hesco Sizes

Unit	Height ft (m)	Width ft (m)	Length ft (m)	NSN 5680-99-xxx-xxxx
Mil 1	4.5 (1.37)	3.5 (1.06)	32 (10)	835-7866 (Beige), 001-9396 (Green)
Mil 2	2 (0.61)	2 (0.61)	4 (1.21)	968-1764 (Beige), 001-9397 (Green)
Mil 3	3.25 (1.0)	3.25 (1.0)	32 (10)	001-9392 (Beige), 001-9398 (Green)
Mil 4	3.25 (1.0)	5 (1.5)	32 (10)	001-9393 (Beige), 001-9399 (Green)
Mil 5	2 (0.61)	2 (0.61)	10 (3.05)	001-9394 (Beige), 001-9400 (Green)
Mil 7	7.25 (2.21)	7 (2.13)	90 (27.7)	169-0183 (Beige), 126-3716 (Green)
Mil 8	4.5 (1.37)	4 (1.22)	32 (10)	335-4902 (Beige), 517-3281 (Green)
Mil 9	3.25 (1.0)	2.5 (0.76)	30 (9.14)	563-5649 (Beige), 052-0506 (Green)
Mil 10	7 (2.12)	5 (1.5)	95 (30.5)	391-0852 (Beige), 770-0326 (Green)

The types of Hescos most commonly used in Iraq are the MIL 1 and MIL 2 (see Figures 8-3 and 8-4).

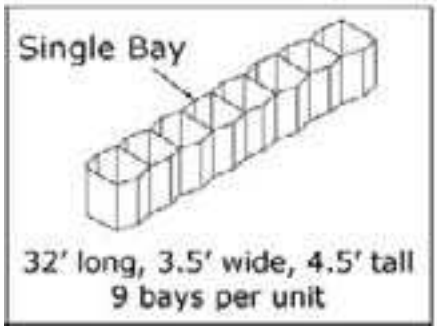


Figure 8-3. MIL 1 type Hesco

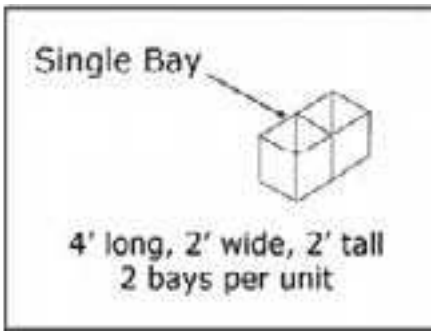


Figure 8-4. Mil 2 type Hesco

Construction Procedure: Each shipment of Hescos comes with detailed guidance for construction. It is important to follow these instructions as closely as possible to ensure that what you build is stable, long-lasting and requires minimal maintenance.

Important Construction Points to Remember:

- ***Site Considerations***: Choose or provide a level surface with a sub grade of sufficient strength and drainage to support the structure. Otherwise, the Hesco may tip over and will have to be rebuilt.
- ***Layout:*** Units come flat-packed. Be sure to place them in the desired location and orientation BEFORE expanding them in the desired direction.
- ***Selection And Placement Of Fill Material:*** 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. CRITICAL – Expand bottom cell 2 in. to 4 in. during placement of first lift. CRITICAL – Insert joining pins before placing fill material.

Use of Hescos for Full-Height Sidewall Protection: The following two methods (see Figures 8-5 and 8-6) can be used to construct full height walls around tents and trailers to provide protection from fragment and blast effects from near miss mortar and rocket rounds.

Figure 8-5. Mil 2 Hesco Bastion soil-filled wall

Wall Dimensions: 2 ft thick × 6 ft tall.

Materials Required: Three Mil 2 units per 4 linear feet of wall plus two additional units for each stiffener. Cost per linear foot is estimated at $45 for the Hescos (excluding labor and fill material).

Figure 8-6. Mil 1/Mil 2 Hesco Bastion soil-filled wall

Additional Comments: To prevent the wall from toppling from close-in detonations, laterally brace the 6 ft tall wall with intersecting walls or integrally built stiffeners. Provide lateral bracing at not more than 12 ft on center.

Wall dimensions: 3.5 ft thick at bottom (2 ft thick at top) × 6.5 ft tall.

Materials Required: One Mil 1 unit and eight Mil 2 units per 32 linear feet of wall. Cost per linear foot is estimated at $39 for the Hescos (excluding labor and fill material).

Additional Comments: Unlike the Mil 2 perimeter wall, no additional wall stiffeners are required to prevent toppling from close-in detonations. This stability is due to the thicker wall base created by the Mil 1 units.

Performance against Weapons Effects: Numerous tests have shown the 2 ft thickness is adequate to stop all fragments from 60 mm Mortar through 122 mm rocket and 155 mm artillery rounds.

Use of Hescos for Anti-Vehicular Barriers: When utilized as an anti-vehicular barrier, the Concertainer® material is normally built with a base two rows wide and at least a second level in order to provide sufficient mass to stop a vehicle (see Figure 8-7 below that uses the Mil 1 size). Tests by the USAF Battle Lab showed that this design effectively stopped a 15,000 lb truck traveling at 30 mph.

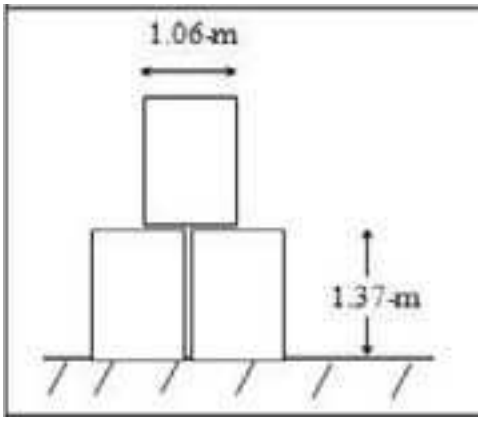


Figure 8-7. Hesco configuration for anti-vehicular barrier

Anti-vehicular barriers can be constructed to mitigate larger threats using a variety of Hesco containers e.g., the 7 ft 3 in. high × 7 ft wide, when constructed as indicated above, will provide a significant barrier.

CORRUGATED METAL BIN REVETMENTS

Description: Metal revetments (See Figure 8-8) can be utilized for supplemental sidewall protection or in the construction of protective positions. Revetments 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 four (4) panel types (side, end, cross, and brace), connecting pins, flaring tools, and corner containment materials (wire mesh and poly film). Corrugated metal bin revetments come in kits of the following sizes:

- 2'x 6'x 104' (NSN:TBP) Estimated fill material required: 47 cubic yards
- 4'x 8'x 64' (NSN:TBP) Estimated fill material required: 76 cubic yards
- 4'x 10'x 48' (NSN:TBP) Estimated fill material required: 72 cubic yards

Wall sections come either 2 ft or 3 ft high. The 2 ft high sections are composed of 16-guage material while the 3 ft high sections are 18-gauge.

Use for Full-Height Sidewall Protection: These 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) has developed a smaller version of this kit for use in JFOBs that will provide protection from blast loadings and shielding from primary fragments from RAMs.

Figure 8-8. Examples of corrugated metal bin revetments

Pertinent Data: Typical revetment unit dimensions: 2 ft thick × 3 ft tall, lengths are cut to meet user requirements (common length is 8 ft). A national stock number (NSN) for this system is being established. The minimum recommended configuration for protection of tents and trailers is a 6 ft high, 2 ft thick wall filled with soil. Figure 8-9 shows the concept for protection of a tent. Note the use of free-standing sections to shield the entrances. A significant advantage of the corrugated metal wall is enhanced resistance to environmental degradation (UV, wind erosion, etc.) as compared to Hesco Bastion.

Figure 8-9. Metal bin revetment used for sidewall protection

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 improved surface (concrete paving, asphalt paving, stabilized soil, etc.), the foundation area must be properly prepared. See the "Metal Revetment Assembly Construction Guide" listed in the references for detailed guidance on foundation and site preparation.

Construction Procedure: See the "Metal Revetment Assembly Construction Guide" for detailed guidance on assembling individual metal bins.

Materials Required: Two revetment units (at 3 ft tall each) are required for a 6-ft-tall-wall.

Cost: Cost per linear foot for a 2 ft thick, 6 ft tall wall is estimated at $88 for the metal bin material (excluding labor and fill material).

Additional Comments: 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 as shown in Figure 8-10. You can also use other materials possessing adequate strength, such as 4×4 timbers. To prevent wall toppling in either direction, apply bracing on both sides of the wall.

Performance against Weapons Effects: Numerous tests have shown the 2-ft thickness is adequate to stop all fragments from near-miss 60 mm mortars through 122 mm rockets.

Use for Rocket Propelled Grenade (RPG) Protection: 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. Figures 8-11 and 8-12 show a revetment subject to RPG-7 attack with and without a "pre-detonation" screen. Since details on the defeat measures for these weapons are classified, contact ERDC for information on the types of material and construction that can be used for a screen and the required standoff distances to prevent perforation.

Use as Anti-Vehicular Barriers: Like Hescos, metal bin revetments can also be used to construct anti-vehicular barriers. They should be constructed of a size equal to or larger than that shown in Figure 8-7 for the Hesco to ensure sufficient mass.

Figure 8-10. Bracing of walls for near miss 122mm rocket threat

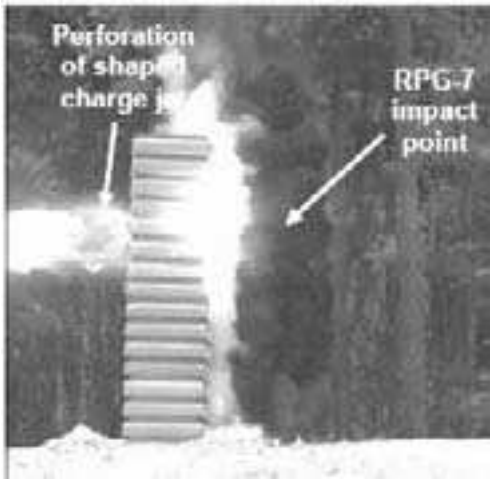
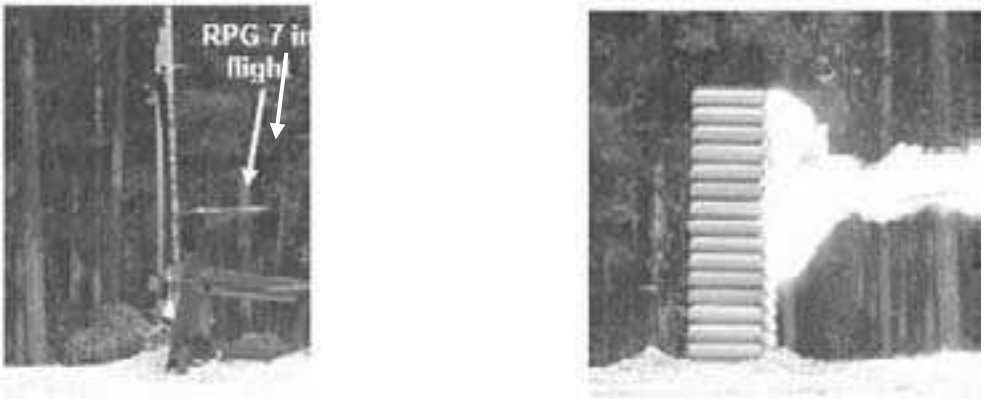


Figure 8-11. High speed photo of RPG-7 detonating and perforating metal revetment.



a. Just prior to impact on pre-detonation screen b. Revetment prevents perforation

Figure 8-12. Protection from RPG-7 using pre-detonation screen in front of metal revetment.

MODULAR REINFORCED CONCRETE WALLS

Use for Full-Height Sidewall Protection: Prefabricated, reinforced concrete barrier walls 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 also known as Texas barriers, Alaska barriers, Bitburg barriers, or T-walls and are fabricated in a wide variety of sizes and configurations (Figure 8-13). The minimum recommended height for these walls is 6 feet but taller units may be needed for trailers with crawl spaces.

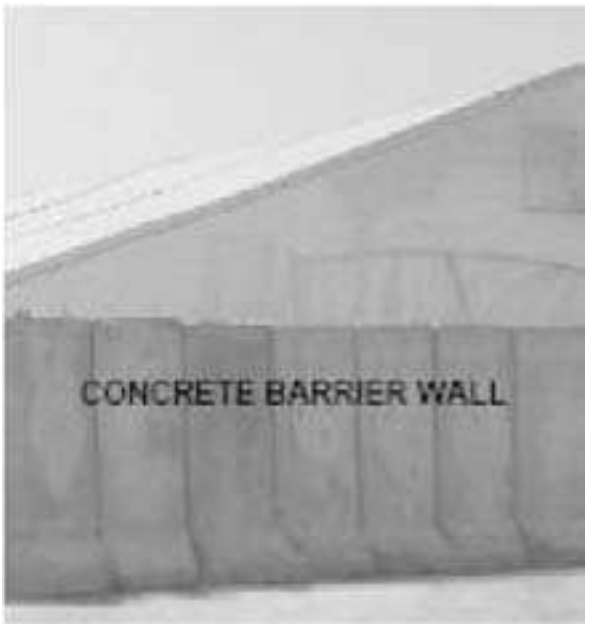


Figure 8-13. Use of concrete revetment
for full-height sidewall protection

Pertinent Data: Minimum recommended thickness: 6 in with a minimum concrete compressive strength of 4500 psi. For lower strength concrete thicker walls (e.g., 8 in. to 12 in. thick) should be used (Figure 8-14).

Limitations: A level, stable foundation is required. Fragments can penetrate gaps between wall sections. Close-in detonations of large mortars and rockets may breach the wall.

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 8-15).

Performance against Weapons Effects: At 4500 psi and 6 in. thickness, concrete walls will stop all fragments from 60 mm mortar through 122 mm rocket at standoffs 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 (e.g., 16 gage) can be used to reduce spall and increase fragment penetration resistance.

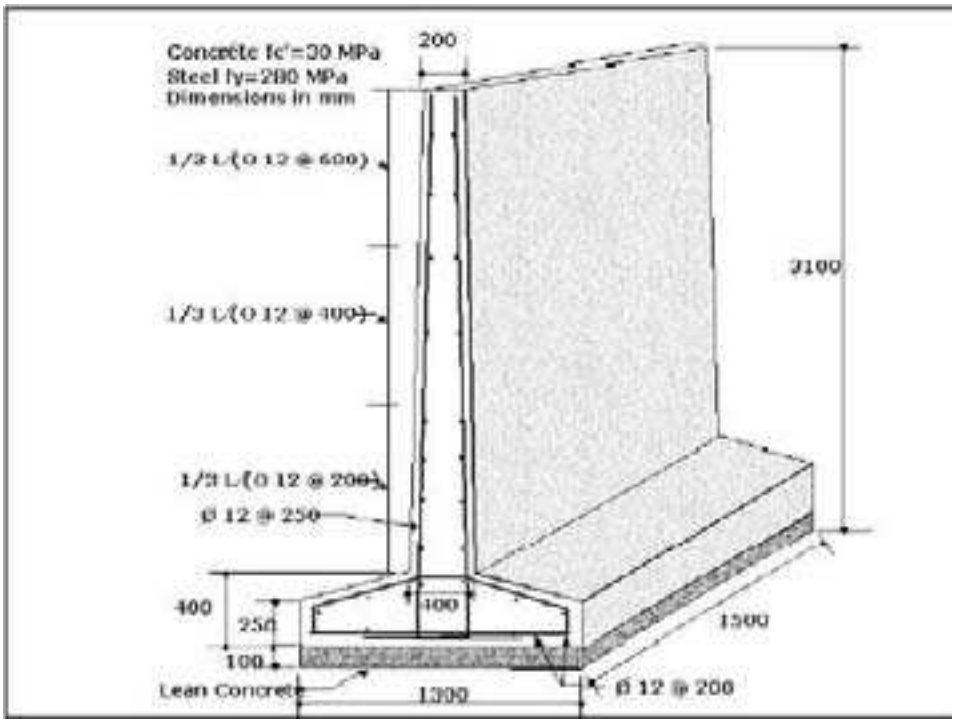


Figure 8-14. Example of a Large Concrete Revetment

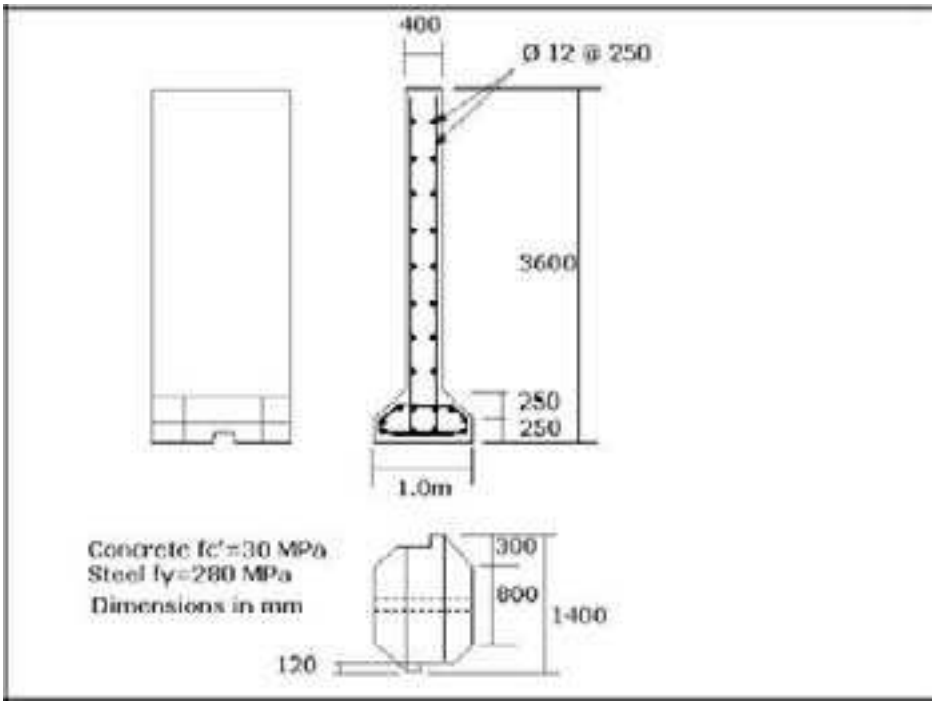


Figure 8 – 15. Example of Overlapping Concrete Revetment with Chamfered Footings.

Other Uses: Prefabricated reinforced concrete barrier walls can also be used for:

- Physical anti-personnel barriers and obscuration along the JFOB perimeter (see Chapter 6)
- Anti-Vehicular Barriers (see Chapter 6)
- As part of the ECP to channel traffic, mitigate blast/fragmentation and protect personnel (see Chapter 6)

E-GLASS AND U-PICKET WALLS

Description: One option that does not rely on the use of soil for fragment protection is the use of multi-layered (6-layer) wall panels of ballistic grade e-glass (NSN 9340-01-533-5758) supported by metal fence posts (NSN 5660-00-270-1587 or similar). This protection technique can be used outside or inside tents but is limited in height (Figure 8-16).

Limitations: Only 4 vertical feet of fragment protection is provided. In testing, detonation of the 120-mm mortar 13 feet away from these walls produced no fragment penetrations of the 6-layer e-glass walls. Some movement/rotation of the walls occurred due to the blast. For larger weapons such as the 122-mm rocket, it is not known whether sufficient support is provided to prevent overturning of walls.

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 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 (reference construction drawings for details).

Acquisition Information*:* Ballistic grade E-glass NSN: 9340-01-533-5758, 72-inch steel fence post NSN: 5660-00-270-1587.

Required/recommended equipment: Fence post driver and drill or wrench to install fasteners. Miscellaneous fasteners – ¼" diameter minimum.

Cost: Approximately $275 per linear foot of 4 ft tall protection (excluding labor).

Space: Nominal 6 in wide footprint at the base. Deflections/rotations on the order of 2 to 3 feet of may be encountered in high blast environments.

Performance against Weapons Effects: Fragment penetrations occurred in 3-layer and 5-layer e-glass walls when a 122 mm rocket was detonated at approximately 10 ft from the walls. The walls stopped approximately 95 percent of the fragments. In tests with 120 mm mortar rounds, a 3-layer e-glass wall stopped approximately 95 percent of the fragments at a standoff of 10 ft

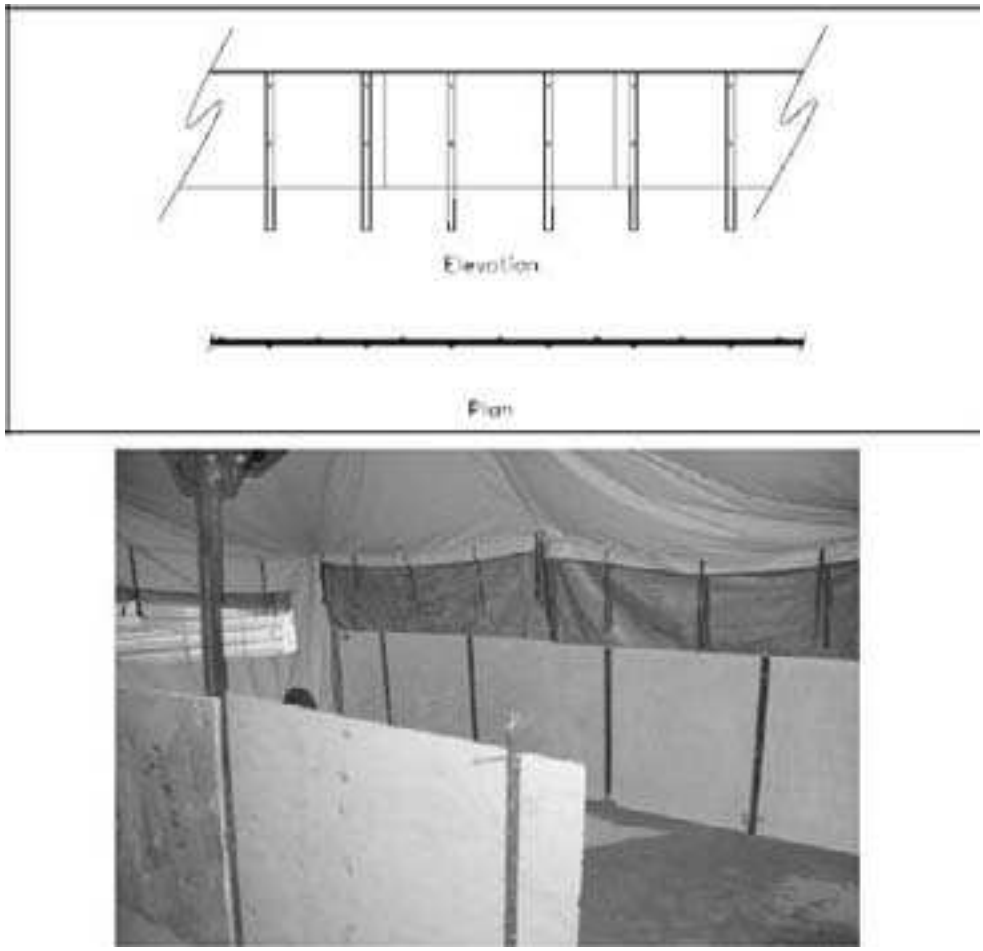


Figure 8-16. Use of E-glass and U-pickets for low-height protection.

OTHER MATERIALS

Other materials that can be used to stop fragments are given in Table 8-2 (based on tests conducted by ERDC).

HELICOPTER REVETMENTS

Revetments can also be used to protect open stores of material and equipment (See Figure 8-17.) Tables 8-3 – 8-5 and Figures 8-18 – 8-21 provide information on using Hesco revetments for making protective enclosures to compartmentalize and protect helicopters from near-miss of RAMs. These designs were developed by the ERDC and the Directorate of Training, U.S. Army Engineer School. Although not shown, Corrugated Metal Bin Revetments of similar sizes can be substituted for the Hesco material if desired.

CONSTRUCTION GUIDE FOR PROTECTION OF ROTARY WING AVIATION ASSETS:

EQUIPMENT, PERSONNEL AND TIME ESTIMATE

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.

Table 8-2. Material Options for Fragment Protection

Material	Thickness	Standoff Distance	Stops Fragments from:		
			82 mm mortar	*120 mm mortar*	*122 mm rocket*
Concrete Wall (4500 psi)	3-3/4" with 16 gauge steel liner[1]	10'	YES*	YES	YES
"	4-1/4"	10'		NO	NO
"	5-1/2" with 16 gauge steel liner[1]	10'	YES*	YES	YES
"	6"	10'	YES*	YES	YES
CMU Wall	8"	15'	YES	NO	NO
	8" with grout-filled cells	10'	YES*		YES
"	8" with 22 gauge steel liner	15'	YES	NO	YES
"	8" with UL Level 3 fiberglass panel (7/16")	15'	YES	YES	YES
Steel Plate (A36)	1/8"	15'	NO	NO**	NO**
"	1/4"	15'	YES	NO**	NO**
"	3/8"	15'	YES	NO**	NO**
"	1/2"	15'	YES	NO	NO
"	5/8"	15'	YES*	YES	NO
"	3/4"	15'	YES*	YES	NO
"	1"	15'	YES*	YES	YES

Results of static arena tests -YES means material stopped all fragments. NO means at least one fragment penetrated. YES* means material will stop fragments based on extrapolation from the other test results. NO** means material will not stop fragments based on extrapolation from the other test results. A blank indicates no test was performed and results could not be extrapolated.

Note 1: Spall liner was mechanically clamped at top & bottom of panel during test. Additionally, a 3/8" dia. horizontal bead of adhesive 6" O.C was used.

Figure 8-17. Hesco revetment design for helicopter protection

Table 8-3. Bill of Materials for various helicopter applications

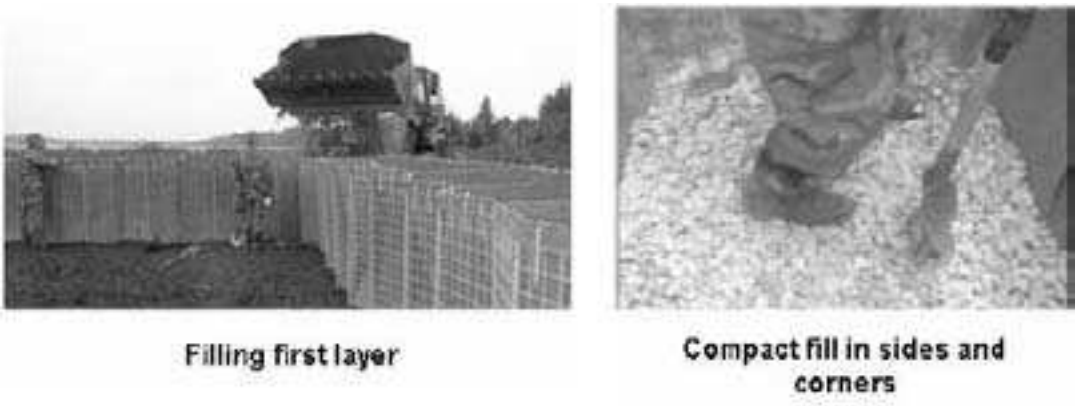
Item Description	NSN	Apache/ Blackhawk	Kiowa Warrior	Cobra	UH-1 Huey
Concertainer®– 4.5 ft high, 3.5 ft wide, 32 ft lg	5680-99-001-9396 – Green 5680-99-835-7866 – Beige/Sand	16	11	14	14
Concertainer® Infill Material, cubic yards	Not applicable	340	230	300	290

Item Description	NSN	Chinook	Super Stallion
Concertainer®– 4.5 ft high, 3.5 ft wide, 32 ft long	5680-99-001-9396 – Green 5680-99-835-7866 – Beige/Sand	11	11
Concertainer®– 7.25 ft high, 7 ft wide, 91 ft long	5680-99-126-3716 – Green 5680-99-169-0183 – Beige/Sand	4	4
Concertainer® Infill Material, cubic yards	Not applicable	1000	1000

Table 8-4. Typical HESCO Revetment Resource Requirements

Aircraft	Task	Equipment Req'd.	Soldiers Req'd. (excluding operators)	Time Req'd.
Apache/ Blackhawk	Site preparation, foundation leveling	bulldozer, DEUCE, ACE	2	45 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader, HMEE	8	8 hr
Kiowa Warrior	Site preparation and foundation leveling	bulldozer, DEUCE, ACE	2	30 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader, HMEE	6	8 hr
Cobra	Site preparation and foundation leveling	bulldozer, DEUCE, ACE	2	45 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader, HMEE	8	7 hr
Huey	Site preparation and foundation leveling	bulldozer, DEUCE, ACE	2	45 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader, HMEE	8	7 hr
Chinook	Site preparation and foundation leveling	bulldozer, DEUCE, ACE	2	1 hr 30 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader w/ clamshell bucket, HYEX	10	16 hr
Super Stallion	Site preparation and foundation leveling	bulldozer, DEUCE, ACE	2	1 hr 30 min
	Haul infill material to site	dump trucks	varies	varies
	Erect walls and place infill	front-end loader w/ clamshell bucket, HYEX	10	16 hr

STEP 1 - FIRST LAYER



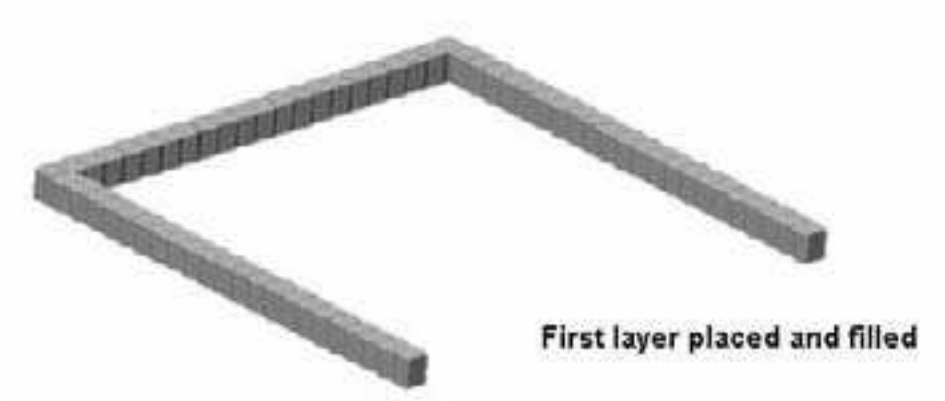


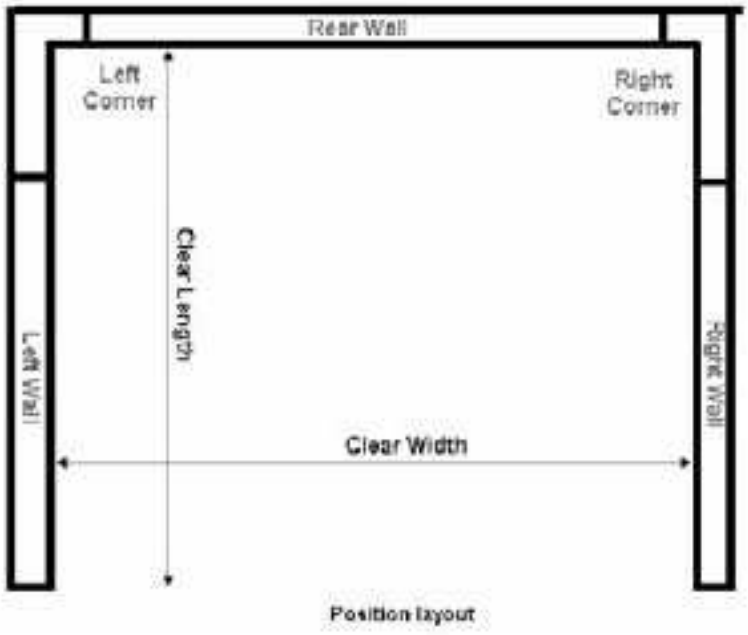
Figure 8-18. First step in revetment construction for helicopters

Note that for each position a minimum clear width and length is indicated (see Figure 8-19 and Table 8-5). These represent the dimensions that are necessary to provide a minimum clearance of 10 ft to 14 ft between the walls and the rotors of the aircraft. Prior to placing any fill, all Concertainer® units should be placed and the clear dimensions should be checked. Only after the dimensions are verified should filling proceed.

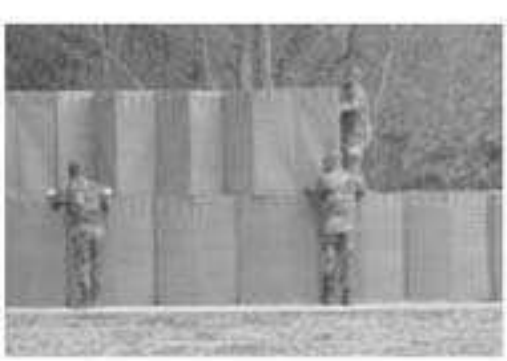
Materials required: 8 sections of Concertainer®– 4.5 ft high × 3.5 ft wide × 32 ft long.

- □ Rear wall – form with 2 full sections
- □ Left corner – form by the "single unit" method; utilize the 3rd and 4th bays from the end of the section to form the corner. Place the section such that the 1st and 2nd bays are attached to the rear wall and the 5th-9th bays are attached to the left wall.
- □ Right corner – form the same as the left corner
- □ Left wall – form with 2 full sections
- □ Right wall – form with 2 full sections
- □ Minimum clear width = 78 ft
- □ Minimum clear length = 82 ft

FIRST LAYER – APACHE & BLACKHAWK



Step 2 - Second Layer



Placing second layer

Connecting second layer to first using plastic wire ties

Figure 8-19. Construction of second layer for Apache and Blackhawk revetment

STEP 2 - SECOND LAYER

With the exception of the Chinook and Super Stallion revetments, the second layer will be constructed with the same type of Concertainer® used in the first. In these cases connect the second layer to the first with the included plastic wire ties as shown above. This will not be possible for the Chinook and Super Stallion revetments.

If necessary, cap the top of the wall to reduce the potential for Foreign Object Damage resulting from rotor wash. You can use several methods to cap the wall, including sandbags or chemical stabilizers. If you use a cap, take care to ensure that the cap itself will remain stationary when exposed to rotor wash.

SECOND LAYER – APACHE & BLACKHAWK

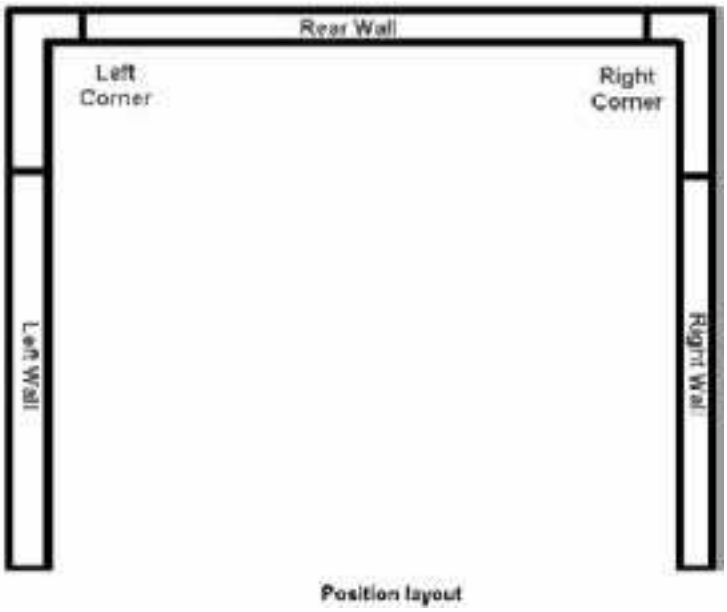


Figure 8-20. Layout of second layer for Apache and Blackhawk revetment

Materials required: 8 sections of Concertainer®– 4.5 ft high × 3.5 ft wide × 32 ft long.

- ☐ Rear wall – form with 2 full sections
- ☐ Left corner – form by the "single unit" method; Utilize the 3rd and 4th bays from the end of the section to form the corner. Place the section such that the 1st and 2nd bays are attached to the rear wall and the 5th-9th bays are attached to the left wall.
- ☐ Right corner – form the same as the left corner
- ☐ Left wall – form with 2 full sections
- ☐ Right wall – form with 2 full sections

STEP 3 - REVETMENT CHECKLIST

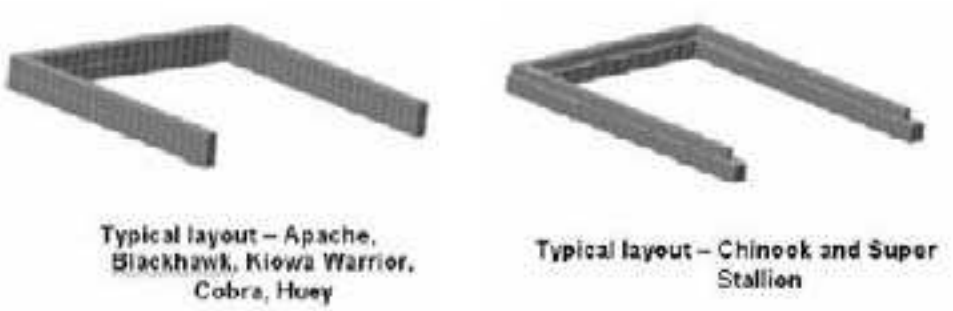


Figure 8-21. Typical revetment configurations for Army helicopters

Check completed revetment to ensure:

- ☐ Walls are straight.
- ☐ There is no excessive settlement of walls.

□ Adequate clear distance is provided between aircraft and walls.

□ Wall caps, if applied, are adequately secured.

Table 8-5. Layout dimensions for various types of helicopters

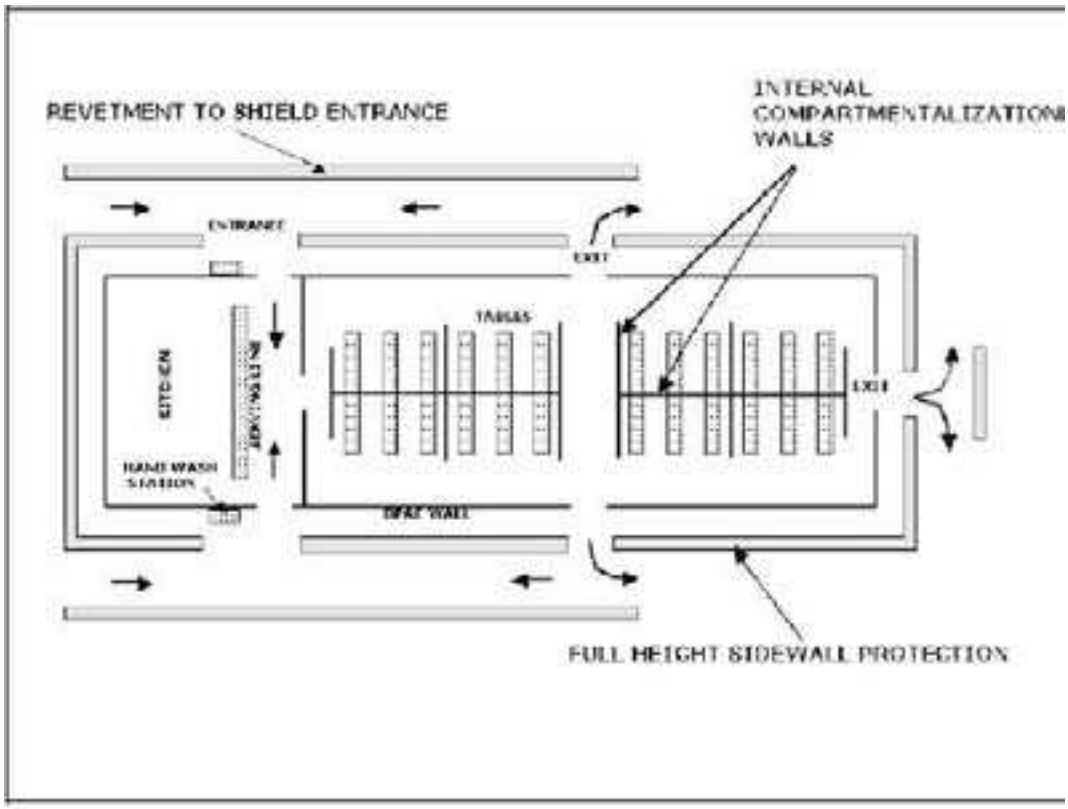
Helicopter	Concertainer®	Quantity	Length (ft)	Width (ft)
Blackhawk/Apache	4.5 x 3.5 x 32'	16	82	78
Kiowa	4.5 x 3.5 x 32'	11	53	57
Cobra	4.5 x 3.5 x 32'	14	78	64
Huey	4.5 x 3.5 x 32'	14	67	71
Chinook	7.25 x 7 x 91'	4	126	91
2nd layer	4.5 x 3.5 x 32'	11	-	-
Super Stallion	7.25 x 7 x 91'	4	112	112
2nd layer	4.5 x 3.5 x 32'	11	-	-

COMPARTMENTALIZATION

Compartmentalization is a technique to reduce casualties in high population-density areas such as dining facilities, recreation facilities, etc. 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 soldiers into smaller compartments as shown in Figure 8-22. 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 that which 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 the weapons of concern in Iraq (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 described below.

PLASTIC BIN SOIL REVETMENT WALL

Description: 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 with male/female templates to allow for interlocking construction. Threaded caps at the bottom provide a way to empty contents when necessary. Figure 8-23 shows an application and Figure 8-24 is a concept drawing of the plastic soil bin wall.



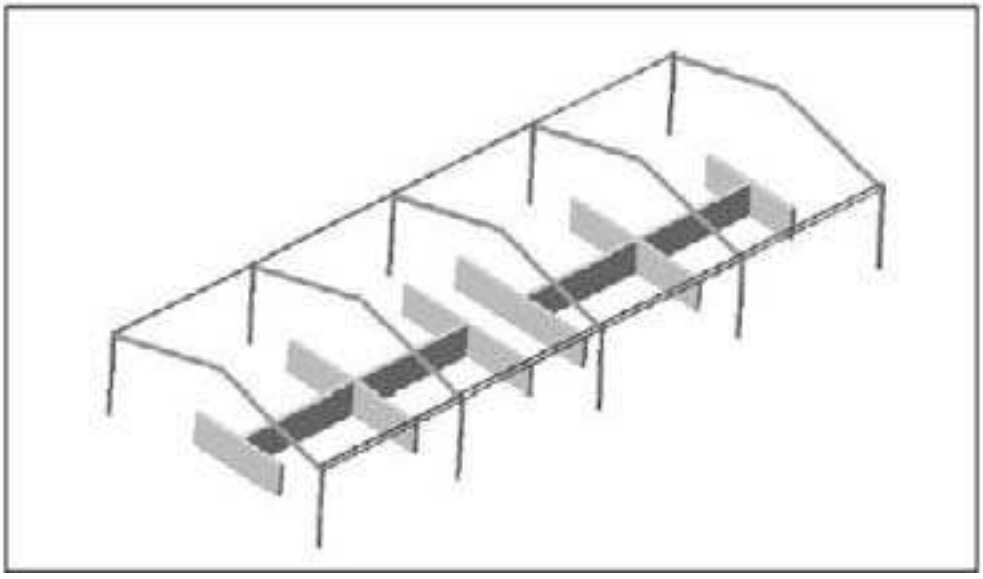


Figure 8-22. Examples of compartmenting a typical dining facility

Figure 8-23. Application of Plastic Soil Bin Revetment in DFAC

Limitations: The wall panel male/female 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 4×4 connections and void portions of the male keys were able to pass through. Two solutions to strengthen the joints against fragment penetration are provided in the instructions for fabricating these walls.

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/lft. Two men can easily hand 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 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.

Acquisition Information: Commercial off-the-shelf material, available from Creative Building Products.

Required/recommended equipment: Plywood funnel to assist in filling soil bins, small soil moving equipment such as a Bobcat to transport and dump soil into the soil bin. If space is tight, the soil bins can be filled by hand using buckets. Each bin holds about 1 cu yd of soil.

Labor: Empty plastic bins can be moved and assembled by two men.

Cost: Approximately $600 per unit having nominal dimensions of 10 in. thick by 5 ft high by 8 ft long.

Weapon effects performance: The 10 in. soil fill and plastic barrier material will stop all fragments from 60 mm mortar through 122 mm rockets detonating 10 ft from the soil bin.

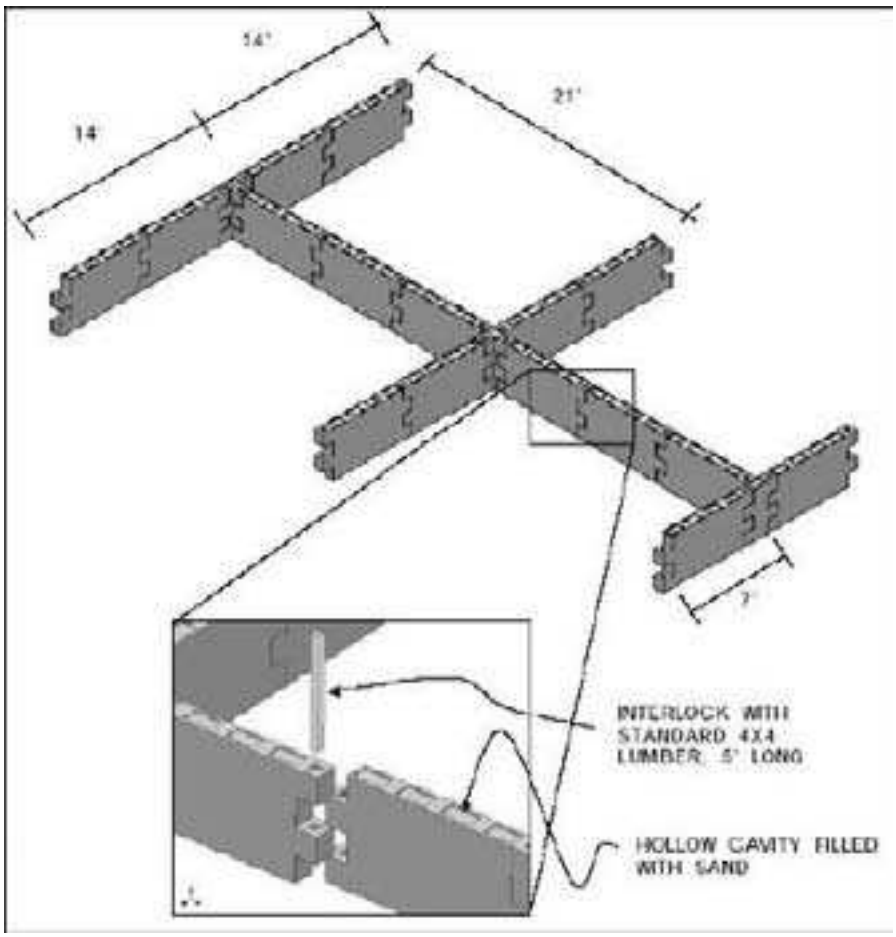


Figure 8-24. Concept drawing of a plastic soil bin wall

WOODEN PARTITION WALL

Description: The wooden partition wall is constructed of 3/4 in. plywood over 2 in. × 8 in. × 57 in.-long studs with 2 in. × 4 in. whaling along the outside. The 7-1/2-in. cavity that is formed is filled with soil and capped with 2 in. × 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.

Limitations: During testing two fragments from a 120 mm mortar penetrated the 2-in. × 8-in. spacers separating the plywood panels, and during the 122 mm rocket test several fragments passed through the wooden cap at the top of the wall due to the reduced ballistic performance of wood. A mini loader is needed to place soil in the small opening at the top of the wall.

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 325 to 400 lb/lft. Install intersecting walls about every 20 ft to provide stability. In addition, anchor the wall to the floor at its ends and midpoints. Anchoring designs are included in the detailed drawings.

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.

Acquisition Information: The walls are constructed from normal Class IV construction materials.

Required/recommended equipment: Plywood funnel to assist in filling soil bins, small soil-moving equipment such as a Bobcat to transport and dump soil into the soil bin. If space is tight, the soil bins can be filled by hand using buckets. Each linear foot of the wooden soil bin holds about 3 cu ft of soil.

Labor: Carpenters to construct the soil bins and labor to fill.

Weapon effects performance: The 7 ½ 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.

E-GLASS WALLS

Description: Multi-layered (3-layer and 5-layer) wall panels of ballistic grade e-glass (NSN 9340-01-533-5758) supported by custom manufactured steel stands See Figure 8-25.)

Limitations: In tests using 120 mm mortars and 122 mm rockets, many fragments penetrated the 3-layer e-glass walls. 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.

Construction Procedure: Walls are constructed with 4 ft wide by 5 ft tall panels that are supported at each edge in steel stands. The steel stands are attached to the foundation with ¾ in. diameter anchors.

Acquisition Information: Ballistic grade E-glass NSN: 9340-01-533-5758.

Required/recommended equipment: Drill, hand tools, welding equipment to fabricate stands.

Cost: Approximately $325 per linear foot of 5 ft tall, 5-layer thick protection (excluding labor).

Space: Nominal 12 inch wide footprint at the base. Deflections/rotations on the order of 2 to 3 feet of may be encountered in high blast environments depending upon the type of flooring being anchored to (concrete vs. wood).

Weapon effects performance: Fragment penetrations occurred in 3-layer and 5-layer e-glass walls when a 122 mm rocket was detonated at approximately 10 ft from the walls. The walls stopped approximately 95 percent of the fragments. In tests with 120 mm mortar rounds, a 3-layer e-glass wall stopped approximately 95 percent of the fragments at a standoff of 10 ft.

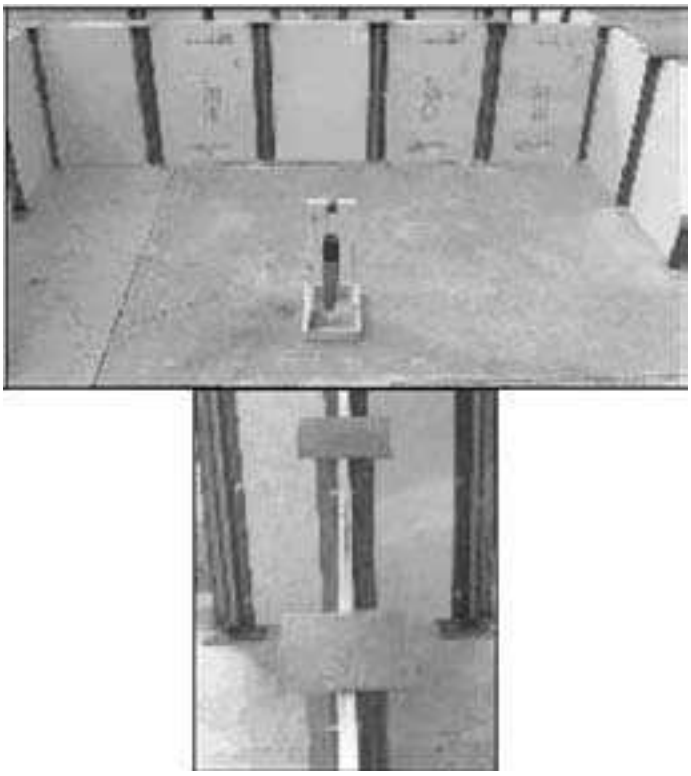


Figure 8-25. Use of E-glass and steel stands for compartmentalization

HESCO BASTION WALLS

Description: Hesco Bastion soil-filled revetments can also be use for compartmentalization. See the section on Revetments for more information. Figure 8-26 shows a small dining facility compartmentalized with 2 ft thick Hesco Bastion soil-filled revetments. The Hescos were not filled for this demonstration. Corrugated Metal Bin Revetments of similar size can also be used for this application.

Figure 8-26. Example of Hescos used to compartmentalize

Limitations: Mil 2 Hesco Bastions are 2 ft wide and can be stacked 6 ft tall. The recommended height for compartmentalization walls is 5 ft. Since these walls are much thicker and taller than the wooden or plastic soil bin walls described above, 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 due to their significant weight. Hygiene is also a consideration in a food service environment due to the presence of loose soil.

Construction Procedure: Installation instructions are in Chapter 6, Section 1 – Hesco Bastion Construction Techniques and General Information. These walls will not need to be anchored to the floor for stability.

Acquisition Information: NSN numbers are available for a variety of sizes and colors of Hesco Bastion Concertainer®. See the section for Revetments.

Performance against Weapons Effects: 2 ft thickness is adequate to stop all fragments from 60 mm Mortar through 122 mm Rocket.

OVERHEAD COVER

Providing overhead cover for areas with large concentration of personnel can help protect personnel from direct hits of indirect fire mortars. The basic concept (shown in Figure 8-27) 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. A matrix of material options for both the pre-detonation and shielding layer is given in Tables 8-6 and 8-7.

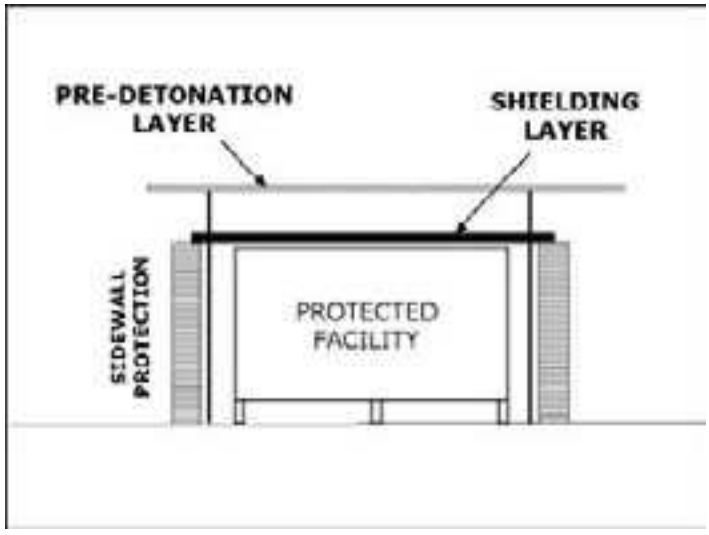


Figure 8-27. Conceptual overhead cover protection

Based on recent assessments of critical facilities throughout Iraq that have been identified as primary candidates for overhead cover protection, the approach for

constructing overhead cover can largely be classified into two categories. These categories include: (1) Internal protection, and (2) External protection. Each of these categories is discussed below.

Internal Protection

As shown in Figures 8-28 through 8-30, the internal protection approach is generally utilized for large metal buildings that are used for DFACs, PXs, 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 constructing the overhead protection 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. The overhead cover structure is constructed in this manner because due to the size of the metal building, the required size of structure 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; reference Table 8-6 recommendations. If the existing roof material on the metal building does not provide the required pre-detonation reliability, then augment or replace it with appropriate material.

Table 8-6. Material Options for Pre-detonation Layer

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[1]
4 in. Foam Sandwich Panel		YES[2]	YES[3]
22 ga. Corrugated Metal Deck, Type 1.5B		YES	NO
¼ in. Steel Plate		YES	YES[4]
1 Layer of Ballistic E-Glass, NSN 9340-01-533-5758		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

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).

[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.

[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.

[3] Based on results of August 2005 live-fire experimentation. Under experimentation, 1 of 1 quick-fused 120 mm mortars was successfully initiated.

[4] Potentially hazardous secondary debris may be generated when the 120 mm mortar pre-detonates on steel plate.

Table 8-7. Material Options for Shielding Layer

Shielding Layer Material	60-mm Mortar	82-mm Mortar	120-mm Mortar
3 ½ in. Sand	YES	YES	YES[1]
¼ in. Steel Plate	YES	YES	NO
5/8 in. Steel Plate	YES	YES	YES
2 Layers of Ballistic E-Glass, NSN 9340-01-533-5758	YES	YES	NO
3 Layers of Ballistic E-Glass[2], NSN 9340-01-533-5758	YES	YES	YES

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.

[1] 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.

[2] 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.

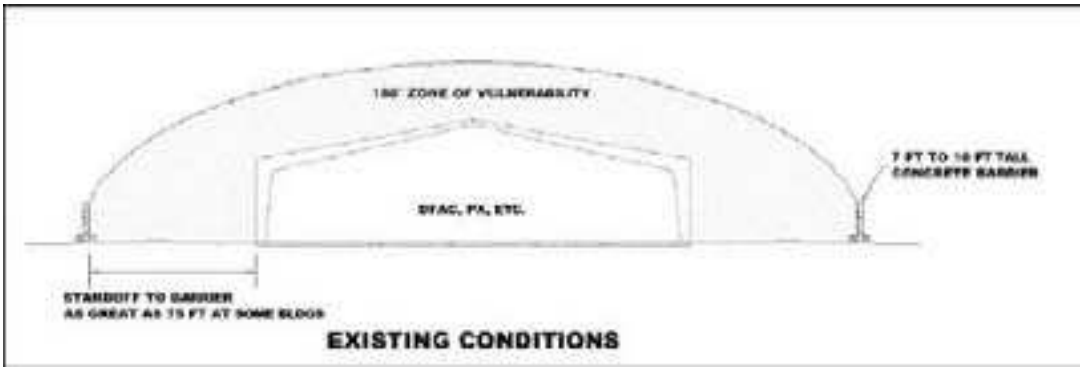


Figure 8-28. Existing conditions

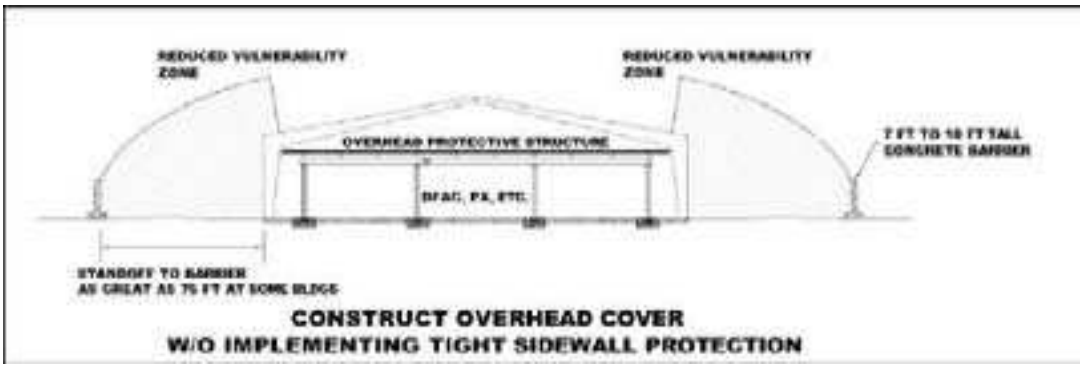


Figure 8-29. Internal protection, overhead cover without tight sidewall protection

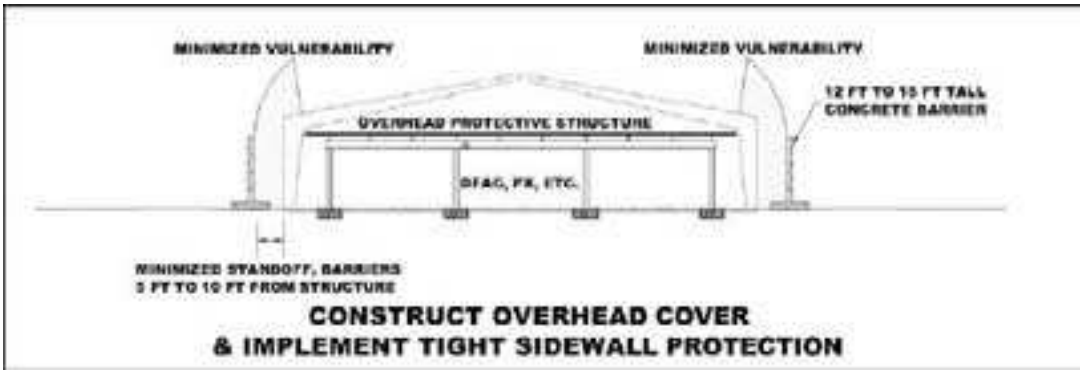


Figure 8-30. Internal protection, overhead cover and tight sidewall protection

Although the above describes construction of overhead cover, this cover does not fully provide protection from the overhead threat. As shown in Figure 8-29, 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 and pose a significant hazard to facility occupants. Therefore, it is recommended that in addition to the overhead cover construction, you place barrier walls of sufficient height tightly against the side of the buildings. By doing so, as shown in Figure 8-30, you significantly diminish the area over which the facility is vulnerable to attack.

External Protection. As shown in Figures 8-31 through 8-33, the external protection approach is utilized for structures that are generally composed of tents, modular trailer complexes or small metal buildings. Due to 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.

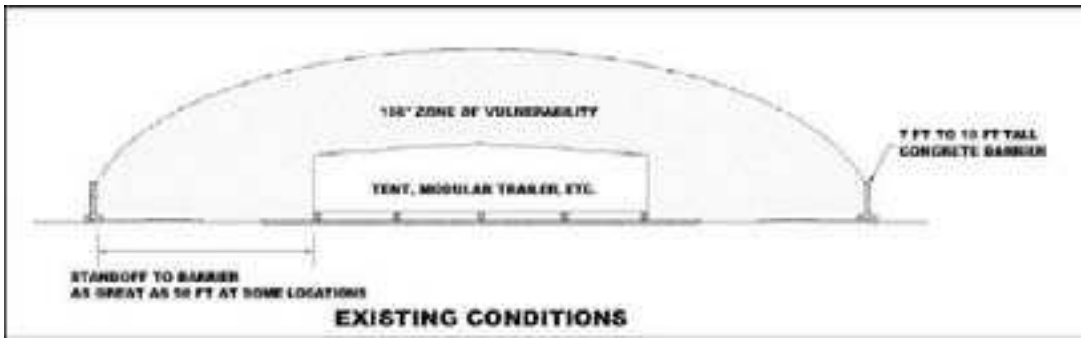


Figure 8-31. Existing conditions

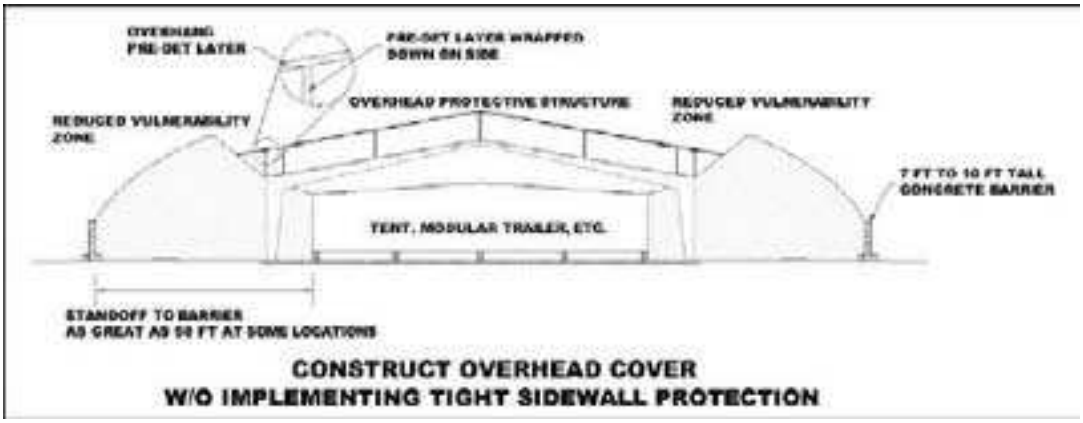


Figure 8-32. External protection, overhead cover without tight sidewall protection

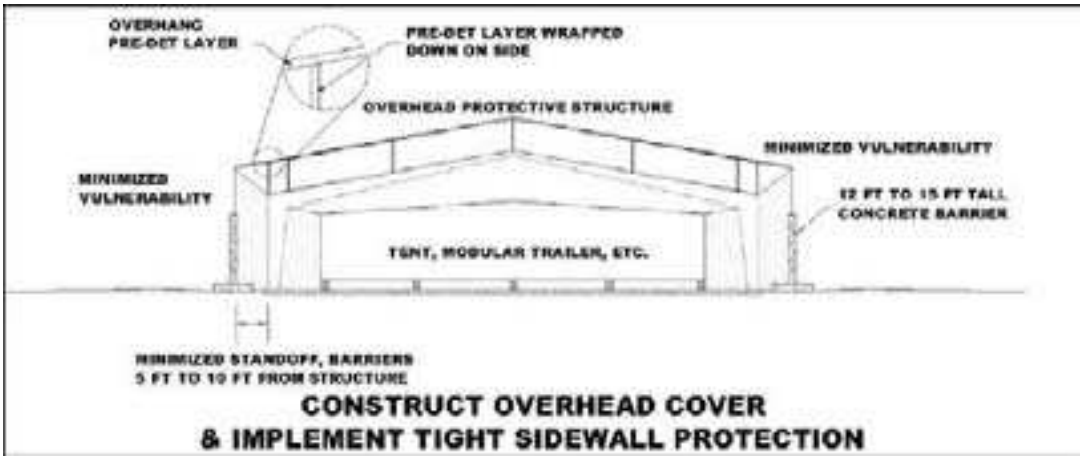


Figure 8-33. External protection, overhead cover and tight sidewall protection

As shown in the above figures, 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. **Although this is the case, it should not be immediately assumed that existing barriers placed at distance from the structures should be relocated.** The reason for this is that the existing barriers may likely be serving to provide protection from threats such as VBIEDs and, if moved, would simply expose the building to a different

threat. Therefore, you must consider the array of viable threats posed to each facility and make a determination whether existing barriers can be relocated, or whether new barriers must be acquired. When considering barrier locations, you must also give thought to ingress/egress, and you must maintained viable accessibility for normal use and in the case of an emergency.

The previous discussions have focused on the protective measures' geometrical layout and how they can be configured to most effectively intercept incoming munitions. It is also critical to reiterate the expected performance of the protective system when it does intercept a weapon – which is largely spelled out in Tables 8-6 and 8-7. Based on guidance provided from Multinational Corps-Iraq/Multinational Forces (MNC-I/MNF) and others, the research used to develop this information was targeted at protecting "less than permanent" facilities. As a result, light-weight, cost-effective solutions that provide significant mitigation of weapons' effects but do not constitute fully hardened structures have been a focus. Because of the lightweight nature of these protective structures, they will not have the capability to stop high-mass projectiles such as dudded 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.

SEAHUT OVERHEAD COVER RETROFIT

Description: Figures 8-34 and 8-35 show 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 3-layers 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 ½ inch plywood roof is utilized as a sacrificial pre-detonation layer.

Limitations: In tests using 120 mm mortars, only one fragment penetrated the 3-layer e-glass shielding layer, but due to 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, it is believed that little to no damage would have been seen 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.

Construction Procedure: Ten foot tall, 4 foot thick, load-bearing revetment walls are constructed around the SEAhut. Steel (W6x9) beams are inserted through the SEAhut sidewalls every 4 feet and rest upon the revetments. Three layers of e-glass are then fastened to the steel beams every 12 inches with self tapping screws before the roof joists are installed. Finally the remaining roofing material for the SEAhut can be installed as usual.

Figure 8-34. Placing Shielding Layer in SEAhut Retrofit

Figure 8–35. SEAhut Retrofit for Overhead Protection

Acquisition Information: Ballistic grade E-glass NSN: 9340-01-533-5758.

Required/recommended equipment: Carpenter tools, loader for revetments, standard hand tools.

Labor: Carpenters to construct SEAhut and retrofit.

Cost: Approximately $31K for metal revetments, $17K for E-glass, $1K for beams. Total retrofit ~$49K.

Space: Overall footprint expands to 28 ft x 62 ft as compared to the un-retrofitted 16 ft x 32 ft.

Weapon effects performance: Provides very near 100 percent protection from near-miss rockets and mortars and good protection from direct hit mortars.

PERSONNEL AND EQUIPMENT BUNKERS

Personnel bunkers are built either above ground or below ground and are made of reinforced concrete, revetment material, or timber. Bunkers offer excellent protection against direct fire and indirect fire effects and, if properly constructed with appropriate collective protection equipment, they 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, bombs). Prefabricated bunker assemblies (wall and roof) afford rapid construction and placement flexibility. Following are descriptions of bunker designs that have proven effective in weapon effects test and troop evaluations.

CONCRETE BUNKERS

An improvised reinforced-concrete bunker, referred to as a "SCUD bunker," has been built throughout the theatre of operations in Iraq and Afghanistan. The bunker, shown in Figure 8-36, was generally constructed with reinforced concrete "c" sections with Jersey barriers placed across each end. Sandbags were placed around the body of the bunker and in front of the Jersey barriers with the intent of increased fragmentation protection from near misses of indirect fire weapons.

Figure 8-36. Improvised Bunker using Concrete Culvert Sections.

Weapon effects test showed the sandbag/concrete walls generate good protection levels from moderately sized threats, but the lack of entrance shielding exposed 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. Although the bunker is referred to as a "SCUD" bunker, it will not protect its occupants from near misses of a SCUD missile.

The "shielded entrance" modular concrete bunker shown in Figure 8-37 was developed to eliminate the concerns of fragmentation entering into the open ended "SCUD bunker" and the possibility of a round landing between the Jersey barrier and the bunker. A series of weapon effects tests using 82 mm and 120 mm mortars and 122 mm rockets were conducted to verify

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 8-37. Basic Modular Concrete Bunker (without soil cover)

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. The following soil cover guidelines are recommended for protection from 82 mm and 120 mm mortars and 122 mm rockets.

- Place 2 to 3 layers of sandbags on the roof (Figure 8-38) 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 (Figure 8-39).
- 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.

(a) Pre-test with mortar on top of 2 layers of sandbags

(b) Post-test showing roof inside with minor spall damage.

Figure 8-38. Test of modular concrete bunker to static detonation of 120 mm mortar

Figure 8-39. Post-test photo of simulated 122 mm rocket over roof of cut and cover configuration of modular concrete bunker with 4' of soil cover: No damage inside.

General dimensions and reinforcing of the primary sections of the bunker are given in Figure 8-40. Concrete compressive strength is 4000 psi. Full construction plans are available in the JAT Guide and on the Antiterrorism Enterprise Portal (ATEP) web site.

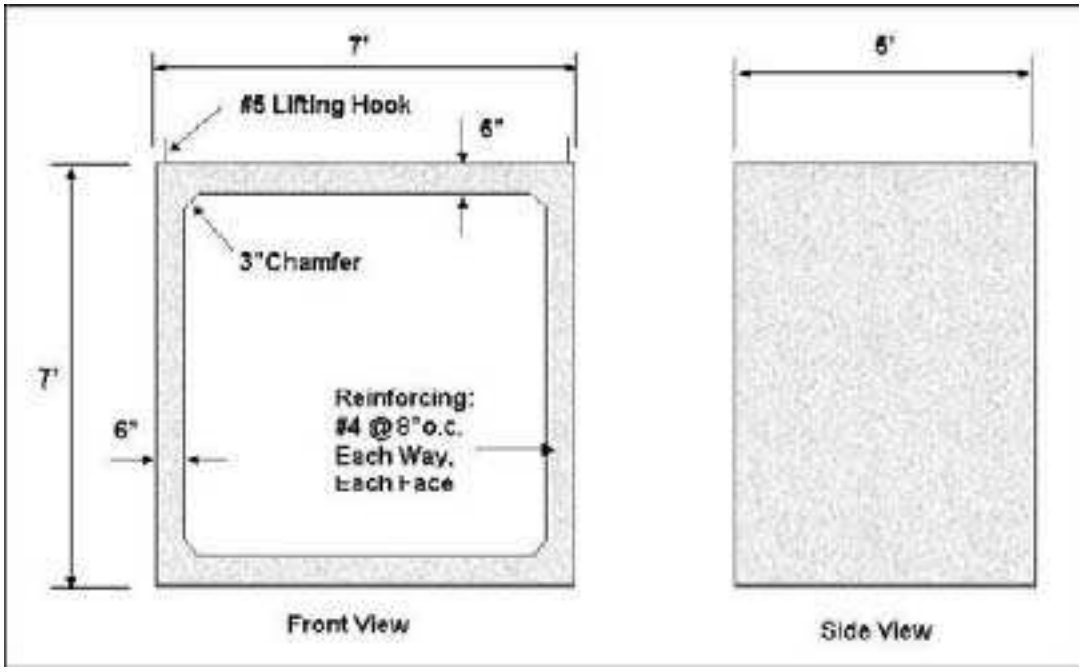


Figure 8-40. Primary Module For Modular Concrete Bunker

HESCO BASTION BUNKERS

Hesco Bastion soil bins have many applications, such as bunkers for personnel and equipment protection, revetments to provide fragment protection for equipment and personnel (this chapter) and as vehicle barriers (Chapter 6). Short descriptions and material requirements are provided for several above- and below-ground personnel bunkers constructed with HESCO Bastion soil bins. 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.

Metal Bins for Bunkers

Similar to the way Metal Bin Revetments can be used instead of Hescos for sidewall and helicopter protection, they can be used in the bunker designs presented in this section. However, the needed quantities may be different due to the different dimensions.

Overhead Cover

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 pulltruded fiberglass Composolite® panels, and larger systems are constructed with steel sheet piling. In the event the specified roof materials are not available, you can construct improvised roof systems. However, if improvised roof systems are utilized give close attention to ensure that they are adequately designed and properly constructed. Possible alternatives for the Composolite® roof materials

are runway landing mats or wooden stringer roofs. If you use wooden roofs, you should design and build them in accordance with the requirements of FM 5-103. Due to span lengths of the larger positions, you cannot replace the steel sheet piling with wooden stringers. Therefore, if you construct an improvised roof system for these positions, you will likely require steel beams to span the structure. After placement of the steel beams, you could use a wooden roof deck. **For the larger positions, it is especially critical that any improvised roof system be designed by a structural engineer to ensure it can safely carry the overhead cover.**

Performance and Weapon Effects

Position performance, with regard to both structural stability and weapon effects, is highly dependent upon infill material. Clearly, materials locally available in the theatre of operations will govern the infill material utilized. However, when multiple options are available certain types of material can be chosen to enhance position performance.

With regard to overall structural stability, coarse-grained soils such as sand, stone, and gravel tend to perform better than silts and clays. Silts and clays tend to be more prone to compression under loading, and will be more likely to exhibit wall shifting than coarse-grained materials. In addition, the strength of silts and clays is highly dependent upon soil moisture levels and are significantly weakened as moisture levels increase. However, the strength of sands and stones is much less moisture dependent.

With regard to weapon effects, sand performs significantly better than silts and clays. When constructed with 24 in. of overhead cover with sand for both the infill and overhead cover, each position will provide protection from the following:

- direct hit of a quick-fused 81 mm/82 mm mortar round
- air burst 155 mm artillery round
- direct fire 0.50 caliber
- 81 mm/82 mm mortars detonating in direct contact with walls
- 155 mm artillery rounds in direct contact with walls.

Positions constructed with silt or clay infill and overhead soil cover will provide less protection (reference FM 5-103, Chapter 3). Chain trigger screens can be utilized to defeat RPG-7's.

Aboveground 20' ISO/Milvan Container Personnel Bunker

An artist sketch of a 20' ISO/Milvan personnel bunker is shown in Figure 8-41.

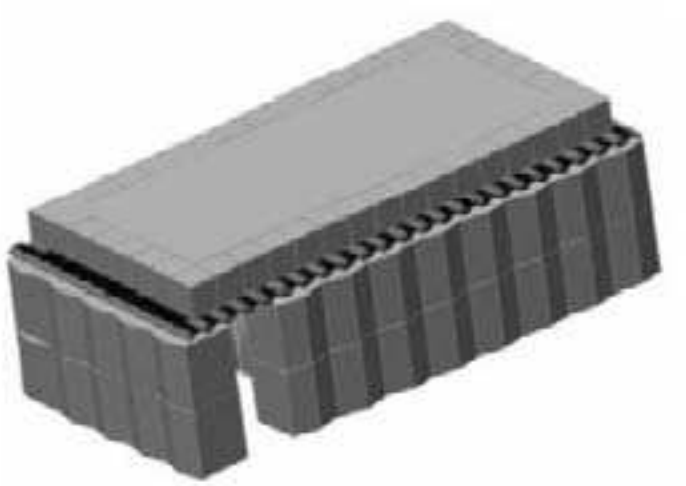


Figure 8-41. Artist sketch of completed bunker (app. 36' long x 18' wide x 12' high)

Bill of Materials. The Bill of Materials (BOM) for constructing the ISO/Milvan personnel bunker is provided in Table 8-8.

Table 8-8. Bill of Materials for the ISO/Milvan personnel bunker

Item Description	NSN	Quantity
Concertainer® * – 4.5 ft high, 3.5 ft wide, 32 ft long	5680-99-001-9396 – Green 5680-99-835-7866 – Beige/Sand	6
Concertainer® *– 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Beige/Sand	22
Sheet piling – 18 ft long Skyline Steel CS 55 steel sheet piling, or equal (see "Sheet Piling Properties" on next page for material requirements)	NSN not available	19
Sandbags	--	100
Waterproof membrane (44 ft x 18 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	180

* Note: Metal Bin Revetments of similar sizes can be substituted for the Hescos (Concertainer®)

Material requirements and properties for the sheet piling are provided in Figure 8-42. Note that width requirement is based on the number of sheet piling required to construct the roof. If piling of a different width is used, the required number of pieces shown in the BOM may change.

- Material Requirements
  - ASTM A572, Grade 50 steel
  - All piling shall be primed and painted as required

- Minimum Section Properties
  - Thickness (t) = 0.2"
  - Height (h) = 6"
  - Width (w) = 27.5"
  - X-axis section modulus = 6.3 in3/ft

- X-axis moment of inertia = 18.7 in4/ft

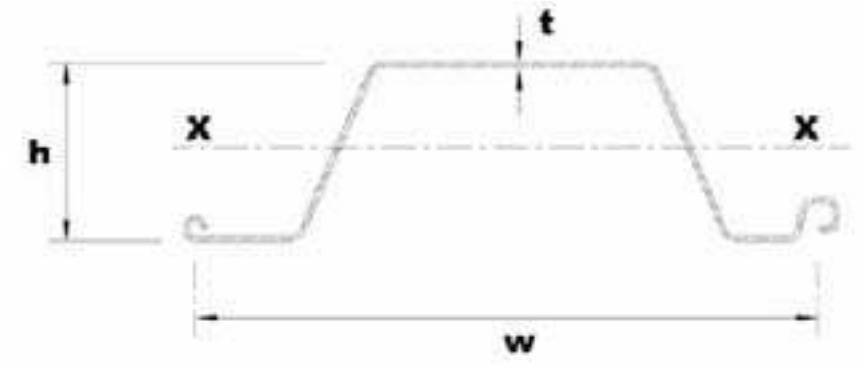


Figure 8-42. Cross section and properties of sheet pile roof support material

Equipment, Personnel and Time Estimate

To assist in planning, estimates of the necessary equipment and soldier assets and total construction time required to construct this position are provided in Table 8-9. In many cases, multiple types of equipment are capable of performing the same task and are listed as alternatives. During planning give consideration to such issues as equipment and operator availability, topographic and work area limitations, maneuverability, etc. and their impact on the construction effort. 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. Additional necessary items are hand tools, such as shovels, rakes, pliers, wire cutters, etc. 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.

Total estimated soldier asset requirements for constructing this bunker are 70 man hours.

Table 8-9. Equipment and soldier assets required to construct the ISO/Milvan personnel bunker

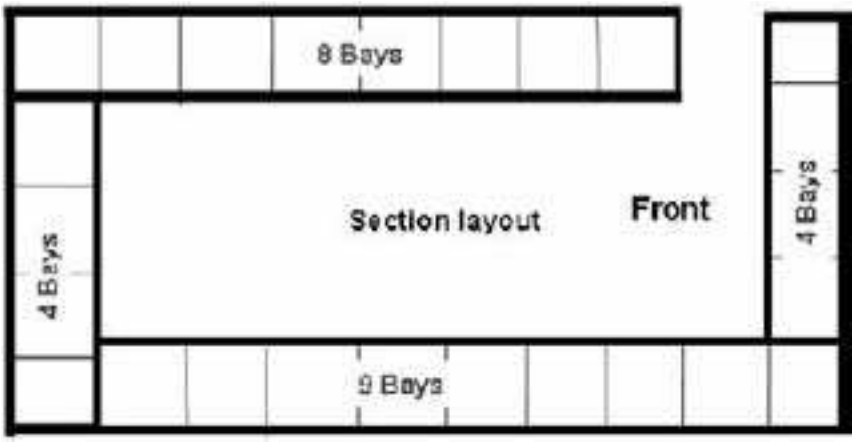
Task	Equipment Req'd.	Soldiers Req'd. (excluding operators)	Time Req'd.
Site preparation and foundation leveling	bulldozer, DEUCE, ACE, front-end loader, HMEE	2	1 hour
Foundation compaction	vibratory roller (smooth drum or pad feet), HSC	2	30 minutes
Haul infill material to site	dump trucks	varies	varies
Position ISO	crane, forklift	2	30 minutes
Erect walls and place infill	front-end loader, HMEE	6	5 hours
Construct roof and place infill	forklift, crane (w/clamshell bucket for infill), HYEX	6	6 hours

Construction Procedures

Step-by-step instructions for emplacing the ISO/Milvan bunker are provided in Figures 8-43 – 8-50. The key points to check during construction are as follows:

- ☐ Ensure that the foundation is level and compacted before constructing bunker walls.
- ☐ Compact infill material.
- ☐ Ensure that the walls are straight and vertical.
- ☐ Center sheet piling support for roof on the walls.
- ☐ Interlock sheet piling forming the bunker roof.
- ☐ Provide waterproof membrane over roof prior to placing soil cover.
- ☐ Maintain proper soil cover depth.

STEP 1 - FIRST LAYER



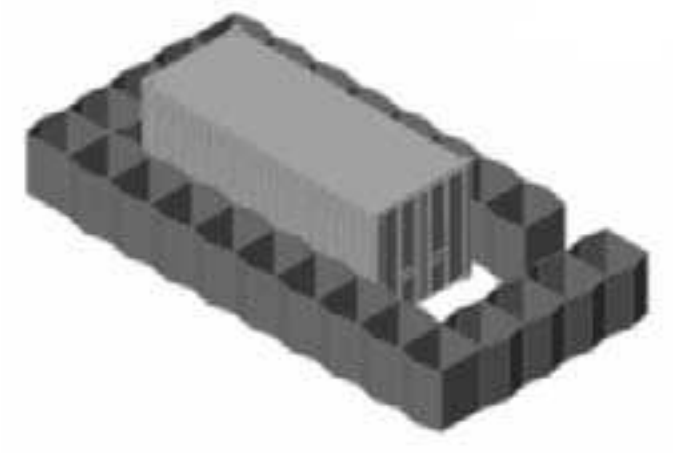
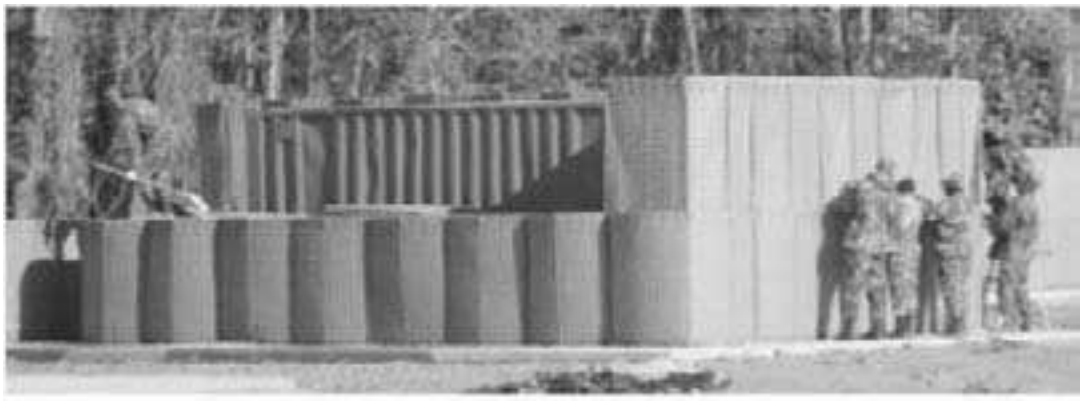


Figure 8-43. Layout and artist concept for first layer.

- ☐ Materials required: 3 sections of Concertainer® – 4.5 ft high x 3.5 ft wide x 32 ft long (9 bays per section).
- ☐ Refer to "Site Preparation and Infill Guidelines" and "Concertainer® Construction Techniques" for detailed information on Concertainer® construction.
- ☐ Collapse one bay to make a section 8 bays long.
- ☐ Break one section into two units, 4 bays each.
- ☐ Arrange Concertainer® as shown in drawing – Ensure flaps at bottom of units are unfolded
- ☐ Fill Concertainer® with infill material.
- ☐ MAKE SURE FILL IS VERY WELL COMPACTED.

Figure 8-44. Filling and compacting first layer (gravel fill material).

STEP 2 - SECOND LAYER



Placing second layer

Connecting second layer to first using plastic wire ties

Second layer in place and filled

Figure 8-45. Construction of second layer.

□ Materials required: 3 sections of Concertainer® – 4.5 ft high x 3.5 ft wide x 32 ft long (9 bays per section).

- ☐ Collapse one bay to make a section 8 bays long.
- ☐ Break one section into two units, 4 bays each.
- ☐ Arrange Concertainer® as shown in Step 1.
- ☐ Connect second layer to first using plastic wire ties as shown.
- ☐ Fill Concertainer® with infill material.
- ☐ MAKE SURE FILL IS VERY WELL COMPACTED.

STEP 3 – SHEET PILING ROOF SUPPORT

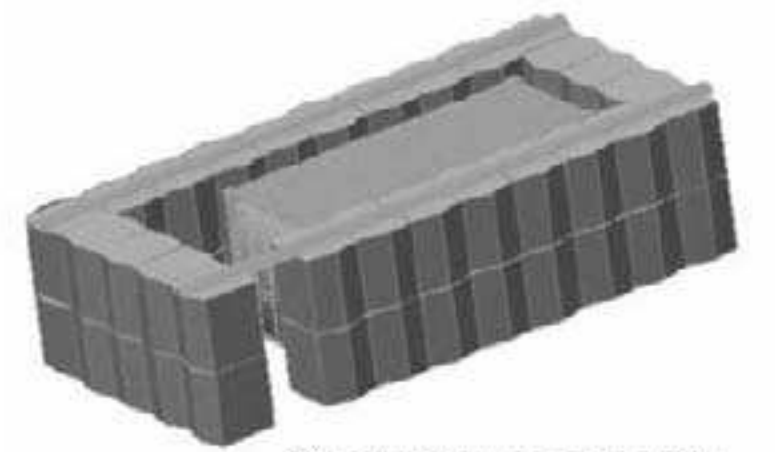


Figure 8-46. Installing sheet piling for roof support.

- ☐ Materials required: (4) – 18 ft long pieces of sheet piling.
- ☐ Place 2 pieces of sheet piling end-to-end on top of each side wall as shown.
- ☐ ENSURE PILING IS CENTERED ON SIDE WALLS.

STEP 4 – SHEET PILING AND SAND BAG ROOF

Interlock sheet piling

Place sheet piling roof

Place waterproof membrane

Figure 8-47. Installing sheet pile roof.

- ☐ Materials required:
  - (15) – 18 ft long pieces of sheet piling
  - (100) – Sandbags
  - (1) – 44 ft × 18 ft waterproof membrane
- ☐ Place sheet piling on top of roof supports as shown. When placing sheet piling, utilize the built-in interlocking system to interlock piling. Interlocking is achieved by sliding the pieces together from the ends.
- ☐ Place waterproof membrane on top of sheet piling. Ensure membrane conforms to shape of sheet piling.
- ☐ Use sandbags to level perimeter of roof.

Sand bags used to level perimeter of roof

Figure 8-48. Waterproof membrane and use of sandbags along roof edge.

STEP 5 - OVERHEAD COVER

Figure 8-49. Construction of overhead protection layer.

- ☐ Materials required: 22 sections of Concertainer®– 2 ft high × 2 ft wide × 4 ft long.
- ☐ Place Concertainer® as shown in drawing. Ensure sandbags are located beneath edge of Concertainer® to prevent soil from leaking between Concertainer® and roof.
- ☐ Fill Concertainer® with loose fill and lightly compact.
- ☐ Fill center of roof with 2 ft of fill.

STEP 6 - BUNKER CHECKLIST

Figure 8-50. Artist concept of completed bunker.

Check completed bunker to ensure:

- ☐ No excessive deflection of roof (up to 0.75 in. is acceptable).
- ☐ Roof supports centered on side walls.
- ☐ Sheet piling roof fully supported by roof supports.
- ☐ Walls straight.
- ☐ No excessive settlement of walls.

HEMTT-LHS/PLS BUNKER

Similar to bunkers for ISO containers, Hesco and Metal Bin Revetment material can be used to construct bunkers for the heavy expanded mobility tactical truck-helicopter landing site (HEMTT-LHS) and palletized load system (PLS) cargo containers. These bunkers can be used to protect any equipment or materials that will fit inside. Examples of the HEMTT and PLS bunkers constructed with Hescos are shown in Figures 8-51 and 8-52. The construction procedure for these bunkers is similar to that shown for the ISO bunker. Additional details are given in the JFOB CD and in the JAT Guide.

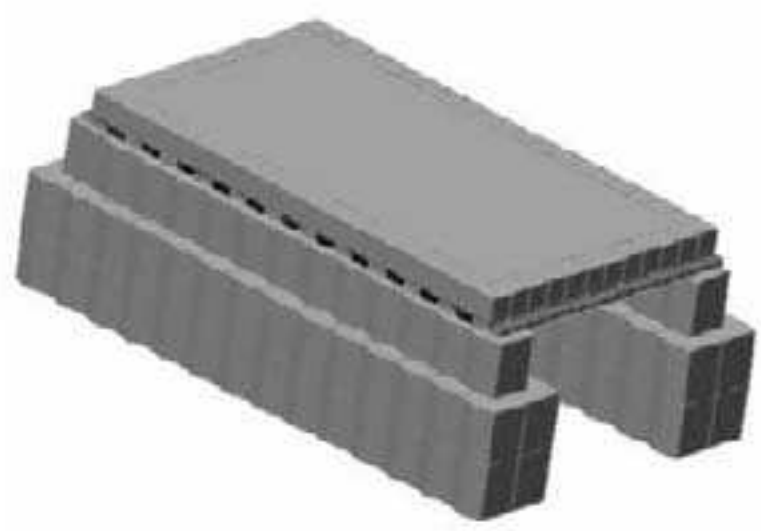


Figure 8-51. Artist concept of HEMTT bunker (app. 49’ long x 28’ wide x 16’ high)

Bill of Materials

The BOM for constructing the HEMTT bunker is provided in Table 8-10.

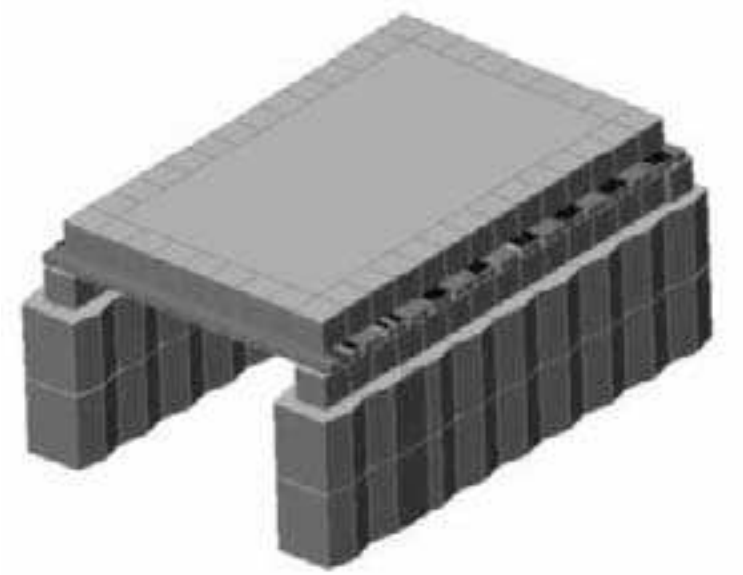


Figure 8-52. Artist concept of the PLS cargo bunker (app. 32' long x 21' wide x 14' high)

Bill of Materials

The BOM for construction the PLS cargo bunker is provided in Table 8-11 below.

BELOWGROUND 40' ISO/MILVAN 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 and pose a serious hazard to personnel inside. Material requirements, fabrication details, and time estimates are provided below.

Bill of Materials

The BOM for constructing the ISO personnel bunker is provided in Table 8-12 and 8-13.

Equipment, Personnel and Time Estimate

To assist in planning, estimates of the necessary equipment and soldier assets and total construction time required to construct this position are provided in Table 8-14. During planning give consideration to such issues as equipment and operator availability, topographic and work area limitations, maneuverability, etc. and their impact on the construction effort. Only heavy equipment is listed below. Hand tools such as wrenches, shovels, rakes, pliers, wire cutters, etc. will also be needed.

The indicated time required for construction does not include fabrication times for the structural steel assemblies. If steel assemblies are not pre-fabricated, factor the appropriate time and resources into the estimates shown below. Time estimates are given for installing steel assemblies in container. Factors such as threat-based urgency, equipment and material availability, soil type, 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.

Total estimated soldier asset requirements for constructing this bunker are 49 man hours.

Table 8-10. Bill of Materials for HEMTT Bunker

Item Description	NSN	Quantity
Concertainer® * – 4.5 ft high, 3.5 ft wide, 32 ft long	5680-99-001-9396 – Green 5680-99-835-7866 – Sand/Beige	18
Concertainer® *– 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Sand/Beige	31
Sheet piling – 25 ft long Skyline Steel CS 76 steel sheet piling, or equal. Note that Sheet Piling is not used on sidewalls as it is for ISO bunker	NSN not available	19
Sandbags	-	136
Waterproof membrane (56 ft x 25 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	470

* Note: Metal Bin Revetments of similar sizes can be substituted for the Hescos (Concertainer®)

Table 8-11. Bill of Materials for the PLS Cargo Bunker

Item Description	NSN	Quantity
Concertainer® * – 4.5 ft high, 3.5 ft wide, 32 ft long	5680-99-001-9396 – Green 5680-99-835-7866 – Sand/Beige	5
Concertainer® * – 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Sand/Beige	40
Sheet piling – 20 ft long Skyline Steel CS 76 steel sheet piling, or equal Note that Sheet Piling is not used on sidewalls as it is for ISO bunker	NSN not available	13
Sandbags	--	96
Waterproof membrane 38 ft x 20 ft	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	170

* Note: Metal Bin Revetments of similar sizes can be substituted for the Hescos (Concertainer®)

Table 8-12. Structural Steel Assembly

Item Description	Quantity
TS 3 × 3 × 3/16 in. steel frame (min. yield stress = 50 ksi) *fabrication details contained herein	20
2 in. × 1/4 in. flat bar, 20 ft-3 in. long (min. yield stress = 50 ksi) *fabrication details contained herein	8
2 in. × 1/4 in. flat bar, 6 ft-4 in. long (min. yield stress = 50 ksi) *fabrication details contained herein	8
L 3-1/2 in. × 3-1/2 in. × 1/4 in., 19 ft-6 in. long (min. yield stress = 50 ksi) *fabrication details contained herein	4
3/8 in. DIA bolts, 4-1/2 in. long, 1-1/2 in. thread length min., w/ self-locking nuts	80
Plate washers, 7/16 in. I.D., 1-1/4 in. O.D., 1/8 in. thickness	16
3/8 in. dia lag screws, 1-1/2 in. long	38

Table 8-13. Revetment Walls & Roof

Item Description	NSN	Quantity
Concertainer® * – 4.5 ft high, 3.5 ft wide, 32 ft long *exact quantity required will vary with application	5680-99-001-9396 – Green 5680-99-835-7866 – Beige/Sand	4
Concertainer® * – 2 ft high, 2 ft wide, 4 ft long *exact quantity required will vary with application	5680-99-001-9397 – Green 5680-99-968-1764 – Beige/Sand	4
Composolite® panels, 10 ft long	5675-01-500-2761	6
Toggle connectors, 10 ft long	5675-01-500-2761	5
Sandbags	-	20

* Note: Metal Bin Revetments of similar sizes can be substituted for the Hescos (Concertainer®)

Table 8-14. Equipment and soldier assets required to construct the ISO/Milvan buried personnel bunker

Task	Equipment Req'd.	Soldiers Req'd. (excluding operators)	Time Req'd.
Install steel assemblies in container	--	4	4 hr
Position excavation	HYEX	1	4 hr
Place ISO	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

Bunker Construction Procedures

Following are step-by-step details on construction and placement of the ISO/Milvan buried personnel bunker. The construction details (See Figures 8-53 – 8-64) describe fabrication of the steel frame used to reinforce the containers to support the soil cover and loading from contact burst munitions as well as instructions on bunker placement. Note: **VERY IMPORTANT TO USE STEEL FRAME FOR STRENGTHENING. IF STEEL FRAME IS NOT USED, BUNKER MAY COLLAPSE UNDER SOIL LOADING OR FROM CONTACT BURST OF MUNITIONS.**

Step 1 – Frame Fabrication Details

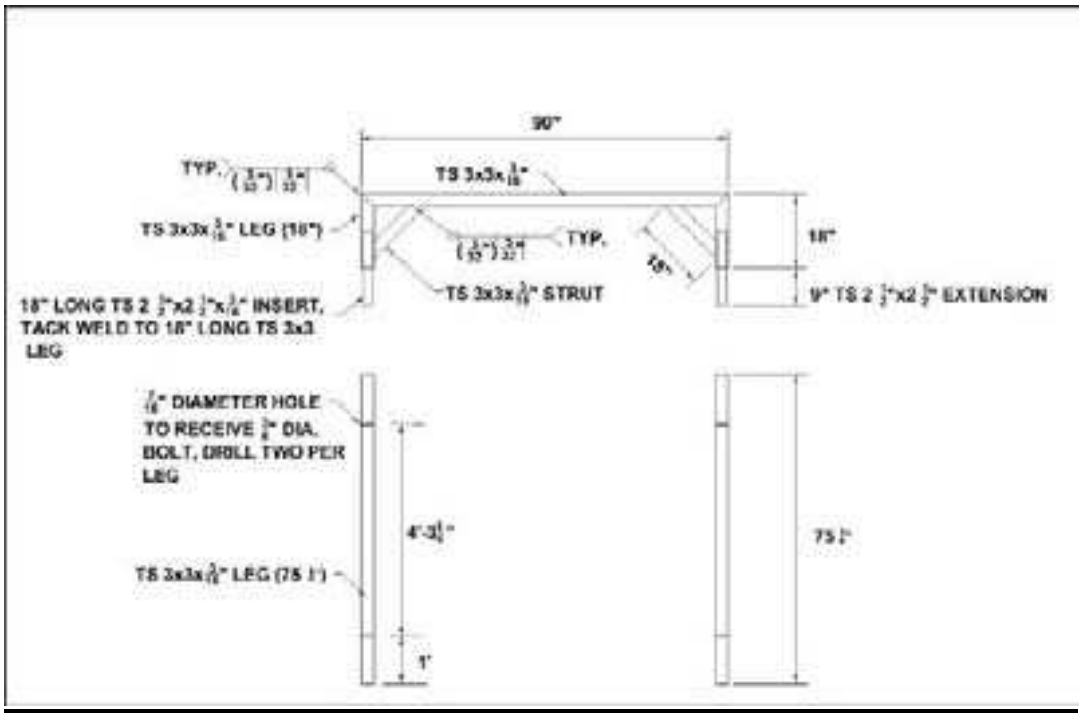


Figure 8-53. Steel frame fabrication details.

- Steel frames are fabricated in 3 pieces and can either be assembled in the container before shipping, or assembled upon arrival at the final destination.
- Reference detail above for frame fabrication requirements. Note that this frame configuration is based upon a standard 8 ft wide, 8 ft tall container.

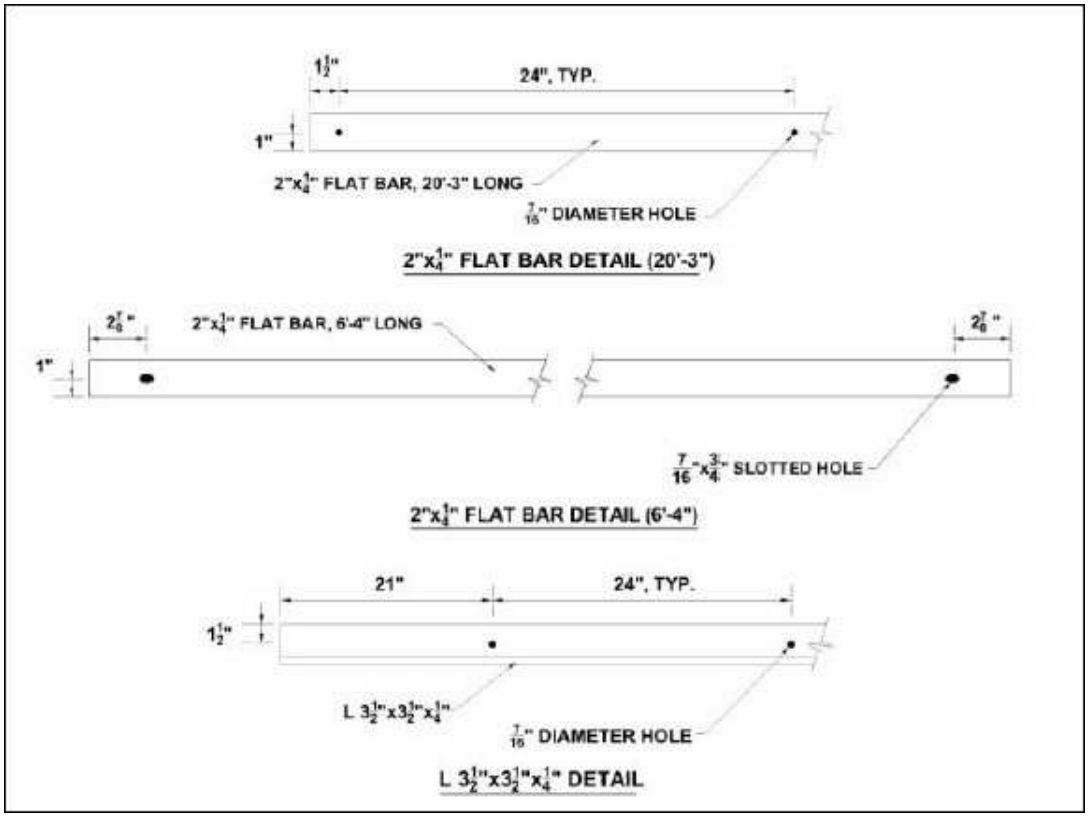


Figure 8-54. Flat bar and angle fabrication detail.

Step 2 – Steel Frame Assembly

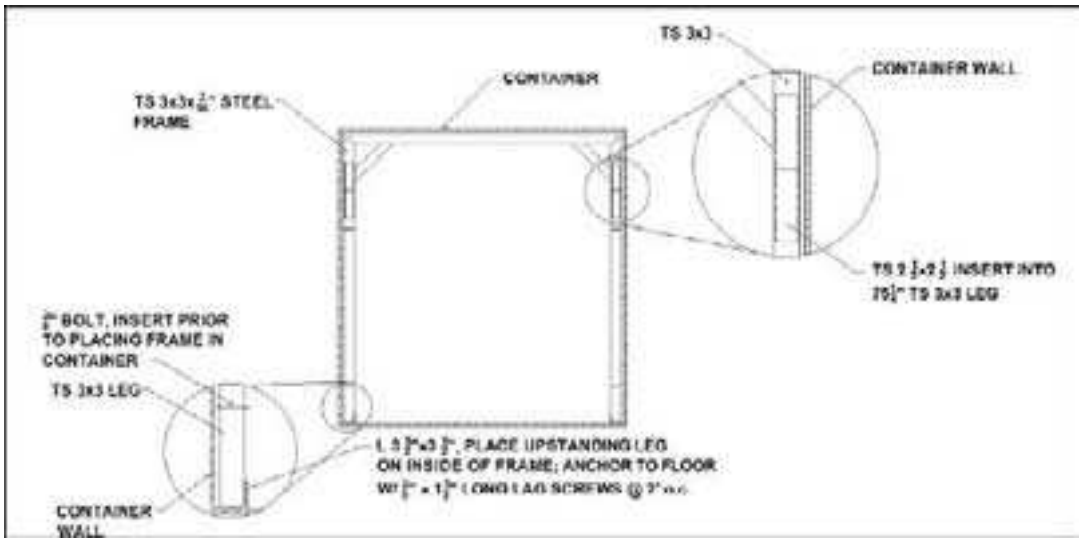


Figure 8-55. Steel frame assembly details.

□ Place two L3-1/2 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 on center (Ensure anchor placement will not interfere with frames).

□ Assemble steel frame by inserting 9 in. long TS 2-1/2 in. × 2-1/2 in. extensions into 75-1/4 in. long TS 3×3 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).

Figure 8-56. Photo of assembled steel frame section.

Step 3 –Steel Frame Installation

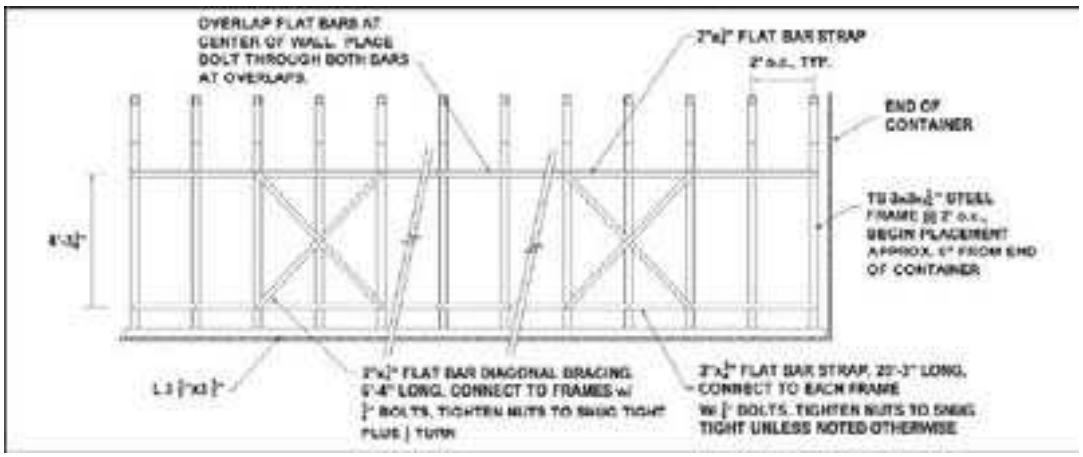


Figure 8-57. Steel frame installation detail.

- □ Install assembled frames at 2 ft on center. 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.

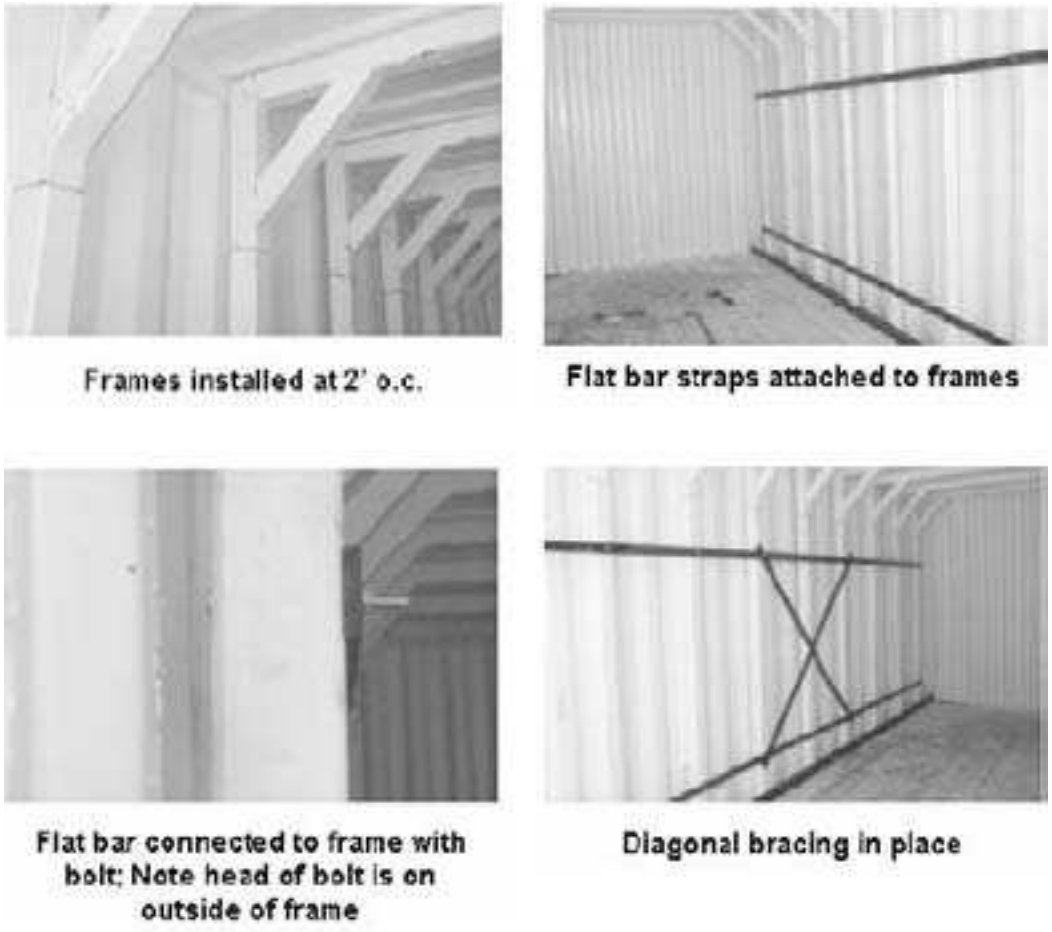


Figure 8-58. Photos of steel frame installed in ISO/Milvan.

Step 4 – Site Excavation & Container Placement

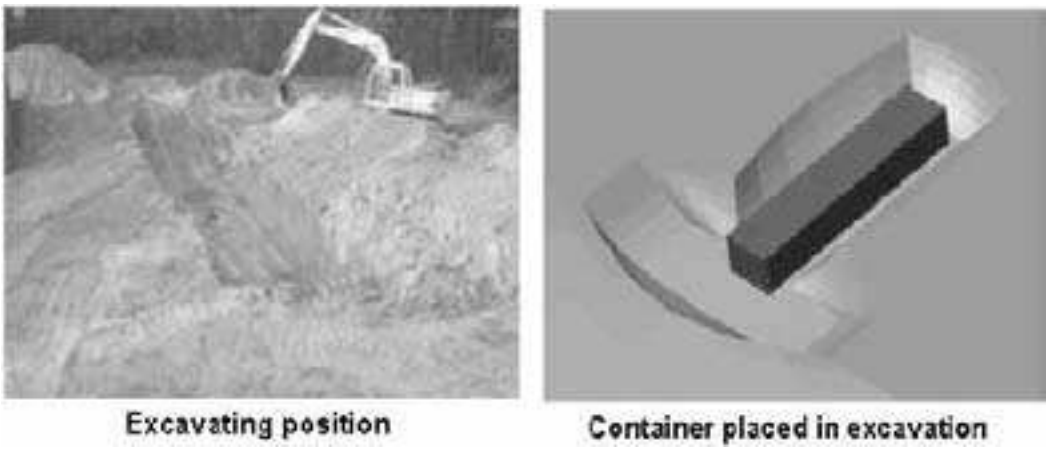


Figure 8-59. Preparing location and placing ISO/Milvan.

- Make "container excavation" by digging a hole approximately 8 ft deep, 38 ft long and 10 ft wide. The container will be placed in this excavation. Slope hole such that when container is placed, the floor will slope slightly towards the doors to promote drainage.

- At the end of the "container excavation" where the doors will be placed, excavate a hole approximately 8 ft deep, 12 ft wide and 32 ft long perpendicular to container. This will be the "entrance excavation" and will be used to provide an entryway to the position. At ends of excavation, taper to natural ground to provide access.
- Place ISO container in "container excavation." After placement, the container should extend approximately 3.5 ft into the "entrance excavation" (see picture above).
- When making excavations, ensure sides are adequately sloped to prevent cave-in while soldiers are working in excavation.

Step 5 – Concertainer® Revetment (1st Layer)

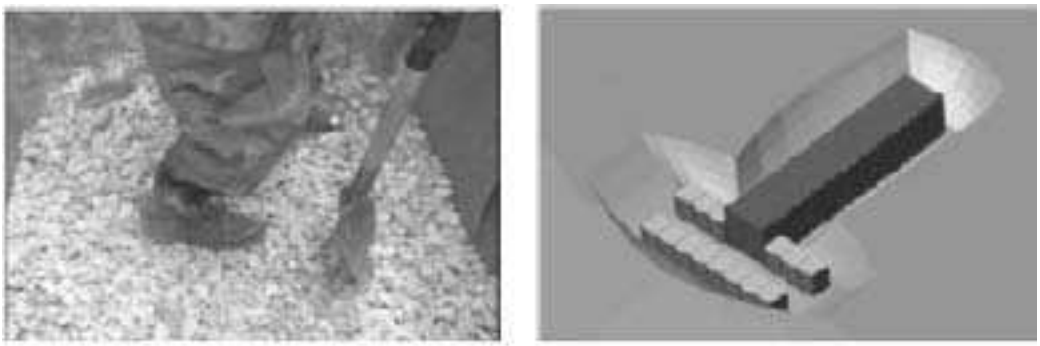


Figure 8-60. Construction of entrance section (first layer).

☐ Materials required: 2 sections of Concertainer® - 4.5 ft high × 3.5 ft wide × 32 ft long (9 bays per section).

☐ Refer to "Site Preparation and Infill Guidelines" and "Concertainer® Construction Techniques" for detailed information on Concertainer® construction.

☐ Collapse one bay to make a section 8 bays long.

☐ Break one 9-bay section into two 3-bay sections.

☐ Arrange Concertainer® as shown in drawing. Ensure revetment walls are placed 5 ft apart.

☐ Fill Concertainer® with infill material.

☐ MAKE SURE FILL IS VERY WELL COMPACTED.

Step 6 – Concertainer® Revetment (2nd Layer)

☐ Materials required: 2 sections of Concertainer® - 4.5 ft high × 3.5 ft wide × 32 ft long (9 bays per section).

☐ Collapse one bay to make a section 8 bays long.

☐ Break one 9-bay section into two 3-bay sections.

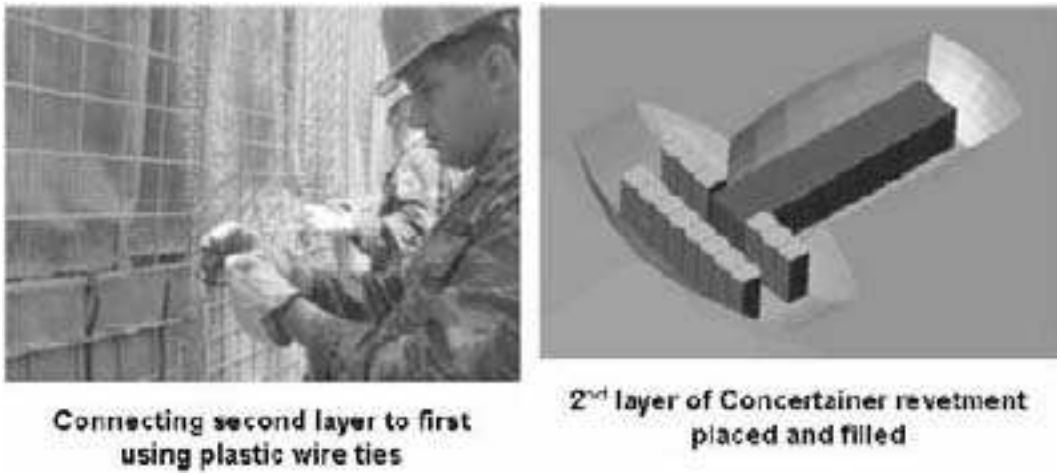


Figure 8-61. Construction of entrance section (second layer).

□ Arrange Concertainer® as shown in drawing. Connect second layer to first using plastic wire ties as shown.

□ Fill Concertainer® with infill material.

□ MAKE SURE FILL IS VERY WELL COMPACTED.

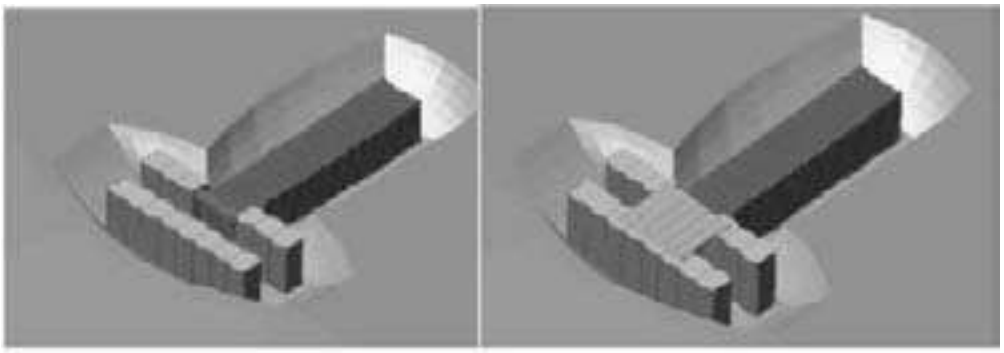
Step 7 – Fiberglass Roof

□ Materials required:
(6) – 10 ft long Composolite® panels
(5) – 10 ft long toggle connectors
(20) – sandbags

□ Place sandbags over container entrance to provide level bearing surface for roof panels.

□ Place Composolite® panels on top of revetment walls. Center roof on entrance to container.

□ Connect panels using toggle connectors. Drive toggle connectors in as far as possible, and then cut flush. Repeat from opposite end as necessary to provide connection along full 10 ft length.



Place sandbags over container entrance to level roof support surfa

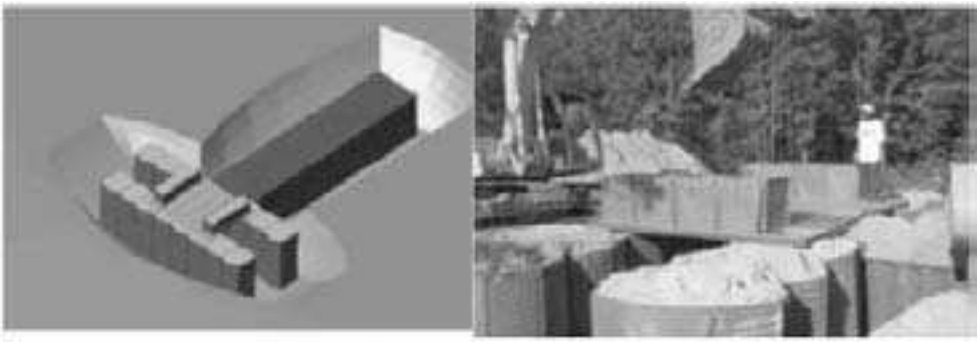
Place Composolite™ panels on revetment walls

Connecting panels with 10' toggle connectors

Figure 8-62. Construction of entrance section (roof).

Step 8 – Roof Overhead Cover

- ☐ Materials required: 4 sections of Concertainer® - 2 ft high × 2 ft wide × 4 ft long.
- ☐ Place Concertainer® along edge of roof panels as shown in drawing.
- ☐ Fill Concertainer® with loose fill material and lightly compact.
- ☐ Fill center of fiberglass roof with 2 ft of infill material.



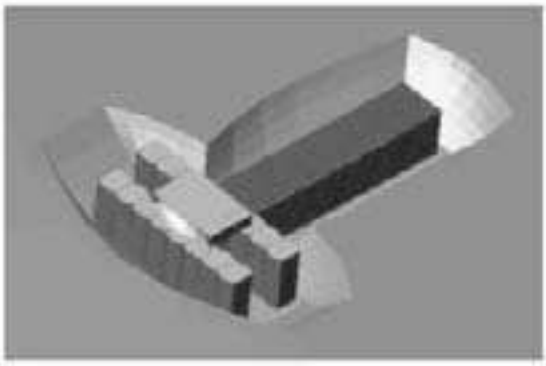


Figure 8-63. Construction of entrance section (overhead cover).

Step 9 – Backfill Bunker

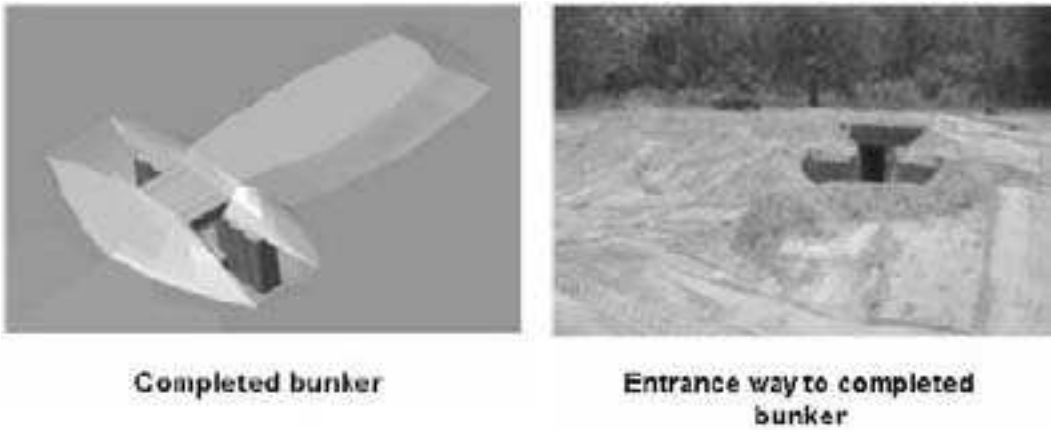


Figure 8-64. Artist concept and photo of completed bunker.

- □ 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.
- ☐ Because of carbon monoxide poisoning, allow no open flames inside of bunker.

Bunker Complex

In the event it is necessary to provide multiple bunkers in close proximity, you can establish a bunker complex in the fashion indicated in Figure 8-65. Each ISO/Milvan container will have to be reinforced with steel frames as described previously. Note that the roof panels and soil cover are not shown for clarity.

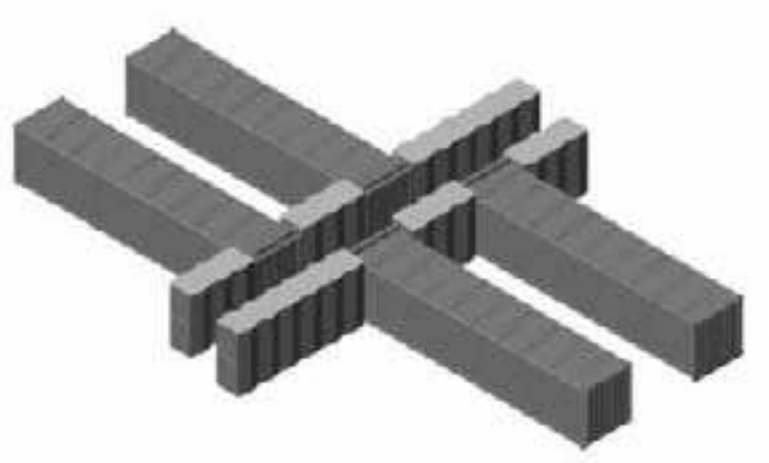


Figure 8-65. Bunker complex using ISO/Milvan containers

TIMBER BUNKERS

Numerous designs are in FM 5-103 “Survivability” for timber bunkers. They are either underground, partially underground, or above ground. In all cases, soil cover provides fragmentation and blast protection. The timbers are used to provide support for the soil cover. Table 8-15 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.

Table 8-15. Center-to-Center Spacing for Wood-supporting Soil Cover to Defeat Various Contact Burst

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				
2x4	2 (0.6)	3 (7.6)	4 (10)	4 (10)	4 (10)	3 (8)
	3 (0.9)	18 (46)	12 (30)	8 (20)	5 (13)	3 (8)
	4 (1.2)	18 (46)	14 (36)	7 (18)	4 (10)	3 (8)
2x6	2 (0.6)	4 (10)	7 (18)	8 (20)	8 (20)	6 (15)
	3 (0.9)	18 (46)	18 (46)	16 (41)	12 (30)	8 (20)
	4 (1.2)	18 (46)	18 (46)	18 (46)	11 (28)	7 (18)
4x4	2 (0.6)	7 (18)	10 (25)	10 (25)	9 (22)	7 (18)
	3 (0.9)	18 (46)	18 (46)	18 (46)	12 (30)	8 (20)
	4 (1.2)	18 (46)	18 (46)	18 (46)	10 (25)	7 (18)
4x8	1.5 (0.5)	4 (10)	5 (13)	7 (18)	8 (20)	8 (20)
	2 (0.6)	14 (36)	18 (46)	18 (46)	18 (46)	18 (46)
	3 (0.9)	18 (46)	18 (46)	18 (46)	18 (46)	18 (46)
		120- and 122-mm Contact Burst				
4x8	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)
6x6	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)
6x8	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)
8x8	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				
4x8	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)
6x6	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)
6x8	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)
8x8	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)

NOTE: The maximum beam spacing listed in the above table 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.

HARDENED FIGHTING AND OBSERVATION POSITIONS

This section presents several designs for construction of fighting positions and observation posts that will allow engagement of an enemy and offer some level of protection from small arms, VBIEDS and near-miss and direct hits of RAMs. Figures 8-66 – 8-73 and Tables 8-16 and 8-17 give construction photos, drawings and details. These positions can be used around the perimeter of the JFOB to enhance security and at ECPs for overwatch positions. Most of these designs have NSNs and have been developed and tested by the ERDC. Tests results indicate that the overhead cover provided will protect from direct hits of 81/82-mm mortar rounds (the Metal Bin Observation Post will protect from 120 mm mortars) 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.

LARGE OBSERVATION POST (HESCO VERSION)

Figure 8-66. Large Observation Post (app. 20’ x 16’ x 10’ high)

Bill of Materials

To assist in planning, estimates of the necessary equipment and soldier assets and total construction time required to construct this position are provided in Table 8-17. In many cases, multiple types of equipment are capable of performing the same task and are listed as alternatives. During planning give consideration 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.

Table 8-16. Bill of Materials for Large Observation Post

Item Description	NSN	Quantity
Concertainer® – 4.5 ft high, 3.5 ft wide, 7 ft long	Modified 5680-99-001-9396 – Green Modified 5680-99-835-7866 – Beige/Sand	7
Concertainer® – 2 ft high, 3.5 ft wide, 3.5 ft long	Modified 5680-99-001-9396 – Green Modified 5680-99-835-7866 – Beige/Sand	6
Concertainer® – 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Beige/Sand	16
Timbers – 6 in. x 6 in. x 16 ft long	--	10
Composolite® panels, 20 ft long	5675-01-496-4896	8
Toggle connectors, 20 ft long	5675-01-496-4896	7
Waterproof membrane (16 ft x 20 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	70

Equipment, Personnel and Time Estimate

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.

Total Estimated Soldier Asset Requirements = 45 man hours.

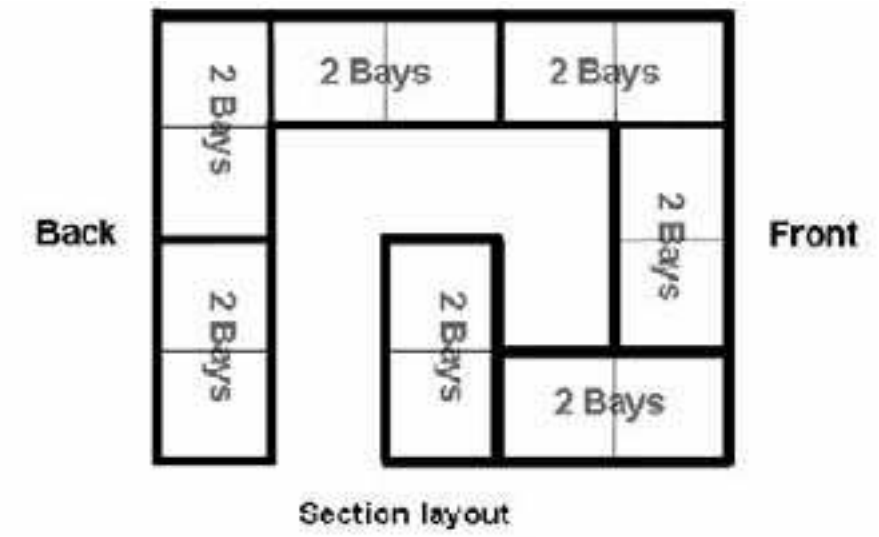
Table 8-17. Equipment, Personnel, and Time Estimate for Large Observation Post

Task	Equipment Req'd.	Soldiers Req'd. (excluding operators)	Time Req'd.
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

STEP 1 - FIRST LAYER

- □ Materials required: 7 sections of Concertainer® - 4.5 ft high × 3.5 ft wide × 7 ft long (2 bays per section).
- □ Refer to "Site Preparation and Infill Guidelines" and "Concertainer® Construction Techniques" for detailed information on Concertainer® construction.
- □ Arrange Concertainer® as shown in drawing. Ensure flaps at bottom of units are unfolded.

□ Fill Concertainer® with infill material.
□ MAKE SURE FILL IS VERY WELL COMPACTED.



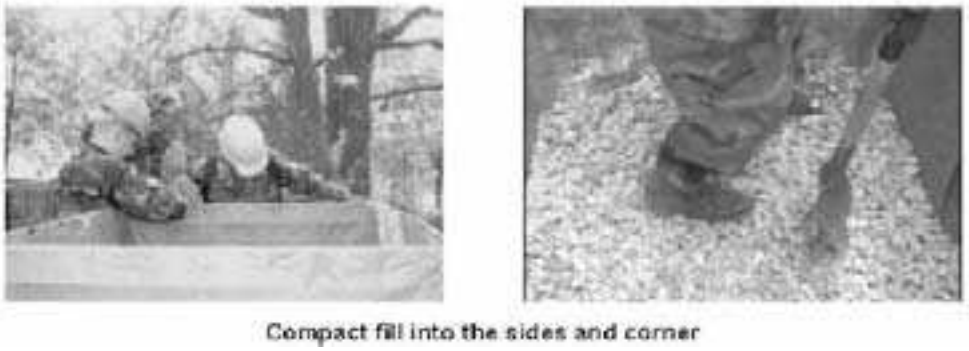


Figure 8-67. Layout and construction of first layer.

STEP 2 - SECOND LAYER

Figure 8-68. Layout and construction of second layer.

- ☐ Materials required: 6 sections of Concertainer® – 2 ft high × 3.5 ft wide × 3.5 ft long (1 bay per section).
- ☐ Arrange Concertainer® as shown in drawing.
- ☐ Connect second layer to first using plastic wire ties as shown.
- ☐ Fill with infill material.
- ☐ MAKE SURE FILL IS VERY WELL COMPACTED.

STEP 3 – TIMBER ROOF SUPPORT

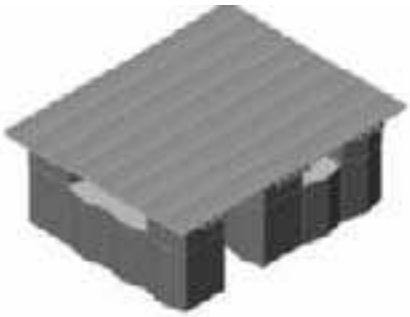
Figure 8-69. Layout and construction of timber roof support.

- ☐ Materials required: 10 timbers - 6 in. x 6 in. x 16 ft long.
- ☐ Place timbers on top of second layer as shown.

□ Ensure timbers are at least 6 in. from the edge of the Concertainer® and centered on top of supports.

□ Ensure all timbers are placed at the proper elevation to provide support to the roof. This is accomplished by sliding one piece of fiberglass panel from one edge of roof to the other. If any gaps are present between timbers and panel, adjust the timbers to eliminate gap.

STEP 4 - FIBERGLASS ROOF



Composolite panels on timber supports

Placing Composolite panels on roof supports

Connecting Composolite panels with 20' long toggle connectors

Figure 8-70. Installing roof.

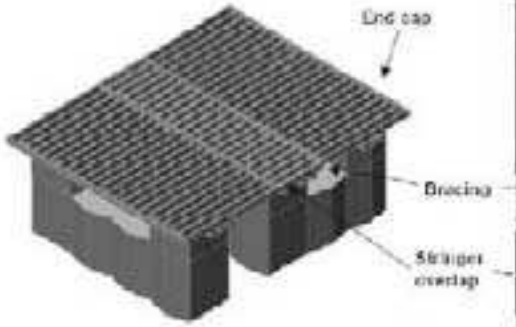
□ Materials required:
(8) – 20-ft long Composolite® panels
(7) – 20-ft long toggle connectors
(1) – 16 ft × 20 ft waterproof membrane

□ Place Composolite® panels on top of timber supports.

□ Connect panels using toggle connectors. Drive toggle connectors in as far as possible, and then cut flush. Repeat from opposite end as necessary to provide connection along full 20-ft length.

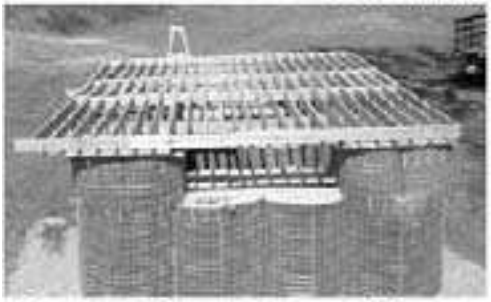
□ Place waterproof membrane on top of roof.

STEP 4 – OPTIONAL WOOD ROOF



Position layout

Bracing nailed at end of stringer overlap to prevent buckling



Completed stringer system, note 16' end caps and spacers

- Materials required:
  (50) - 2" x 8" x 12'
  (2) - 2" x 6" x 16'
- Cut 48 - 2" x 6" x 6.5" long spacers
- Place stringers 8" on center as shown in drawing
- Nail end of stringers to 16' end cap
- Nail bracing at both ends of stringer overlap

Position layout

Plywood decking nailed to stringers

- Materials required: 10 sheets - 4' x 8' x 3/4" plywood
- Cut 2 sheets of plywood in half to form 4 sections 4' x 4' x 3/4"
- Place decking in the pattern shown
- Nail to stringers using 10d nails spaced every 12"
- Place water proof membrane on top of roof

Figure 8-71. Construction of optional timber roof.

STEP 4 – OPTIONAL SHEET PILE SUPPORT AND ROOF

Figure 8-72. Artist concept of optional sheet pile roof.

□ Sheet Pile Supports:
- Materials required: 3 sheet pilings- 6”high x 27.5”wide x 14’long
- Place sheet pilings on top of second layer as shown in Step 3 for timber supports.
- Ensure sheet pilings are centered at top of support

□ Sheet Pile Roof:
- Materials required: (6) – 20’long sheet pilings (1) – 16’x20’ waterproof membrane
- Connect sheet pilings into one panel using the interlocking sleeves.
- Place panel on top of supporting sheet piling (welded wide flange and a crane are the “preferred method”).
- Place waterproof membrane on top of roof.

STEP 5 - OVERHEAD COVER

□ Materials required: 16 sections of Concertainer® – 2 ft high × 2 ft wide × 4 ft long.
□ Place Concertainer® as shown in drawing. Ensure flaps at bottom of units are folded in.
□ Fill Concertainer® with loose fill and lightly compact.
□ Fill center of roof with 2 ft of fill.

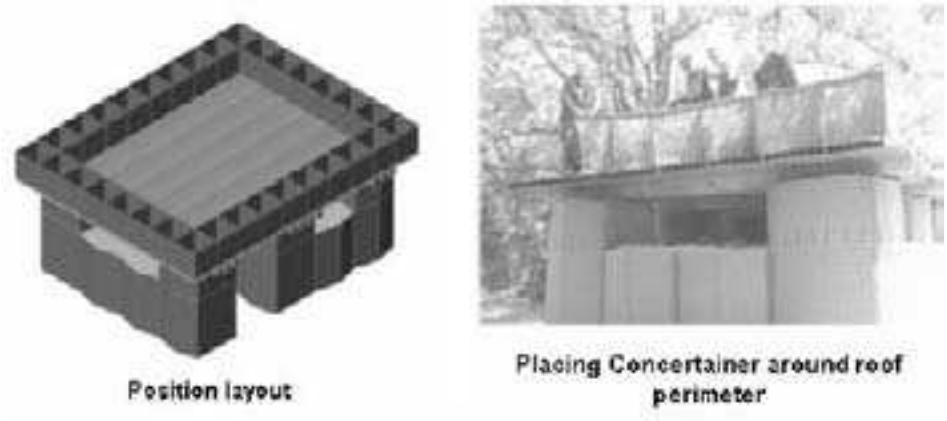


Figure 8-73. Addition of overhead protection.

STEP 6 - POSITION CHECKLIST

- ☐ Check completed position to ensure:
- ☐ No excessive deflection of roof (up to 2 in. is acceptable).
- ☐ No cracked timbers.
- ☐ Timbers well positioned on support.
- ☐ Walls straight.
- ☐ No excessive settlement of walls.

OPTIONAL CONSTRUCTION FOR ECP GUARD HOUSE

This position can be adapted for use at an ECP by adding an additional entrance if desired. Figure 8-74 shows the modified layout for the first and second layers of Hescos.

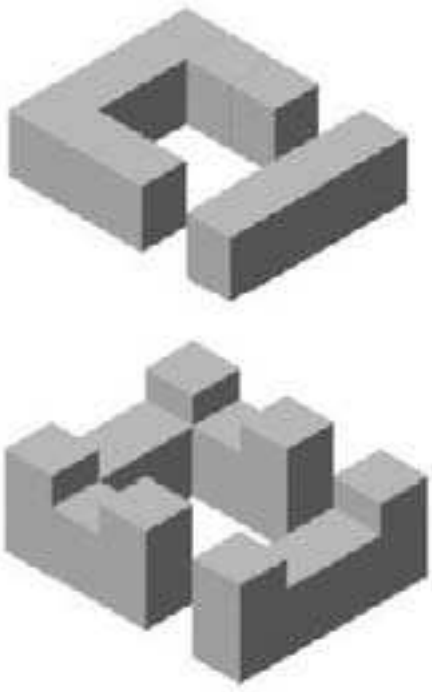


Figure 8-74. First and second layer for optional guard house layout.

LARGE OBSERVATION POST (METAL BIN REVETMENT VERSION)

Description

The metal revetment protective position is based on the Above Ground Large Observation Post (Hesco Version). One advantage of the use of the metal revetment instead of the geotextile-lined Concertainer® is the increased life span when subjected to the long-term effects of severe environmental conditions (UV, severe sand/wind loadings, etc.) as seen in Iraq and Afghanistan. Another advantage of this design is the overhead cover system has been shown through static and live-fire testing to protect from the direct hit of a 120 mm mortar. The overall footprint of the structure is 20 ft x16 ft. The interior of the structure has 7ft of clearance. Overhead cover is provided by 2 ft of soil contained within a 2-ft-high perimeter of metal revetments. Figures 8-75 – 8-85 show construction and details.

Figure 8-75. Aboveground Metal Bin Large Observation Post

Bill of Materials

The following is a list of the bill of materials for the metal revetment bunker.

Table 8-18. Bill of Materials for Large Observation Post

Item Description	NSN	Quantity
Metal Revetment Protective Position Kit	To Be Provided	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
Composolite® 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

Equipment, Personnel and Time Estimate

The estimates of the necessary equipment and soldier assets required to construct this position (Table 8-19) are similar to those for the Hesco Version. The total construction time is estimated at 51 man hours.

Table 8-19. Equipment, Personnel, and Time Estimate for Large Observation Post (Metal Bin Revetment Version)

Task	Equipment Req'd.	Soldiers Req'd. (excluding operators)	Time Req'd.
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

STEP 1 – LEVEL SURFACE, LOCATE COLUMNS

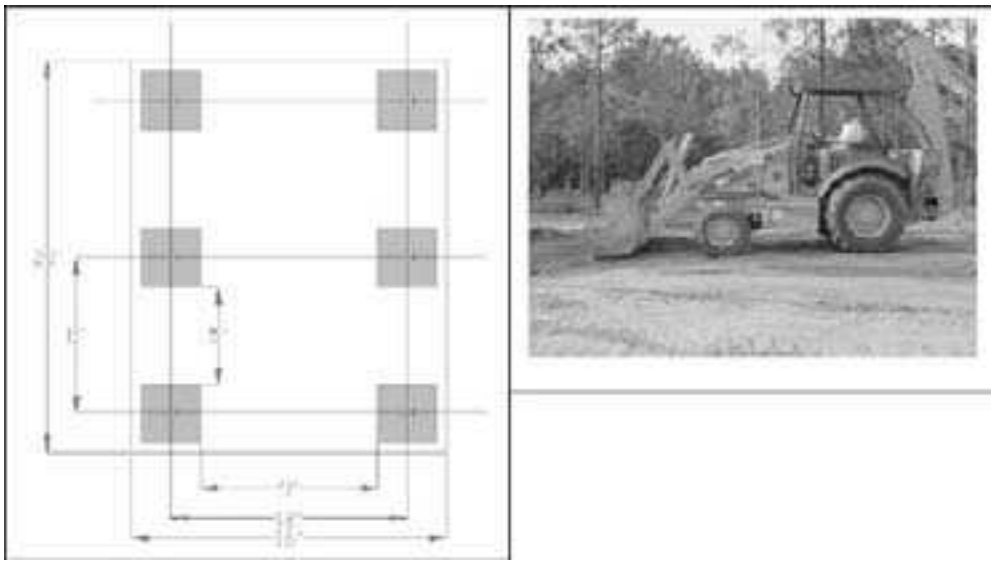


Figure 8-76. Position layout and leveling site.

- ☐ Ensure ground surface is completely level and well compacted
- ☐ Mark positions for column placement.

Step 2 – Place Columns (Columns are very important for a stable structure)

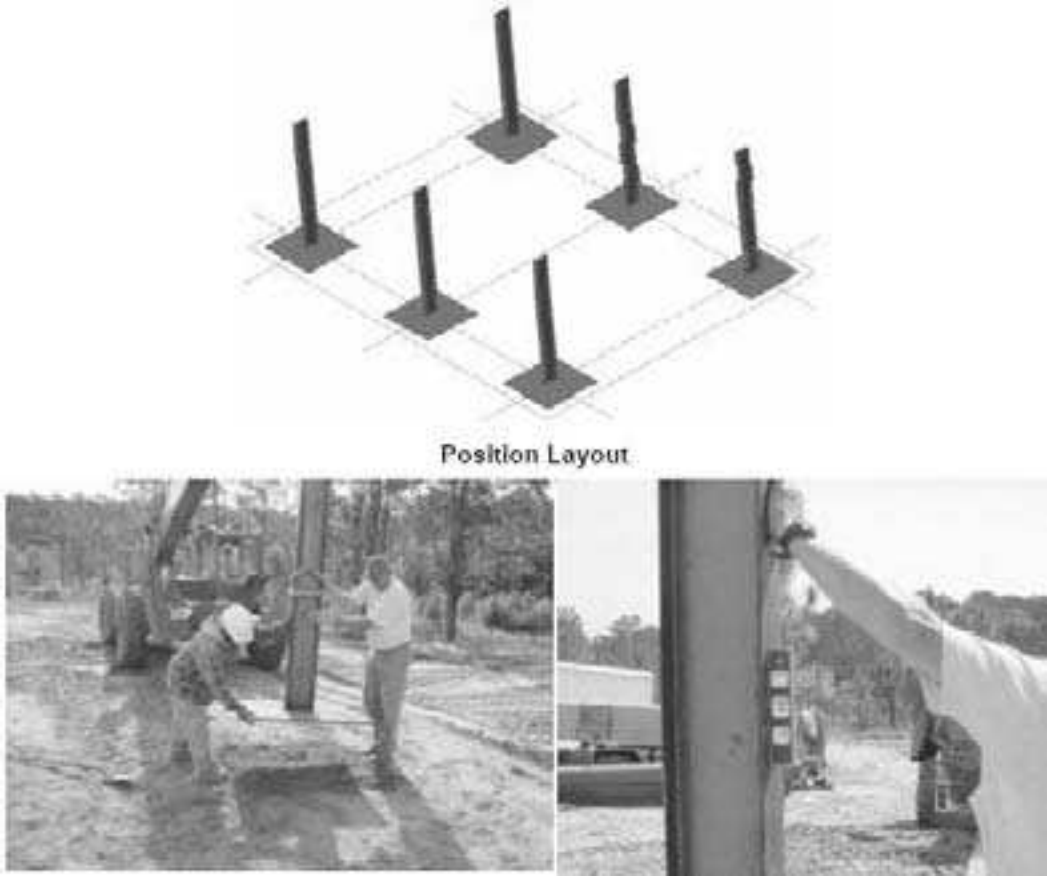


Figure 8-77. Positioning and installing columns.

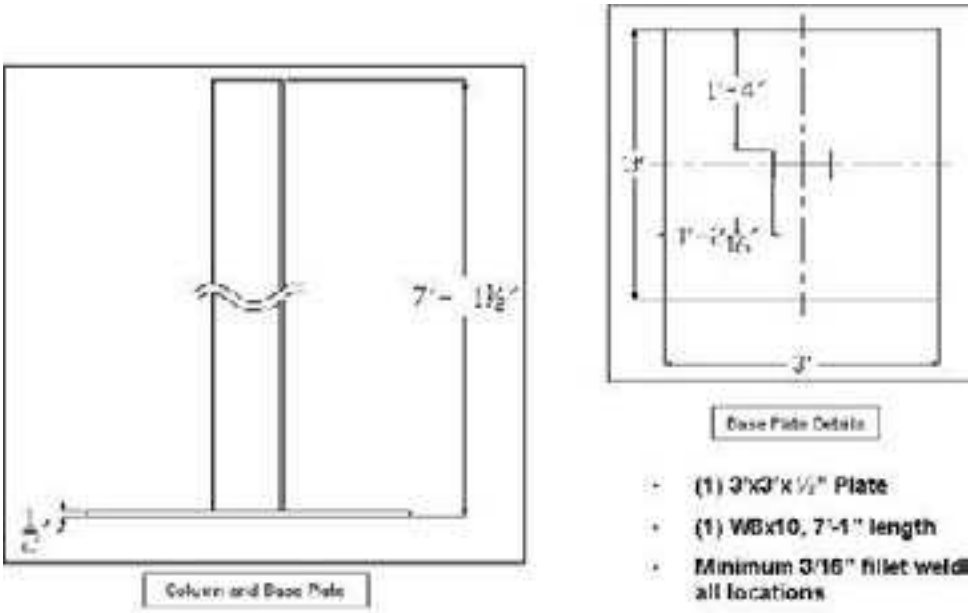
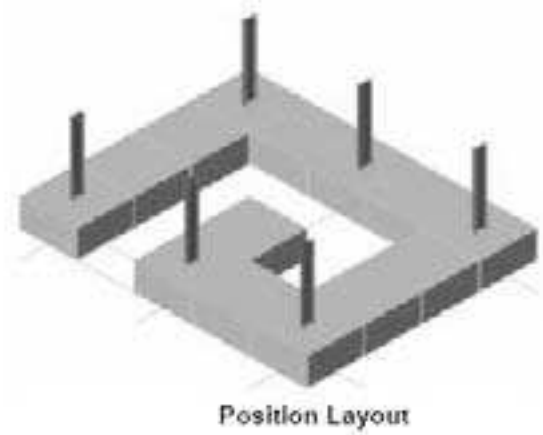


Figure 8-78. Steel details for column and base plate.

- ☐ Materials required: 6 Steel Columns with Base Plate Sections.
- ☐ Ensure webs of columns are parallel with short side of positions.
- ☐ Check columns for plumb and level.

STEP 3 – FIRST LAYER



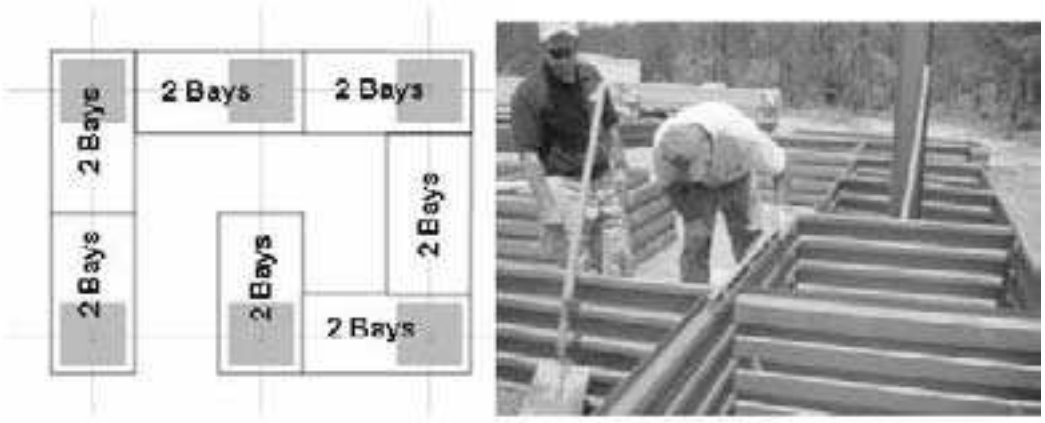


Figure 8-79. Layout and construction of first layer.

- ☐ Materials required: (7) - 4’x8’x2’ metal revetment kits.
- ☐ Arrange as shown above.
- ☐ Refer to “Metal Revetment Assembly Construction Guide” for detailed guidance on assembling individual metal bins.
- ☐ Check revetments to ensure they are level.
- ☐ Fill with infill material.
- ☐ MAKE SURE INFILL MATERIAL IS WELL COMPACTED.

STEP 4 – SECOND LAYER

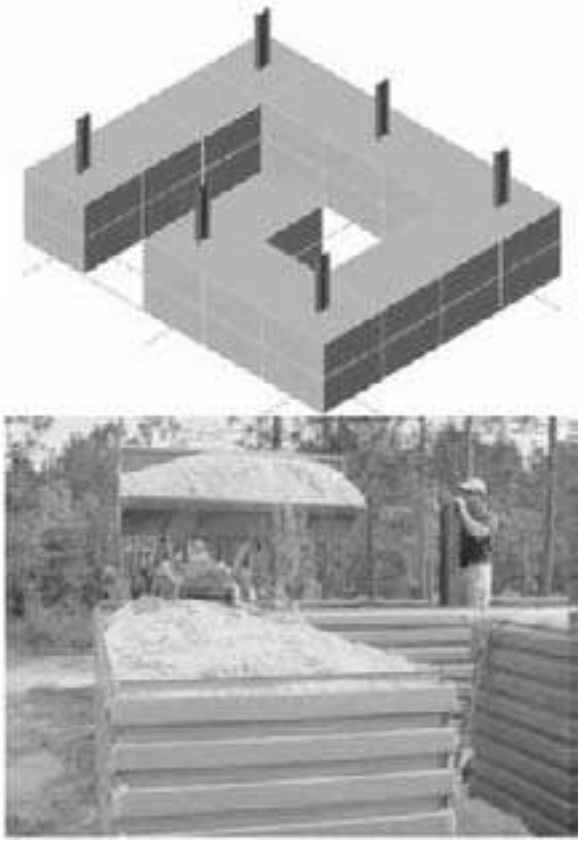
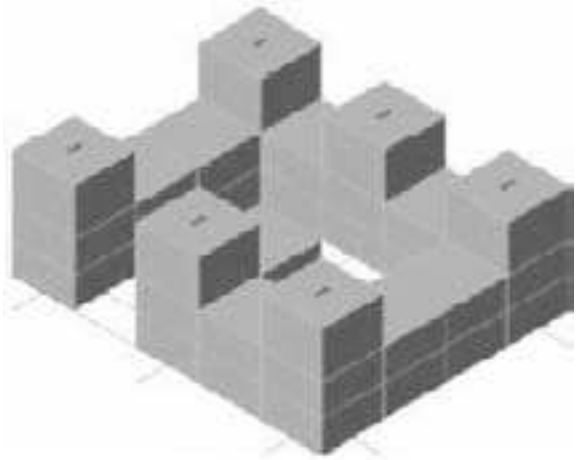


Figure 8-80. Layout and construction of second layer.

- ☐ Materials required: (7) - 4’x8’x2’ metal revetment kits.
- ☐ Construct second layer directly on top of first layer.
- ☐ Refer to “Revetment Assembly” for detailed guidance on assembling individual metal bins.
- ☐ Check revetments to ensure they are level.
- ☐ Fill with infill material.
- ☐ MAKE SURE INFILL MATERIAL IS WELL COMPACTED.

STEP 5 – THIRD LAYER



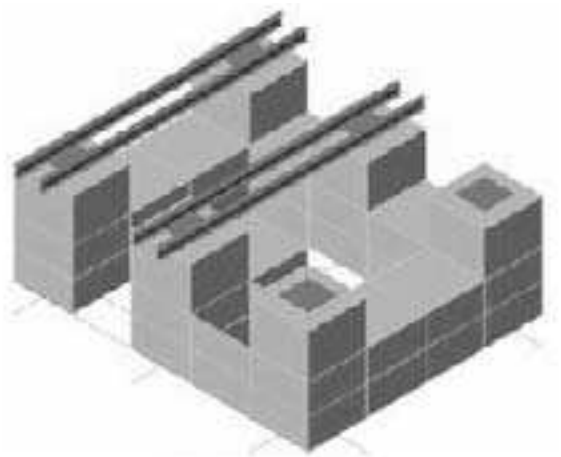
Position Layout

Figure 8-81. Layout and construction of third layer.

- ☐ Materials required: (6) - 4’x4’x3’ metal revetment kits.
- ☐ Construct third layer around column layers.
- ☐ Refer to “Revetment Assembly” for detailed guidance on assembling individual metal bins.
- ☐ Check revetments to ensure they are level.
- ☐ Fill with infill material

□ MAKE SURE INFILL MATERIAL IS WELL COMPACTED.

Step 6 – Cap Plates & Roof Support



Position Layout

Position Layout

Figure 8-82. Layout and installation of cap plates and steel roof support beams.

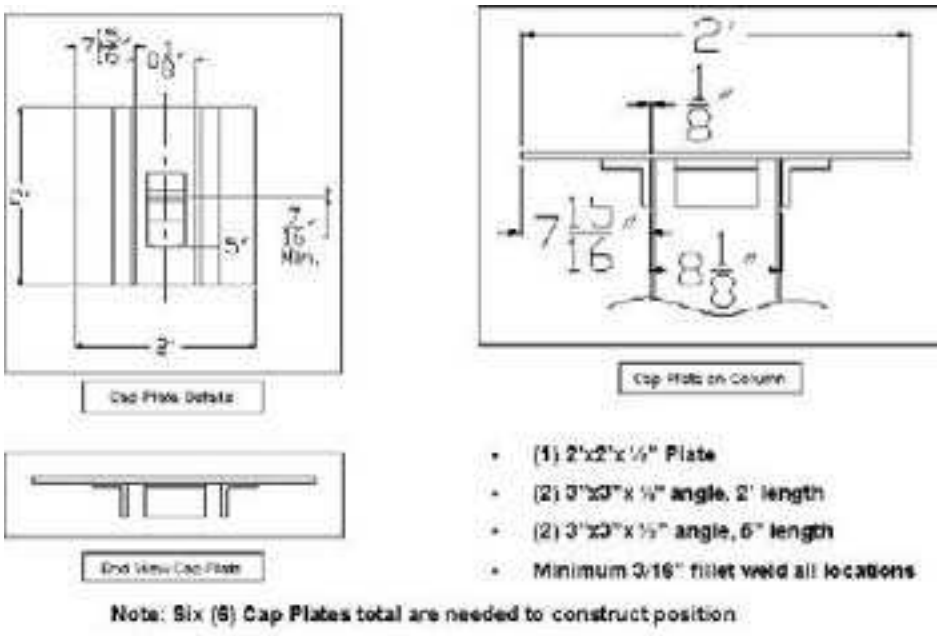


Figure 8-83. Steel details for cap plate.

☐ Materials required:
☐ (6) - 2'x 2'x ½" steel cap plates.
☐ (6) – Steel beams, W 8 x 10, 18 ft. long
☐ Place cap plates on top of columns.
☐ Bring fill material up to flush with cap plates.
☐ Place steel beams on cap plates; ensure 1 ft overhang on each side.

Step 7 – Fiberglass Roof

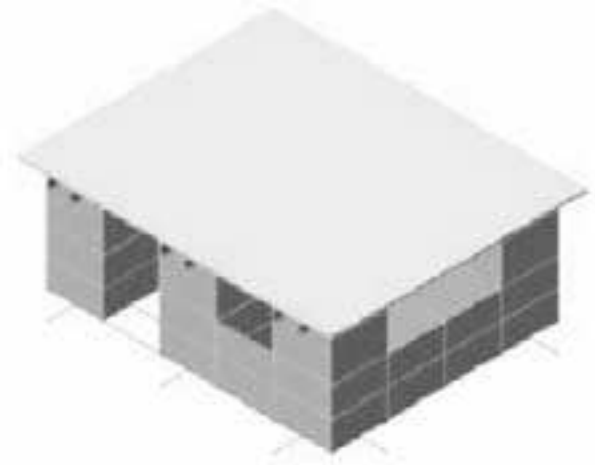


Figure 8-84. Artist concept of completed Composolite® roof.

☐ Materials required:
(9) - 22' long Composolite® panels.
(8) – 22' long toggle connectors
(1) – waterproof membrane, 18'x 20'
☐ Place Composolite® panels on top of steel beams

- ☐ Connect panels using toggle connectors. Drive toggle connectors in as far as possible then cut flush. Repeat from opposite end as necessary to provide connection along full 22 ft length.
- ☐ Place waterproof membrane on top of roof.

Step 7 – Optional Sheet Pile Roof

- ☐ Materials required:
  (8) – 22 ft long sheet pile sections (See ISO bunker for details) (1) – 18 ft × 20 ft waterproof membrane
- ☐ As a replacement for the Composolite® decking, place the 22 ft long sheet pile sections on top of the steel beams. Be sure to interlock the sheet pile sections during placement (See ISO bunker for details).
- ☐ Place waterproof membrane on top of roof.

Step 8 – Overhead Cover

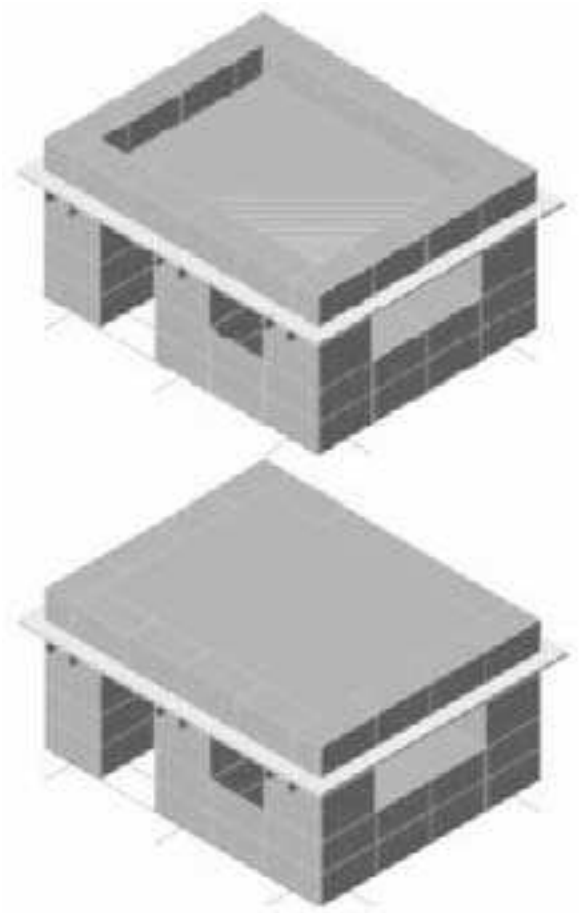


Figure 8-85. Artist concept of construction of overhead protection layer.

- ☐ Materials required: (8) - 2'x 8'x 2' metal revetment kits.
- ☐ Place 2-ft-high revetments around perimeter of roof as shown above.
- ☐ Allow 1ft clear space around each side.
- ☐ Fill revetments with infill material.
- ☐ Lightly compact infill material.
- ☐ Fill area inside revetments with infill material.
- ☐ Lightly compact infill material.

Performance against Weapons Effects

Results of static and live-fire tests conducted by ERDC have shown that this bunker design will protect from direct hits of 82 mm and 120 mm mortars (Figure 8-86) and near-miss (4 ft) of 122 mm rockets with no significant structural damage and no penetration of fragments through the sidewalls or roof.

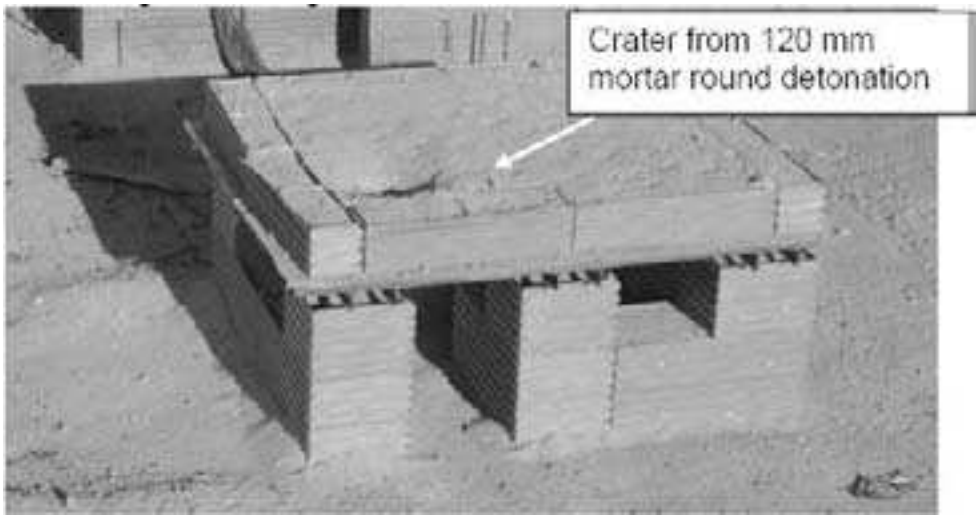


Figure 8-86. Damage to roof from direct hit of 120 mm mortar. No damage inside.

ADDITIONAL FIGHTING/OBSERVATION POSITIONS

Hescos and Metal Bin Revetments can be used to construct other fighting and observation bunkers that are similar in design and construction to the Large Observation Post. Examples are shown in Figures 8-87 - 8-89. Additional details are given in the JFOB CD and in the JAT Guide. Similar versions of these positions can be built with a stringer (timber) roof, landing mat, or sheet pile roof.

ABOVEGROUND TWO-BAY FIGHTING POSITION

Figure 8-87. Aboveground two-bay fighting position

Bill of Materials

The materials required to construct this position are available in a pre-assembled package under the NSN 5680-01-501-1357. If the materials are not ordered as a package, a listing of the BOM and associated NSNs is given in Table 8-20.

Table 8-20. BOM for Aboveground Two-Bay Fighting Position

Item Description	NSN	Quantity
Concertainer® – 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Beige/Sand	33
Composolite® panels, 14 ft long	5675-01-500-2808	6
Composolite® panels, 12 ft long	5675-01-500-2803	3
Toggle connectors, 14 ft long	5675-01-500-2808	5
Waterproof membrane (14 ft x 12 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	30

Aboveground Single-Bay Fighting Position

Figure 8-88. Improvised above-ground, single-bay fighting position with Composolite® roof

Bill of Materials

The materials required to construct this position are available in a pre-assembled package under the NSN 5680-01-501-1235. If the materials are not ordered as a package, a listing of the BOM and associated NSNs is given in Table 8-21.

Table 8-21. BOM for Improvised Aboveground Single-bay Fighting Position with Composolite® Roof

Item Description	NSN	Quantity
Concertainer® – 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 – Beige/Sand	23
Composolite® panels, 14 ft long	5675-01-500-2808	2
Composolite® panels, 8 ft long	5675-01-500-2729	7
Toggle connectors, 8 ft long	5675-01-500-2729	6
Waterproof membrane (8 ft x 14 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	20

SMALL OBSERVATION POST

Figure 8-89. Small observation post

Bill of Materials

The materials required to construct this position are available in a pre-assembled package under the NSN 5680-01-501-1462. If the materials are not ordered as a package, a listing of the BOM and associated NSNs is given in Table 8-22.

Table 8-22. Bill of Materials for Small Observation Post

Item Description	NSN	Quantity
Concertainer® – 2 ft high, 2 ft wide, 4 ft long	5680-99-001-9397 – Green 5680-99-968-1764 –Beige/Sand	30
Composolite® panels, 12 ft long	5675-01-500-2803	4
Composolite® panels, 8 ft long	5675-01-500-2729	3
Toggle connectors, 12 ft long	5675-01-500-2803	3
Waterproof membrane (8 ft × 12 ft)	5650-01-504-5373	1
Concertainer® infill material, cubic yards	Not applicable	24

USE OF EXISTING BUILDINGS

(Note: this information is taken from a draft unified facilities criteria (UFC) on retrofit of existing buildings being produced by the Air Force Civil Engineer Support Agency AFCESA)

Many times a JFOB may make use of existing conventional buildings for housing, office space, AAFES facilities, MWR, etc. However, in most cases these buildings do not provide acceptable levels of protection (LOP) from blast from VBIEDs or overhead protection from RAMs. Table 8-23 can be used as an aid to decide what level of protection is acceptable for the VBIED threat.

Table 8-23. Damage Estimated at Different AT Protection Levels

Level of Protection	Potential Damage to Building	Potential Door and Window Hazards	Potential Injury
Below AT standards	Severely damaged. Frame collapse/ massive destruction. Little left standing.	Doors and windows fail and result in lethal hazards.	Majority of personnel in collapse region suffer fatalities. Additional fatalities in other areas likely.
Very Low	Heavily damaged – onset of structural collapse. Collapse of masonry walls and debris thrown into building.	Doors and windows fail and result in severe hazards.	Majority of personnel suffer injuries, most in the minor to moderate range. A number of serious injuries and fatalities will likely occur.
Low	Damaged – unrepairable. Major deformation of walls, some walls may collapse.	Glass breaks and creates moderate hazard. Doors fail but present minimal hazard.	Majority of personnel suffer minor to moderate level injuries. A few serious injuries and fatalities are possible.
Medium	Damaged – repairable. No walls collapse. Minor debris hazard. No permanent damage to structural members.	Glass breaks but does not present a significant fragment hazard. Doors stay in frames, but will not be reusable.	Some minor injuries, but fatalities unlikely.
High	Superficially damaged.	Glazing will not break or present only minimal hazard. Doors will be reusable.	Only superficial injuries are likely.

Assuming that a berm or some perimeter wall is in place and is capable of stopping fragments from VBIEDs, the Table 8-24 provides an estimate of level of protection vs. standoff for different size vehicle bombs provided by typical Iraqi, low-rise (1 to 3 story), unreinforced masonry buildings. Note: This table assumes the building has a reinforced concrete or masonry frame for structural support and small (app. 2 ft by 4 ft, 1/4-in.- thick windows). If the building is of load-bearing wall construction, it should not be used to house assets. For more precise estimates of standoff, more refined tools such as AT Planner or BEEM can be used.

Table 8-24. Standoff Distances

VBIED Explosive Weight (lb)	Standoff Distance Needed for Specified Level of Protection (ft)				
	High	Medium	Low	Very Low	Below AT Standards
50	205	145	115	90	20
220	340	260	195	165	56
500	450	350	270	230	100
1000	630	465	375	310	150
4000	1130	780	585	510	320
40000	3000	2100	1620	1520	820

If the existing level of protection 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. The following retrofit techniques for masonry walls can be used, depending on the particular building and situation. CAUTION: Before proceeding with any of these options, engage structural engineers to provide detailed designs. In addition, these retrofits apply only to the walls of the structure. Windows and doors will still fail at most of these standoffs and create a hazard. Locate personnel away from these areas and, where possible, remove windows and board up openings.

HIGH CAPACITY WALL CATCHER SYSTEM

Description: The High Capacity Wall Catcher System (see Figure 8-90 below) is an aggressive retrofit concept designed not to strengthen the wall but rather 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 is completely covered by the plate, including the windows (if any).

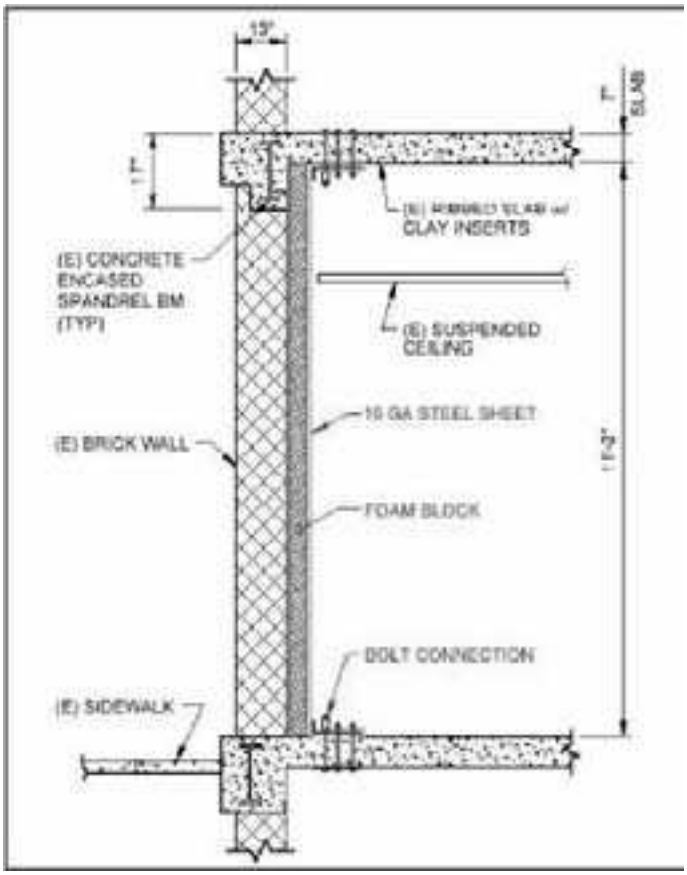


Figure 8-90. Schematic of High Capacity Wall Catcher System

Applicability: 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.

Level of Protection: Tests conducted with 500 lb of ANFO at a standoff of 8 ft showed this retrofit capable of providing a medium level of protection. Extrapolation of this data to other explosive weights is given in Table 8-25.

Table 8-25. Standoff Requirements for All Other Systems for Different VBIED Sizes

VBIED Equivalent TNT Explosive Weight (lb)	Standoff needed to provide Medium Level of Protection (ft)
50	3
220	6
500	10
1000	13
4000	33
40000	108

GEOTEXTILE FABRIC CATCHER SYSTEM

Description: A curtain of geotextile fabric (see Figure 8-91 below) 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.

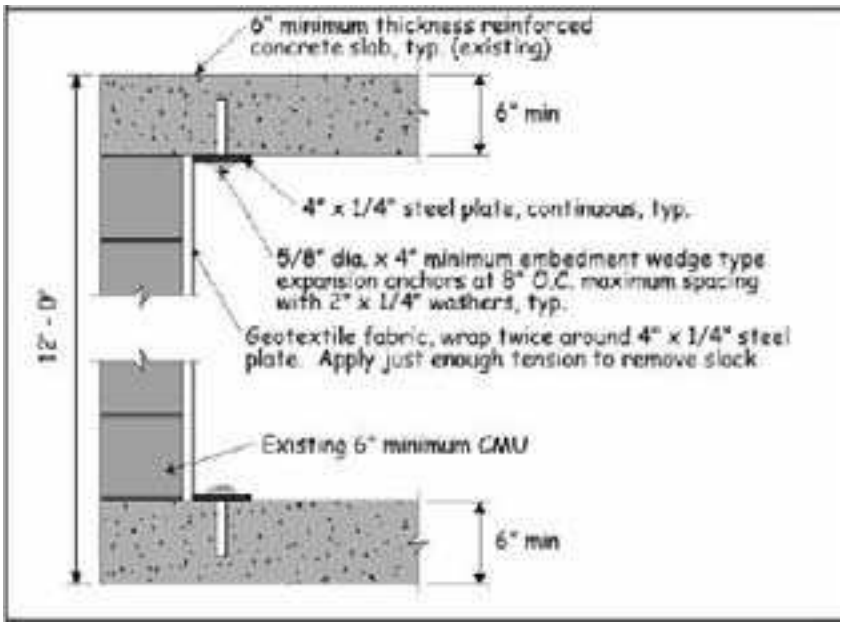


Figure 8-91. Geotextile fabric catcher system

Applicability: This retrofit is applicable to unreinforced, concrete masonry infill walls. It is not applicable to walls with windows, as the fabric must span continuously from floor to ceiling without interruption, nor is it an aesthetically pleasing solution. DO NOT USE it for load-bearing wall structures.

Level of Protection: Table 8-26 presents the standoff information for this retrofit. 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.

Table 8-26. Standoff Requirements for Geotextile Fabric Catcher System for Different VBIED Sizes

VBIED Equivalent TNT Explosive Weight (lb)	Standoff needed to provide a Medium Level of Protection (ft)			
	Type of Fabric			
	Comtrac R500	HS 1715	HS 800	UK Aramid
50	15	18	23	26
220	34	41	56	69
500	61	71	92	110
1000	92	110	151	171
4000	215	271	342	400
10000	902	1100	1400	1700

POLYMER RETROFIT SYSTEM FOR MASONRY

Description: 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 event, the polymer material remains intact and contains the debris. Figure 8-92 shows frames from high-speed videos of the blast response of a normal masonry wall and one coated with polyurea. 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 8-93). The other is a "trowel-on" system (see Figure 8-94).

a. Hazardous debris, normal wall b. Polymer coating catches wall debris

Figure 8-92. Blast response of masonry wall.

Figure 8-93. Spray-on polymer retrofit system

Figure 8-94. Trowel-on polymer retrofit system

Applicability: This retrofit is applicable to unreinforced concrete masonry infill walls. It should not be used for load-bearing wall structures. Wall penetrations (e.g., doors and windows) are permitted but must be carefully tied into the polymer coating.

Level of Protection: Table 8-27 presents the standoff criteria for this retrofit. The criteria were developed by analytical methods and verified by comparison with experimental results to give 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.

Table 8-27. Standoff Requirements for Polymer Retrofit System for Different VBIED Types

VBIED Equivalent TNT Explosive Weight (lb)	Standoff needed to provide Medium Level of Protection (ft)
50	17
220	41
500	62
1000	90
4000	180
40000	492

REFERENCES

FM 5-103. *Survivability*, 10 June 1985. (Available from www.train.army.mil)

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

UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings*, 8 October 2003.

UFC 4-023-02 (Draft). *Security Engineering: Structural Design To Resist Explosive Effects For Existing Buildings*, April 2005.

Appendix 2 to Annex V to USCENTCOM OPORD 97-01B (Antiterrorism). *Antiterrorism Construction Standards*, 4 January 2002.

The following references are from the Survivability Engineering Branch, Geotechnical and Structures Laboratory, U.S. Army Engineer Research and Development Center and most can be accessed via the ATEP (https://atep.dtic.mil) or in the JAT Guide Reference section (https://atep.dtic.mil/jatguide/JATGuide/4_Resources/index.htm):

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. Basecamps, 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.

This page intentionally blank

Chapter 9

INCIDENT RESPONSE AND CONSEQUENCE MANAGEMENT

Contents

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 JFOB to full operational capability

Standard actions the JFOB should have the capability to perform are as follows:

- Establish command and control at the incident site. Establish an on-scene commander who coordinates all activities at an incident site through an Incident Command System (a systemic procedure whereby JFOB staffs are organized to provide response to an incident). A typical installation response team should be task organized to respond to all incidents regardless of threat, tactic, or event.
- Perform a tactical appraisal of the situation.
- Prepare a damage and casualty assessment.
- Take immediate actions to save lives, prevent suffering, or mitigate great property damage.
- Determine a priority of response effort and subsequent order for follow-on response forces, equipment, and supplies.
- Establish staging bases where forces and equipment can be located to support an incident.
- Establish mass casualty/care/evacuation centers.

Five phases of IR which are under the control of the base defense operations center (BDOC) are as follows:

- **Preparation.** The pre-strike phase that focuses on identifying mission essential vulnerable areas (MEVA), developing IR 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.

Each phase of the operation is coordinated with the BDOC where actions are coordinated with the battle staff.

PREPARATION PHASE

JFOB 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.

Common Participants

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 (see Figure 9-1). 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 to the incident site.
- Search and Rescue Teams. These teams usually work in pairs and are responsible for casualty extraction. A structural engineer on the team can conduct safety and damage assessment.

- EOD. The EOD Team is responsible to detect, identify and render safe any suspected munitions and to look for secondary devices.

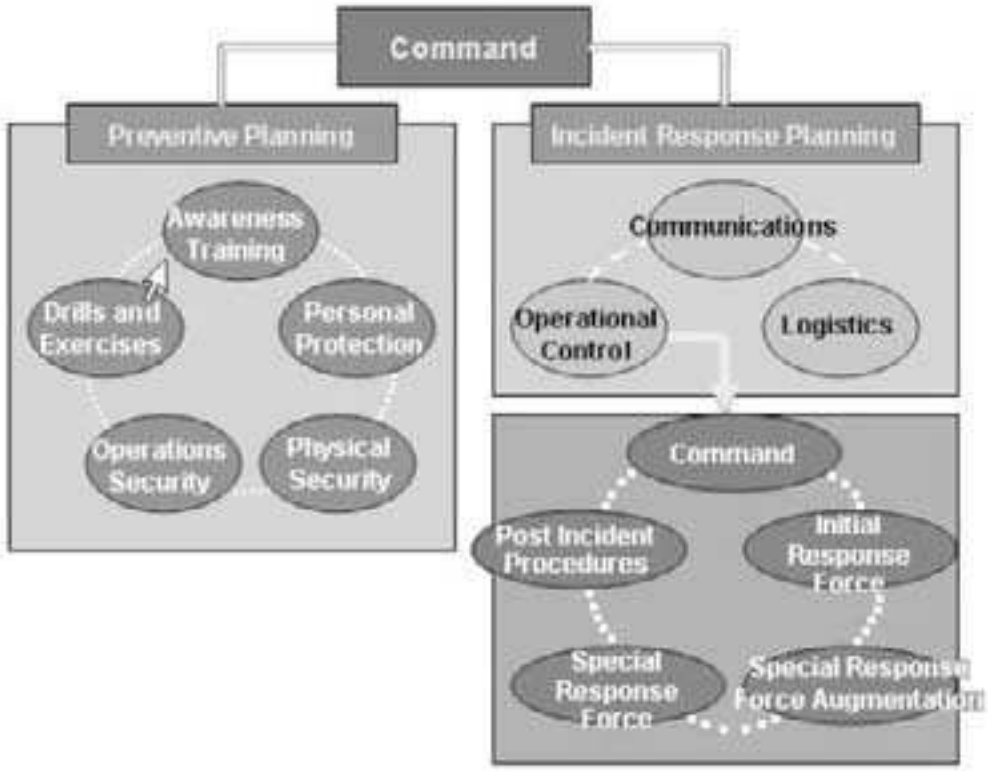


Figure 9-1. Antiterrorism Program Functions for JFOB Commanders

Incident Response Equipment

During the planning process, equipment that will be utilized during the IR process will be identified. This equipment includes:

- Weapons
- Communication Systems
- Ambulances
- Fire Trucks
- Rescue Vehicles
- Extraction Equipment (Jaws of Life, Extraction Equipment, Ropes, Block & Tackle)
- Construction Equipment (HYEX, Bulldozers)
- Barriers
- Aviation Assets
- EOD assets.

Incident Response Preparation

During the preparation phase, the JFOB should be organized to ensure optimum reactions and control of incidents. Actions to be carried out during the master planning and construction of JFOBs are as follows:

- Ensure forward operations base (JFOB) streets are named and are wide enough to accommodate emergency vehicles.
- Establish designator numbers for all JFOB buildings.
- Establish a specific frequency/land line number for emergency incidents within the JFOB.
- Develop "Big/Giant Voice" communication systems to warn or advise of emergency situations.
- Erect fuel points/farms with a 25 m standoff from any occupied building or personnel staging area.
- Establish barrier wall containment for critical structures; i.e. fuel farms, dining facilities (DFACs), latrine/shower areas, PX, bed-down areas, bus stops, and chapels.
- Establish access control at the entrance to include separate check points for identification and contained search areas.
- Establish inner layer security zones for staging areas for incoming material shipments to be staged.
- Establish an Incident Response Center (IRC) with supporting staff and communication resources.
- Implement escort procedures for all extraneous personnel conducting business within the JFOB.
- Establish quick reaction force (QRF) controlled by the BDOC to react to emergency incidents.
- Establish emergency vehicles/ambulances with fire extinguishers, litters, extraction tool sets, bolt cutters, barrier materials, and first aid kits.
- Designate, train and equip Combat Lifesavers for IR within the JFOB.
- Prepare and post "ACTIONS TO TAKE IN CASE OF AN EMERGENCY" instructions in conspicuous areas (bulletin boards) of the JFOB.
- Train and equip the QRF to defeat up to a Level II threat.
- Designate a commissioned officer or a non-commissioned officer (E-7 or above) as the JFOB AT Officer.
- Conduct IR training exercises to validate plans and procedures.

RESPONSE PHASE

Initial Response Force

- Immediately identifies and reports the nature of the situation.
- Isolates the incident, and contains the situation until relieved by the reaction force commander.
- Ensures that no one enters or leaves the area.
- Tries to locate witnesses and directs them to a safe location for debriefing.
- Is prepared to interface with HN police or military forces that may also be responding to the incident.

Base Defense Operations Center (BDOC)

- Ensures security personnel establish traffic control points (TCP) to control access into and out of the site.
- Determines the need to activate the Incident Command System based upon casualties, infrastructure damage, and degradation of the entry controlled point (ECP).
- Determines the need to evacuate or protect in place personnel in and adjacent to the incident site.

OCCUPATION PHASE

The BDOC's decision to activate the ICP is based upon the magnitude of the incident. Thereafter, the BDOC is responsible for:

- Dispatching the Incident Site Commander to the ICP.
- Commanding the overall JFOB, allowing the ICP to control the area of the incident
- Dispatching the medical regulating officer to assess the situation and the need for additional medical materials and personnel. Additional asset requirements are coordinated through the ICP.
- Coordinating any additional fire and rescue assets if required.
- Coordinating any EOD, mortuary, and chaplain services required.

SUPPORT PHASE

Second Response personnel report to the ICP in order to receive situation updates and take direction for emergency operations. The following actions are completed:

- Senior fire/rescue personnel arrive and direct fire fighting operations and serve as liaison officer to the ICP.
- Medical personnel respond to the incident site as required.
- BDOC increases the base security posture as required and deploys the QRF.

- The Combat Support Hospital (CSH) alerts and mobilizes medical response teams as required to the site and initiates the mass casualty plan as required.
- The Operations, Plans, and Training Staff (G3) coordinate the disconnection of power and water as required and coordinates resource support.
- Structural damage is assessed and a recovery action plan is initiated.
- PAO prepares media operations to receive visitors and collects information for an initial statement to the media.
- Additional water distribution points may be opened to provide water support for fire fighting vehicles as required.
- All personnel are accounted for and the status is reported to the BDOC.
- The BDOC coordinates off-post operations and establishes a marshalling point for rescue vehicles.
- Civil Affairs coordinates the treatment of Local Nationals (LN) with the Ministry of Health officials and prepares to receive local family members.

RECOVERY PHASE

The following actions are completed during the Recovery Phase:

- Engineer support is dispatched as required to assess and support recovery operations.
- G3 provides emergency purchase requests in support of the recovery operations and coordinates all movement of recovery assets with the BDOC.
- G3 compiles a list of equipment required to establish essential services and submits for purchase.
- Civil Affairs coordinates with the BDOC and LN for recovery of LNs as required.
- MEDEVAC is organized if required.

SPECIALIST CAPABILITIES

Fire Fighting

The JFOB firefighting capability will support the JFOB Commander by providing immediate response to fire, bomb, and medical emergencies. The JFOB Fire Department provides the following services:

- Immediate emergency medical response
- EOD/bomb threat remediation
- Structural inspections for fire safety for all buildings located within the JFOB in accordance with the National Fire Protection Association (NFPA) code
- Fire safety education

- The elimination or reduction of the fire threat to personnel, aircraft, and facilities.
- The defense of fire protection resources.
- Post attack suppression and rescue response to fire incidents that may jeopardize the combat capability of the JFOB.

Fire protection consists of many interdependent elements that contribute to the survivability and operability of the fire fighting force. Elements include:

- Crash and structural rescue operations.
- A sufficient number of trained and capable firefighters.
- Ancillary equipment, including proximity suits, self-contained breathing apparatus (SCBA), a recharging apparatus for SCBA, chemical warfare defense equipment (CWDE), mobility gear and weapons.
- Consumable materials such as water, Class A&B foam, and breathing air.
- Base station, mobile and portable communication units.
- Essential support services to include vehicle maintenance, spares, fuel, and food service, medical re-supply facilities and utilities.
- Adequate training in contingency skills, priorities, tactics, strategies, and procedures.

Planning

Effective planning is essential for the success of the fire fighting capability of the JFOB. A comprehensive understanding of what is required must be communicated by the commander. As a minimum, fire fighters shall do the following:

- Survey water supplies for use during the pre-attack phase to include on-base and off-base sources. Examples of these resources may include swimming pools, reservoirs, tankers, pumps, wells, storage bladders, and mobile water distribution systems.
- Construct expedient access routes to auxiliary water resources as required.
- Establish a system of pumps, hoses and support equipment to supply water where hydrants are not available.
- Survey the JFOB terrain for naturally protected areas for fire vehicles, chemical agents, equipment, and personnel. Utilize natural terrain features such as ditches, hillsides and trenches combined with camouflage for concealment.
- Identify locations where expedient construction can be used to provide protection for fire vehicles, agents, and personnel. Provide sandbags needed to construct expedient protective facilities, including the use of earthen berms.
- Ensure petroleum, oil, and lubricants (POL) storage points have adequate facilities to prevent spillage from endangering other tanks. Establish tank

drainage diversion areas where spilled fuel can burn without endangering other critical fuel supplies.

- Establish firefighting procedures for a chemical warfare environment. Inventory fire suppression agents, critical equipment, and supplies. Backfill shortages to standard.
- Ensure vehicle spare parts and tires are available and protected. Fire protection vehicles will be to 10-20 standards with priority for maintenance.
- Locate firefighter housing, feeding procedures, rest and relief areas within dispersion areas. Establish duty hours and shift changes.

Constraints. Firefighters will encounter the following conditions during a wartime environment.

- A lack of CWDE equipment.
- A lack of adequate water supply.
- Unarmored fire trucks.
- Inadequate firefighting material to extinguish large totally involved fires such as large frame aircraft and POL tanks.
- An adequate number of firefighters to fight extended fires in a continuous operation.
- Extreme climatic conditions.

MEDICAL SUPPORT

Medical forces support military operations that range from humanitarian missions to force protection (FP) to high intensity conflict. Medical planning, command, control, communications and computers (C4), air-medical evacuation, medical logistics, HN support, environmental concerns, preventive medicine and humanitarian civic programs within the JFOB are part of the Health Service Support (HSS) mission of the JFOB.

The HSS concept of operations establishes conditions to deploy and sustain a healthy and fit force. This accomplishment requires a responsive medical surveillance system to maintain health and combat effectiveness as well as to simultaneously prevent casualties.

Services

The HSS encompasses the promotion of wellness and preventive, curative, and rehabilitative medical services. It is designed to maintain a healthy, fit force and conserve the force's strength. The effectiveness of the HSS system is focused and measured on its ability to do the following:

- Provide prompt medical treatment consisting of those measures necessary to recover, resuscitate, stabilize, and prepare patients for evacuation to the next level of care.
- Employ standardized air and ground medical evacuation units/ resources. The use of air ambulance is the primary and preferred means of medical

evacuation on the battlefield. Its use is METT-T driven and can be affected by weather, availability of resources, NBC conditions and air superiority issues.

- Establish Preventive Medicine Programs (PVNTMED) to prevent casualties through medical surveillance health assessments and personnel protective measures.
- Provide advice to the JFOB commander about significant health risks to the deployed force and the recommended interventions needed to prevent exposure and protect the health of the force.
- Perform disease outbreak investigations and develop intervention recommendations.
- Provide rapid detection and identification of chemical warfare agents, toxic industrial chemicals in soils, water and air samples.
- Provide dental care to maintain the dental fitness of the force.
- Provide combat operational stress control (COSC)/mental health (MH) to enhance the unit and soldier effectiveness through increased stress tolerance and positive coping behaviors.

Constraints

Medical support requires base operating support (BOS) for logistic support and site preparation, utilities, communications, equipment transportation, POL, consumable re-supply, messing and berthing, financial and fiscal support administration and personnel security.

- Effective lines of communication are required for both in theater and communicating back to the Continental United States (CONUS). Reporting requirements IAW the operations order (OPORD) will be followed.
- The medical facility is dependent upon reagent quality water, electrical load, refrigeration, and a responsive re-supply system. The logistics/ administrative component will plan and coordinate with BOS to assure the mission requirements.
- Troop, organization, and equipment (TOE) vehicles are required for task organization for administrative and logistical functions. Medical facilities will be accessible by air and ground transportation for the purpose of sending and receiving samples from the Theater of Operations.

QUICK REACTION FORCE (QRF)

QRFs are identified, trained, and equipped to support the security of JFOBs. Typically, the QRF is designed to defeat Level II threats. The specific organization and planning requirements are driven by mission, enemy, terrain and weather, troops available and civilian (METT-TC) and must be continuously reassessed. The QRF may be attached or assigned but is normally under operational control (OPCON) to the BDOC commander.

The QRF is 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. Minimum QRF size is three high mobility multipurpose wheeled vehicles (HMMWVs) with basic load of ammunition.

Training

The QRF develops and implements battle drills to defeat Level II threats in their area of responsibility. Examples of Level II threats and QRF responses include but are not limited to the following:

Indirect fire. QRF finds impact site, secures impact site, reacts to unexploded ordnance (UXO).

Enemy attack. (Breach in perimeter, sniper, VBIED inside the base). QRF responds to suspicious vehicles or personnel and protects a MEVA (evacuate and cordon, provide external security, react to hostage).

Additionally, 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.
- 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.
- Enemy prisoner of war (EPW) procedures.
- Coordination. 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 SOP.

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 (N) 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 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 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.

CONSEQUENCE MANAGEMENT SCENARIOS

- IED detonated at the ECP or nearby
  - Explosive devices may contain anti-personnel features such as nuts and bolts or ball bearings.
  - Explosives may produce secondary hazards such as unstable structures, damaged utilities, hanging debris and other physical hazards.
  - Multiple IEDs may be used in one attack.
  - Explosive devices may be designed to disseminate chemical, biological, radiological (CBR) agents.
- Weapons of Mass Destruction (WMD) attack.
- HAZMAT - industrial chemical spill as a result of accident or enemy action.

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, MWD).
- 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-lacrimination-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.
  - Structural Damage
  - Utility Damage
- Weather Considerations
  - Downwind Exposure
  - Monitor weather forecast
- Psychological Effects
  - Long-term stress on Soldiers
  - Fear Factor

REFERENCES

SWEAT/IR BOOK. The U.S. Army Engineer School has published a reference titled "SWEAT/IR Book Version 2.1 Infrastructure Reconnaissance" that is an excellent reference for infrastructure inspection and resourcing. This book is a result of work by the Engineer School, the U.S. Military Academy, the Engineer Research and Development Center and countless MTOE units operating in Iraq and Afghanistan. The SWEAT Book consists of infrastructure categories identified by smart card form developed by the Engineer School. The SWEAT/IR Book can be accessed through AKO through the "groups" folder under the "general engineering" site. The link https://www.us.army.mil/suite/kc/4571701 will access the General Engineering-USAES page. Choose the "Infrastructure (i.e.-SWEAT) file on this page. This book is a functional tool that is available and should be utilized.

Consequence Management by Scott R. Taylor, Amy M. Rowe and Brian M. Lewis

4th Marine Expeditionary Brigade (AT) ESG 35 Consequence Management

Third Air Force Instruction 10-245 16 February 2004 Air Force AT Standards

Air Force Capability-Based Medical Planning LTG George Peach Taylor, Jr.

Concept of Operations for the Forward Deployable Preventive Medicine Unit 14 June 2005

Fundamentals of Force Health Protection in a Global Environment

Correlating Medical Forces Forward by J. H. Binford Peay III

Chapter 4-Wartime Operations http://ataiam.train.army.mil

Standard Operating Procedures-Version 3-Victory Base Complex-Iraq

This page intentionally blank

Chapter 10

COMMUNICATIONS (COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS-C4)

Contents

INTRODUCTION

Command, Control, Communications and Computers (C4) is the joint terminology for those information systems that enable leadership to effectively manage their areas of responsibility. JFOB FP C4 systems focus on the networks that allow voice and data communications among command posts, staffs, and critical components of the FP activities. C4 systems enable commanders and staffs to effectively manage ongoing operations. Without a reliable, redundant means of communicating threat status, intelligence, and operations, the JFOB 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.

This chapter will focus on the C4 basic requirements, characteristics and considerations required to maintain minimum operations.

Communications components are the hardware (radios, telephones, computers) and software (operating systems, service specific operating systems, associated data networks) used to send and receive messages for a variety of purposes to accomplish the mission.

PURPOSE OF FORCE PROTECTION (FP) C4 SYSTEMS

The primary purpose of FP communications systems is to provide commanders and staffs, as well as the resident organizations within the JFOB, the capability to communicate requirements, intelligence and situational updates among their respective sites. It must encompass organizational operations centers and those teams and posts essential to FP.

Examples of FP activities that C4 supports include:

- Maintain vigilance against insurgent attack
- Report status of teams and organizations
- Sound alarms
- Request assistance from fire, medical or other emergency response resources
- Call for rapid response forces (quick reaction forces), close air support or fire support
- Direct counterstrikes
- Coordinate incident response and consequence management tasks

CHARACTERISTICS OF FP C4 SYSTEMS

A JFOB C4 system is composed of multiple systems and must be capable of simultaneous, real time or near real time communications among defense units, staff elements, headquarters, and operations centers. It must allow for immediate and continuous access to the base defense operations center (BDOC) by sector command posts, mobile reserve, patrols, and critical defense positions. Additionally the C4 systems should allow continuous access by the BDOC to the base operations center, rear area operations center, rear tactical operations center, coalition, and host nation (HN) forces as well as access by supporting intelligence/counterintelligence, fire support and air defense units.

The JFOB C4 system architecture must also possess the following minimum characteristics:

- Secure. The system must be able to restrict unauthorized monitoring and access to prevent information from being provided to unauthorized personnel. The JFOB commander, force protection officer and communications/C4 officer must insure that all systems meet all guidance from higher headquarters commands regarding policies on encryption. Unauthorized personnel must not be allowed access to information over the systems.
- Robust. The systems must be able to withstand both the natural and man made interference that may be in the area. Weather (heat, cold, rain, etc) can dramatically impact radio systems and this impact must be evaluated prior to establishing the systems. Man made factors such as interference created by urban areas, high tension power lines, commercial radio transmitters, cell phone towers and interference from radar and directional systems will impede communications and must be identified

and factored into the plan prior to system establishment. Additionally, the system must be developed to withstand a single point of failure brought on by enemy attack.

- Redundant. To be robust, a system must have a duplicate and offer multiple links. Reliance on any single form of communications (radio, telephone, data, etc) will not support the commander's requirements. Every JFOB should have a minimum of three alternate means of communications. Each should be properly identified as primary, secondary and tertiary that work as fail-safe systems in the event of a major attack or loss due to weather or interference. These three systems must be separate in type so as not to be impacted by the same event.
- Reliable. Systems must be dependable. Use of both commercial-off-the-shelf (COTS) communications technology and DOD-provided systems is the norm but each system and network must be researched as to its specific reliability. Systems with low mean time between failure or limited capabilities must not be relied on as key systems. Additionally, periodic and thorough maintenance of all systems must be directed and properly conducted to ensure system stability.

JFOB C4 CONSIDERATIONS

PLANNING

Pre-execution planning is essential to the successful installation, operation, and maintenance of JFOB force protection C4 systems. The force protection officer and the communications/C4 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 JFOB communications, the communications/C4 officer and the antiterrorism/FP 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), 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/C4 officer must develop signal operating instructions and communication plans and disseminate them to tenant and supporting units. JFOB Communications plans must be integrated into the Joint Communications Electronic Operating Instructions to ensure de-confliction of frequencies and call signs. Additionally there must be coordination with HN, Coalition Forces, and transient units to ensure interoperability and C4 effectiveness.

The following list of considerations should be addressed in all C4 plans at a minimum:

- Requirements. The actual C4 requirement must be understood and assessed for feasibility. Requirements must be based on need - not want. Fiscal limitations will prevent the acquisition of state of the art systems used by commercial and most stateside garrison organizations. The JFOB FP officer must work with the communications/C4 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. 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 JFOB. 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 C4 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 FP 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. C4 system components such as cables, wires, antennas, and generators are particularly susceptible. C4 planners can minimize this vulnerability by planning for hardening and/or providing alternate wire/cable routes for key C4 assets.
- Flexibility. As in any plan, C4 system architecture must be flexible. Rigid reliance on a single means, capability or concept will be counter effective. As previously stated, a minimum of three means should be developed for each requirement. The systems identified may have multiple uses but must be both capable and available to meet their primary mission.

- Interoperability. Interoperability of C4 systems is currently one of the major ongoing programs within the DoD. JFOB C4 system planners must include this capability as a key point in their planning. The capability for interoperability allows mult-functionality for a single system which both decreases the overall equipment requirement and increases capabilities for users. Understanding the frequency spectrums utilized and computer/network operating system capabilities and limitations can allow enhanced interoperability within the JFOB C4 architecture. Full interoperability may not be achievable; however, full interoperability will remain a goal within the joint community until the services identify and procure C4 systems that provide the myriad of capabilities required by each specific service.

EQUIPMENT

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 JFOB 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 FP C4. Frequencies, bandwidth and range considerations must all be identified for any radio system utilized. All frequencies used must be approved and directed by the JFOB 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 JFOB. 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 not utilize telephone systems for sensitive FP information 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 a BDOC 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.

JFOB C4 NETWORK CONSIDERATIONS

The following are recommended requirements for JFOB FP C4 systems:

Security Forces. The JFOB security forces (SF) require radio systems that allow continuous secure communications with the BDOC at all times despite net saturation, jamming, or interference. A minimum of three frequencies should be available to the SF. Additional frequencies may be required depending on the specific mission and JFOB. SF radio systems include the following components:

- Base Stations. Fixed two-way radios, usually located in control centers.
- Base Station Remotes. Fixed two-way radios installed on fixed posts. Remotes are basically amplifiers connected to the base station with telephone lines. They use the base station to send and receive calls.
- Mobile Two-Way Radios. These devices are usually installed in SF vehicles. These radios transmit and receive over great distances in dispersed situations. Some models can be easily removed from vehicles, making them mobile-portable radios.
- Portable Radios. Two-way radios, used on walking patrols, special response teams (SRTs) or the Quick Reaction Force (QRF), security patrols, and fixed posts. These radios transmit over short distances and are used for most normal day-to-day operations.

JFOB Tenant Units. The tactical command post for each tenant unit/organization within the JFOB must have the capability to communicate with the BDOC at all times. Although tenant units may provide forces to or in support of the SF, the C4 requirements are different. A separate radio net (minimum of two secure frequencies to allow for potential disruption) that uses base stations or other fixed station two-way radios should be available as the BDOC Command net. Additionally, the use of both telephone systems and computer data systems should be used to maximize “ordinary” traffic, allowing the radio net to be available for critical missions only. Units must devise manual systems at each installation with protection level resources to back up the radio and landline systems.

Supporting Units. The BDOC requires an immediate communications capability with supporting organizations such as medical/medevac, intelligence/counterintelligence, fire support and air defense units. Secure radio

systems should be used as the primary means if the requirement exists for instantaneous communications while telephone systems and computer data networks can be used for less critical communications. Usually medical/medevac, fire support and air defense units have dedicated radio frequencies provided by the theater and/or JFOB Communications office. A back up system must be available to back up the radio and landline systems.

Backup Systems. The primary backup system is comprised of telephone systems that are either installation or tactical. The telephone system provides lines for calling on and off the installation, connection of special (hot) lines, lines for fixed posts, and DSN capability. Tactical systems are service-provided phone systems that are normally manually operated to provide service to stations connected to the system. The secondary backup system is comprised of manual signal techniques. These signals include hand and arm signals, flashlights, flares, smoke grenades, or sounds, and are normally directed in the Joint Communications- Electronics Operating Instructions (JCEOI) A tertiary backup system is the messenger. Although normally less time responsive than radio, telephones or data, the messenger is also the most secure means of communicating information.

NETWORK OPTIONS

The following units should operate stations in the base defense network:

- Base Operations Center and other command and control facilities.
- Base Defense Operations Center (BDOC).
- Fire support element (FSE) or Fire Support Coordination Center (FSCC).
- Defensive sector command post.
- Base observation posts (OPs), listening posts (LPs), and patrols.
- Base mobile reserve.
- Theater air control system.
- Base Combat Operations Center (BCOC).
- Nuclear, Biological, Chemical (NBC) air defense, and missile warning.
- Maritime and offshore defense force.
- Rear Area Operations Center (RAOC) and Rear Tactical Operations Center (RTOC).
- Response forces and Tactical Combat Force (TCF) or Incident Response Force (IRF).

Figure 10-1 provides a notional base defense communications network diagram. The figure shows that all communications go through the BDOC.

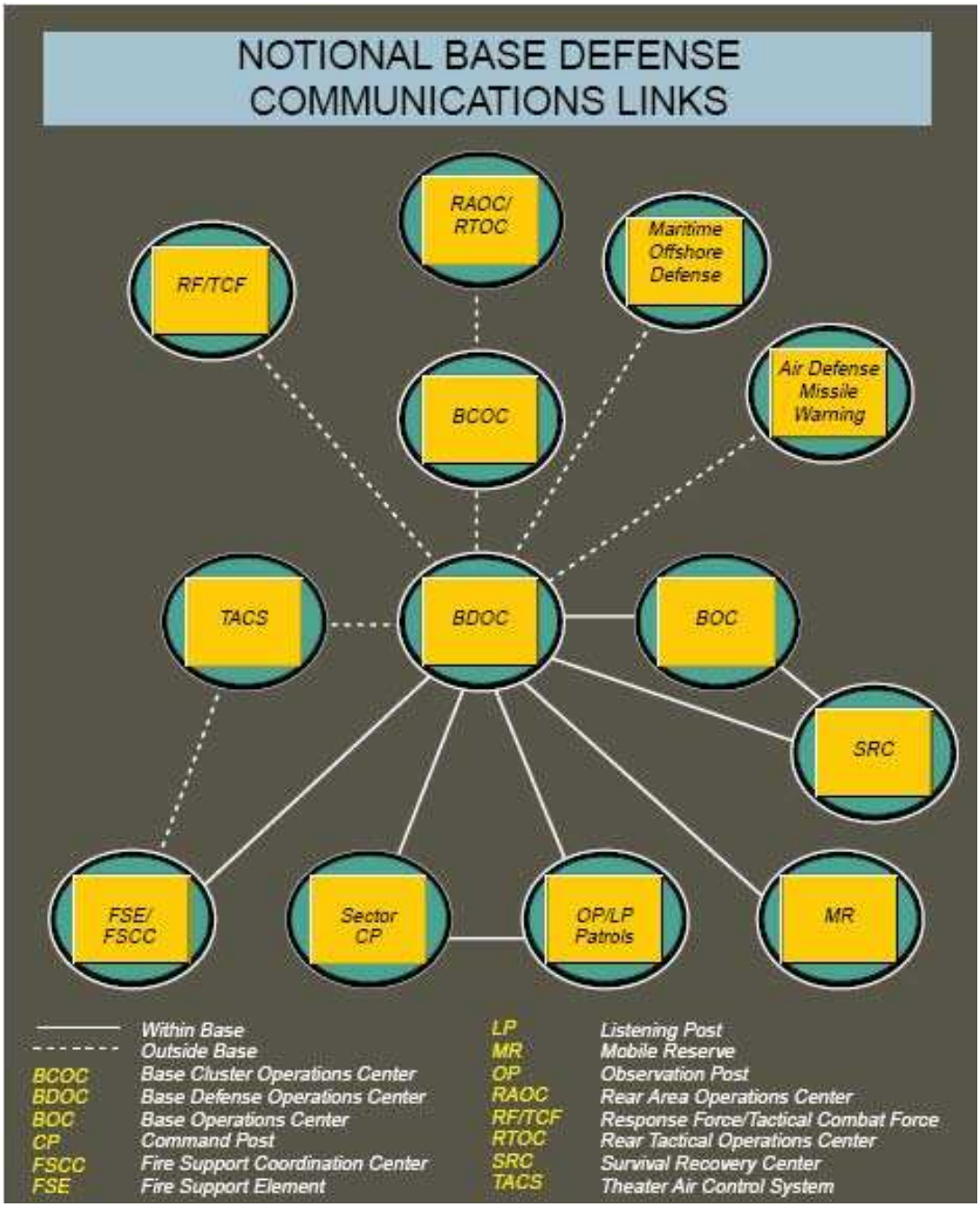


Figure 10-1. Notional Base Defense Communications Links

To enhance security at the JFOB, other locations should also have land-line links and computer network links for calls and messages in case of emergency as well as for everyday work use. These locations should also be able to hear Giant Voice broadcasts for emergencies as well. Examples of these locations are presented as a reminder in Table 10-1.

Housing	Dining facilities and other gathering locations	Solid, Medical, and Hazardous Waste Storage/Treatment/Pumping
Command Centers/Offices	Education Center	Guard Towers
Fuel Operations-Aircraft and Land Vehicles	Post Office	Entry Control Points
Vehicle Maintenance/Motor Pool/Wash Rack	PX	Detainee Facility
Medical-Clinic/Hospital	Barber	Perimeter sites with personnel
Morgue	Laundry	Snow removal
Kennel	Fire Department/Fire Fighting	Flight line
Warehouses and Storage	Fitness Center	Aviation Fuel, Maintenance, and Control Towers
Munitions Storage Area	Recreation locations: Community Center, Theater	Chapel
Roads/Streets (Dept. of Public Works/Civil Engineering) Offices	Defense Re-utilization Management Office	Utilities-Electric power production; water supply, treatment, and pumping stations; Natural gas supply and pumping; Propane storage and transfer

Table 10-1. Examples of Locations Requiring Land-lines or Computer Network Connectivity or Within Hearing Distance of Giant Voice/Public Address Systems

C4 SYSTEM PROTECTION

Common sense practices help protect C4 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.

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 C4 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. The processes of OPSEC are listed below.

Identification of critical information to be protected: Critical information constitutes the "core secrets" of the organization.

Analysis of the threats: Knowing who the adversaries are and what information they require to meet their objectives is essential in determining what information is critical.

- Analysis of the vulnerabilities. Determining the organization's vulnerabilities involves systems analysis of how the operation or activity is actually conducted.
- Assessment of the risks. Vulnerabilities and specific threats must be matched.
- Application of the countermeasures. Countermeasures need to be developed that eliminate the vulnerabilities, threats, or information to the adversaries.

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.

- Crypto security. The component of communications security that results from the provision of technically sound cryptosystems and their proper use. This type of security includes message confidentiality and authenticity.
- Emissions Security. Protection resulting from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto equipment, automated information systems (computers) and telecommunications systems.
- Physical Security. The component of communications security that results from all physical measures necessary to safeguard classified equipment, material and documents from access thereto or observation thereof by unauthorized persons.
- Traffic-Flow Security. Measures that conceal the presence and properties of valid messages on a network. It includes the protection resulting from features, inherent in some crypto equipment, that conceal the presence of valid messages on a communications circuit normally achieved by causing the circuit to appear busy at all times.
- Transmission Security. The component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g., frequency hopping and spread spectrum).

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 C4 planners, network managers, and system users. Service specific, theater and JFOB 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.

JFOB FP C4 CHECKLIST

GENERAL

- Has the FP officer coordinated FP/communications requirements with the JFOB Communications/ Information 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 FP 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 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 FP 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 JFOB 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 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 FP officer coordinated with the JFOB C4/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 FP 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.)?

REFERENCES

AF Handbook 31-305. *Security Forces Deployment Planning Handbook*, 26 February 2003

AFI 31-101. *Air Force Installation Security Program*,, 1 March 2003

AFI 10-400. *Aerospace Expeditionary Force Planning*, 16 October 2002

AFI 10-404. *Base Support and Expeditionary Site Planning*, 9 March 2004

AFMC Suppl 1 to AFI 10-404, 26 November 2001,

AFMC Sup 12 to AFI 10-404, 15 February 2002

AR 25-2. *Information Assurance*, 14 November 2003

AR 380-19. *Army Information Systems Security*, 27 February 1998

Communications Security Web Site at myWiseOwl.com (available at http://www.mywiseowl.com/articles/Communications_security)

DoD O-2000.12H. *DOD Antiterrorism Handbook*, February 2004

JP 3-10.1. *Joint Tactics, Techniques, and Procedures for Base Defense*, 23 July 1996

USCENTCOM Reg 415-1. *Construction and Base Camp Development in the USCENTCOM Area of Responsibility (AOR) - "The Sand Book,"* 1 December 2004

U.S. Department of Energy. *An Operations Security (OPSEC) Primer*, (available at http://www.defendAmerica.mil/articles/a021202b.html)

This page intentionally blank

Chapter 11

PRINCIPAL CRITICAL INFRASTRUCTURE ASSURANCE MEASURES

Contents

INTRODUCTION

Infrastructure in the Iraq Area of Operations (AOR) is very important to mission success. Infrastructure is built to operate in a peacetime scenario and is not normally hardened to protect from sabotage and deliberate destruction by anti-Iraqi forces (AIF).

Critical infrastructure assurance measures are implemented to assure that the JFOB will maintain operations during periods of heightened security and during attacks from rockets, artillery, mortars (RAMS), improvised explosive devices (IEDs) etc. This chapter will define the most critical infrastructure and methods of protecting it.

OBJECTIVES

- To protect people, physical entities and cyber systems that are survivable, continuity of operations and mission success.
- To deter or mitigate attacks on critical infrastructure by people (terrorists, hackers, etc), by nature (hurricanes, tornadoes, etc), or by hazardous materials (HAZMAT) accidents (chemical spills, etc).

Infrastructure protection involves the application of a systematic analytical process fully integrated into all infrastructure functions of the JFOB. 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 infrastructures essential for the accomplishment of missions (i.e., fire suppression, HAZMAT containment, sewer treatment, water supply, electrical systems, and cyber systems.
- □ Determining the threat against JFOB infrastructures.
- □ Analyzing the vulnerabilities of JF0B infrastructures.
- □ Assessing the risk of the degradation or loss of a critical infrastructure.
- □ Applying countermeasures where risk is unacceptable.

IDENTIFY CRITICAL INFRASTRUCTURES

SWEAT

Several of the most important infrastructure areas that must be addressed are covered in the acronym "SWEAT." The critical infrastructure areas are as follows:

Sewer. The sewer systems in JFOBS can range from burn-out barrels in an initial construction to a municipal sanitary sewer and wastewater treatment plant like those found in small towns. Sometimes the sewer may be tied into a local municipality. Sewer systems start with burn-out barrels, then evolve to leech fields/lagoons and then to lagoons/treatment plants.

Initial sewer treatment may involve hauling liquid wastes off site in sewage disposal trucks. These trucks become prime targets for use of vehicle-borne improvised explosive devices (VBIEDs). Security should implement the following force protection (FP) 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.
- □ Provided security for the driver when the sewage disposal truck leaves the JFOB.
- □ Search the truck thoroughly before allowing it back on the JFOB 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 JFOB as the JFOB matures.
- □ Include FP measures and emergency backup plans when contracting with outside sources, to include municipalities, for disposal service.

Water. A reliable water source is critical for the successful operation of a JFOB. The initial standard is bottled water, then bottle/ROWPU (Reverse

Osmosis Water Purification Unit), and then well and treatment plants as the JFOB matures. 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.

Figure 11-1. Reverse Osmosis Water Purification Unit (ROWPU)

A water supply threat involves the release of biological organisms or toxins into the reservoir or water tank. In order for this contamination to cause illness or death, the dilution provided by the large volume of water would have to be overcome. 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 of the potable water currently being used is bottled water that is being trucked in. 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 JFOB against sabotage.

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

In order to sabotage the JFOB's water supply, the enemy would have to have large amounts of an agent and knowledge of the water supply network. Important points to consider are the following:

- 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 treatment process (i.e., 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 infrastructures, 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 JFOB and/or commercial generators. As the JFOB matures, larger generator sets (Prime Power (see Figure 11-2)) 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. Iraqi 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 JFOB.

Figure 11-2. Prime Power generator

Many JFOBs 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 (SAF) and RAMs with concrete T Walls and overhead cover if possible.

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

□ Consider hardening for critical power nodes that drive command, control, communications, computers, and intelligence (C4I), medical, and food storage.

Overall, existing electrical systems have not been primary targets.

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

□ Protect and monitor schools.

□ Guard mosques as any other key terrain in order to maintain good relations with the host nation (HN).

□ Monitor minarets at local mosques for AIF 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.

Trash. Initially, trash in JFOBs is almost always burned and buried. As the environment becomes more permissive, trash may be disposed of off the JFOB by other methods. Security measures that should implemented are the following:

□ 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.

□ Keep garbage trucks on base while not being used to prevent them from being setup with VBIEDs. Garbage trucks are currently the vehicle of choice for VBIEDs.

Most JFOBs are converting to on-site incinerators. The base commander can reduce the volume of garbage for disposal by implementing reduce, reuse, recycle (RRR) programs.

ADDITIONAL INFRASTRUCTURE AREAS

Communication. Communication is covered in greater detail in Chapter 10. 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 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.
- Towers should be illuminated at night to warn aviators.
- Maintain positive control of secure items, and conduct regular sensitive-items inventory so that sensitive equipment is accounted for.
- Minimize use of cell phones.

Transportation. Transportation is covered in greater detail in Chapter 6. Transportation assets include pavement, bridges, pipelines, rail 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. These issues are addressed in Chapter 7.

CRITICAL INFRASTRUCTURE EVALUATION

The following is a checklist of 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 for 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.

For FP, it is generally better to have several smaller systems than one large system. Power generation can be divided among functional areas within the JFOB. Potable water production can be divided among several wells.

Tie in to public utilities. Public utilities including, but not limited to potable water, electricity, and sewer, can be considered for use by the JFOB. 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 JFOB. 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 for the only source of a service. Water, sewer, and electricity are all subject to sabotage and routine outages.

Infrastructure Resources. The U.S. Army Engineer School has developed "The SWEAT/IR Book version 2.1 dated 6 October 2005," which is a thorough how-to manual for performing Infrastructure Reconnaissance. It is loaded with tools, checklists, and processes to assist units in developing their Infrastructure Assurance and Recovery Plans for their respective AORs. An electronic version of this handbook is available on the JFOB CD under the COOP master planning tab. POC for this handbook is the U.S. Army Engineer School General Engineering Division at www.wood.army.mil.

For specific infrastructure guidance in support of JFOBs in Iraq, refer to U.S.CENTCOM Regulation 415-1. It can be found on the JFOB CDs COOP under "References."

REFERENCES

FM 3-34. *Engineer Operations*, 2 January 2004. (available from www.adrdl.army.mil)

JP 3-10. *Doctrine for Joint Rear Area Operations*, 28 May 1996. (available from www.dtic.mil/doctrine)

JP 4-04. *Joint Doctrine for Civil Engineering Support*, 27 September 2001. (available from www.dtic.mil/doctrine)

Chapter 12

RESOURCING-FUNDS AND CONTRACTING

Contents

INTRODUCTION AND OVERVIEW

As unit personnel make plans for any operation, competing requirements make demands on resources. Examples of competing requirements are weapons systems, command, control, communications and computers (C4), force protection (FP) needs, logistics support, and other mission-essential equipment. Resources are time, funds, personnel (troop labor), 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, the FP officer 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.

This chapter is intended to acquaint the FP officer with terms, processes, and personnel in the requirements generation, funding and contracting processes. This will enable the FP officer to identify, justify, fund and contract for necessary supplies and services to meet mission requirements.

In the U.S.CENTCOM area of responsibility (AOR), the Army is in charge of contracting through the Assistance Secretary of the Army for Acquisition, Logistics, and Technology (ASAALT).

The normal steps in the acquisition process are the following:

- ☐ Requirements generated by unit
  - ○ Statement of Work (SOW) & Independent Government Cost Estimate (IGCE)
  - ○ DA Form 3953, "Purchase Request and Commitment" (PR&C)
- ☐ Requirements Package Validated by Joint Acquisition Review Board (JARB) and Approved by Task Force Commander (COMJTF) or his appointee
- ☐ PR&C certified by Resource Manager for funding/commitment
- ☐ PR&C and SOW sent to Contracting for execution/obligation
- ☐ Goods/services delivered to customer
- ☐ Vendor paid by Finance

The same acquisition process diagramed in Figure 12-1:

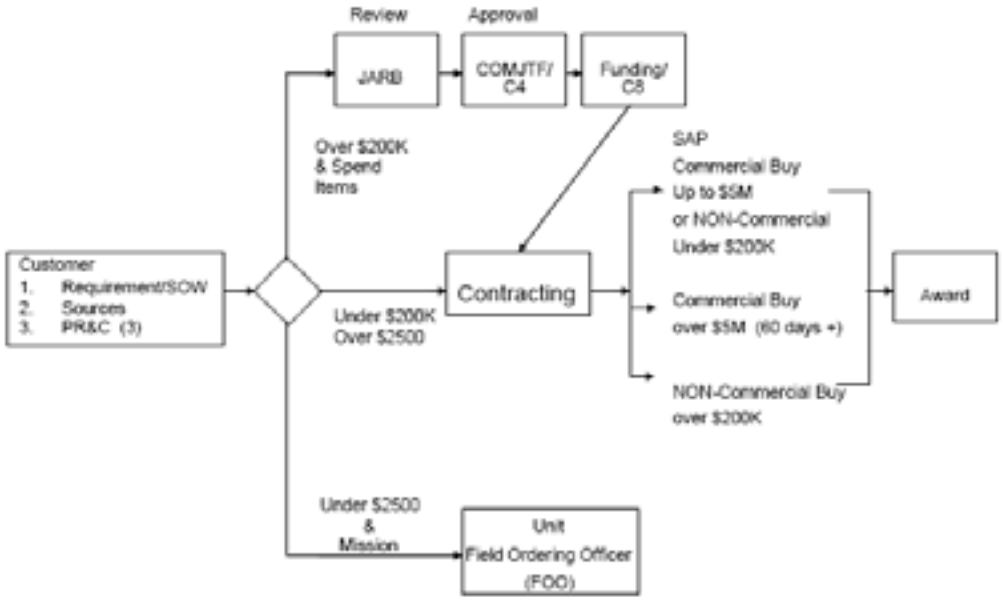


Figure 12-1. Sample Acquisition Process

As the diagram shows, the formal requirements (or hurdles) to contracting relate primarily to the dollar threshold of the acquisition: **as the value goes up, so do the formalities**. For example, acquisitions under $2500 can generally be accomplished by a Unit Field Ordering Officer (FOO); but, higher command approval of the requirement is required where the amount exceeds $200,000. There are obvious and not-so-obvious reasons for this. The obvious reason is that money is always in short supply when placed against requirements. The not-so-obvious reason is that fiscal laws that govern the disbursement of money carry **severe penalties for violations**, including criminal penalties or taking of pay. Consequently, the requirements generation process has its own checks and balances that the FP officer must understand and follow.

Similarly, in higher-level procedures (typically over $200,000), once the command has validated a requirement, there are generally three staff offices that work in tandem to assist the unit in fulfilling their contracting requirements. Such offices are referred to as the "Fiscal Triad," which is made up of the Comptroller or C8, the Finance Unit, and the Contracting Officer. Comptrollers acquire, control and certify funds in accordance with fiscal law. Finance units make the payment. Contracting Officers receive unit requirements and complete the process of acquiring goods and services as shown in Figure 12-2.

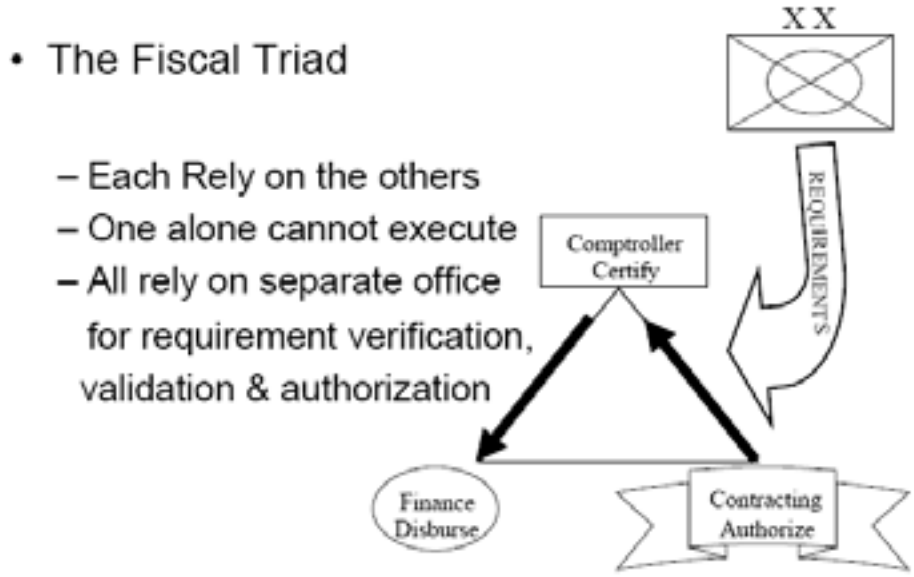


Figure 12-2. Fiscal Support Staff

The key steps in any contracting process are to (1) identify and justify the requirements, (2) identify appropriate funding sources and fiscal constraints, and (3) use the proper contracting authority and methods. At the end of this chapter, we will also discuss some issues with which to be particularly concerned in a contingency environment. With this knowledge, an FP officer should be equipped to participate in the contracting process and fill the gaps in resources that will ensure the security of the Joint Forward Operations Base (JFOB). Next, we'll discuss each of the key steps in the process.

IDENTIFY AND JUSTIFY REQUIREMENTS

Key Task -Identify programmatic and procedural requirements to reduce the risk from the threat: what needs either to be done or acquired to make the JFOB more secure that cannot be satisfied with existing resources?

Key Products – Commander's Justification Memorandum, Purchase Request and Commitment (PR&C), Statement of Work (SOW), and Independent Government Cost Estimate (IGCE).

Key Players - FP officer, Unit Commander, Installation Property Book Officer (IPBO), Joint Acquisition Review Board (JARB), and COMJTF or his/her designee for approval of PR&Cs (requirements).

IDENTIFY REQUIREMENTS

Through various planning processes, the FP officer must identify areas where changes or improvements should be made to JFOB layout, equipment, and procedures. These changes or improvements should be required to reduce the risk to people, mission, and property. To assist the FP officer in these planning processes, there are analytical tools or procedures. For example, the FP staff, using AT Planner – an Army Corps of Engineers tool for estimating damage – may analyze an improvised explosive device's (IED's) projected effects on tents, modular buildings, and personnel. From this analysis, the staff may determine requirements to reduce risk. These requirements can be categorized as either **programmatic or procedural**. Examples of programmatic requirements are a need for funds for bomb-detection equipment, more security forces, and more military working dogs. Examples of procedural requirements are more personnel assigned to foot patrols, variation by 10 minutes of the timing of spot checks around the area, and leaving the JFOB by different routes.

The key thing to remember is that, unless there is only one possible source to fulfill a requirement, FP officers should **describe the requirement as generically as possible** so that contracting has options when asked to fulfill it. Simply stated, identify what is needed, not how it is to be done. To do this, the FP officer will often need to conduct a detailed analysis of the requirement and reduce it to its essence. The FP officer should be able to defend requirements using experience, proven operating procedures, and results from analytical tools in a concise and convincing manner. Most likely, the FP officer will write the reasons for the requirements (this justification information) and submit them through the appropriate staff to the Unit Commander for approval. This information is developed into a Joint Acquisition Review Board (JARB).

The main institutional tool for identifying requirements along with justification, requested funding, and other data is the Core Vulnerability Assessment Management Program (CVAMP). CVAMP is a web-enabled application resident within the Antiterrorism Enterprise Portal (ATEP) that captures results of vulnerability assessments, prioritizes area of responsibility (AOR) vulnerabilities, identifies deficiencies, and lists corrective actions needed or completed. CVAMP resides on the ATEP at http://www.atep.smil.mil. Its characteristics are as follows:

- Resides on SPIRNET – CVAMP and can store classified data up to SECRET.
- Accessible over the SPIRNET via the ATEP.
- Accessible to commanders at every level within chain of command.

- Documents a commander's risk assessment decision for each vulnerability.
- Tracks the status of known vulnerabilities until mitigated.
- Informs decision makers of a given installation's ability to counter the assessed terrorist threat.
- Provides commanders a vehicle to identify requirements to the responsible chain of command.
- Prioritizes resource requirements for request of Combating Terrorism-Readiness Initiatives Funds (CbT-RIF) and/or Unfunded Requirements (UFRs).

A user's guide to CVAMP is available on the website.

For the purposes of requirements review and contracting, however, the key document for identifying, approving, funding, and tracking a requirement within the Army is DA Form 3953, "Purchase Request and Commitment" (PR&C). Where manufactured supplies or services are to be acquired, a statement of work (SOW) and an Independent Government Cost Estimate (IGCE) will also be needed.

JUSTIFY REQUIREMENTS (JARB PACKAGE)

With a PR&C drafted, the FP officer proceeds to preparing justification documentation, or JARB package. The two most important questions to answer in justifying requirements are "Why is this needed?" and "Why should this receive priority?" The requirement may reduce the risk of death and injury, but it must be explained sufficiently to pass the scrutiny of an outsider to the unit. Intense analysis may or may not be required. It depends on the threat, the location, expected incident response, and consequence management actions with their results, and expected losses of personnel and equipment and risk to the mission.

Analysis is often needed to justify requirements. This analysis may include results from Antiterrorism (AT) Planner – a tool in the Joint Antiterrorism (JAT) Guide-showing predicted damage to structures and personnel. Or, the analysis may include the blast radius from a rocket or mortar with expected injuries. Multiple tools are available for predicting weapons effects on structures and personnel. In any case, defending the requirement using experience, proven operating procedures, and results from analytical tools in a concise, convincing manner will help. Most likely, the FP officer will need to write and present the requirements with justification and submit for approval. Therefore, good verbal and written communication skills are tremendously helpful when justifying requirements, and there will always be a timeline for seeking funding.

For a fairly recent example of how the process works, we can draw on Operation Iraqi Freedom (OIF). In 2004 during OIF, the acquisition approval process generally followed a monthly cycle. Joint Task Force (JTF) Staff Officers held weekly meetings to consider and recommend disposition on pending theater requirements. The framework for these meetings was called the Joint Acquisition Review Board (JARB) and the

Facilities Utilization and Support Board (FUSB), respectively. The JARB and the FUSB consisted generally of intermediate representatives from all JTF-level staff sections. The JARB focused upon all requirements exceeding $200,000. The FUSB, as an engineer-centric board, considered and mandated uniform basing requirements across theater for the JARB to apply. Both of these Boards were responsible for vetting requirements so the Chief Logistician and Chief Engineer could appropriately prioritize and approve requirements.

The JARB and FUSB were only the end of the process. In the Iraq acquisition cycle, staff officers from the JARB and the FUSB would begin the month briefing the Deputy Commanding Generals for Support at each Division on their duties and current actions. They would then receive feedback about pending requirements. This meeting came to be known as the Executive Logistics Review Board (ELRB). After appropriate staffing, staff principles briefed senior leaders, who would then issue strategic guidance providing priorities on theater-wide issues. A diagram of this process is shown in Figure 12-3:

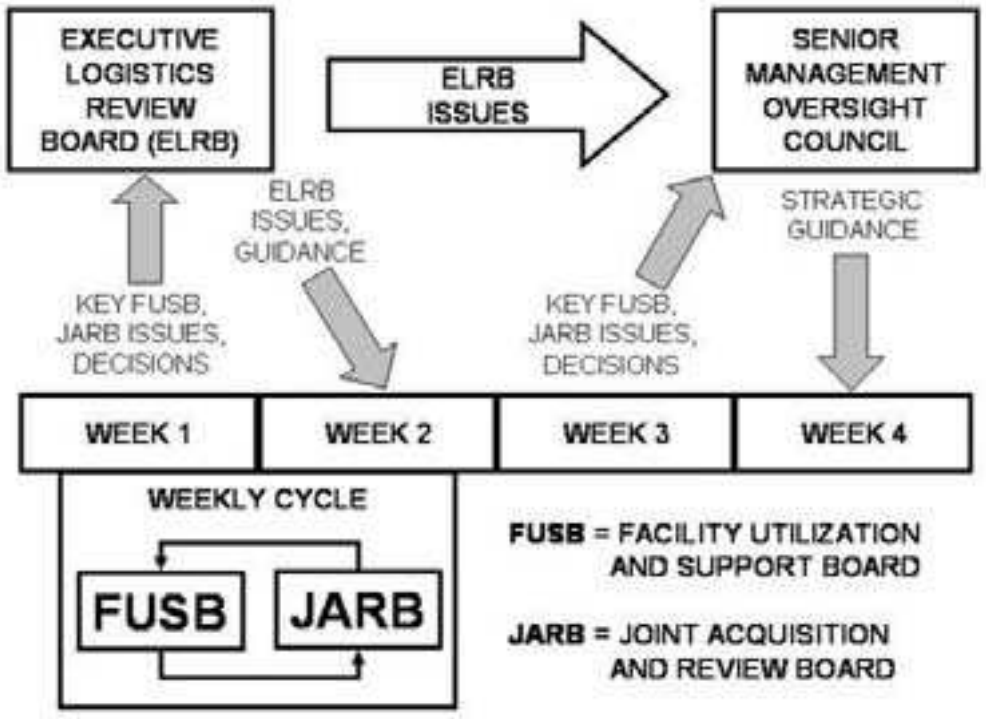


Figure 12-3. Battle Rhythm

This process served to ensure that theater-wide standards were set and that all requirements were appropriately vetted prior to going to the JARB/FUSB, and ultimately, COMJTF's designee, the C4, for approval. Generally, no acquisition exceeding $200,000 could go to the comptroller or contracting without a JARB recommendation and an approval signature on the PR&C by the C4. Similar procedures have been used in every

contingency operation in the last decade. Therefore, is critical for unit FP Officers to have a basic understanding of how to develop a JARB package when justifying their requirements.

First and foremost in every JARB package is the indication that it has been properly staffed up from the requesting unit through the Major Subordinate Commander (MSC) before it comes to the JARB. As for the specific documentation required, it will vary from package to package depending on what is being requested, but there are some basics that apply to all packages:

- **Justification Memo**. The request must have a justification memo that clearly states what the requirement is and what is requested to meet the requirement. Obviously, stating how the requirement was determined and what options were considered is important. Also be sure to consider completely the second and third order effects of what is requested. For example, the FP officer should not come in with a request to buy trailers, and then expect to come back later for a separate request to buy furniture for the trailer, and then again for separate requests for power and computer hookups, etc. Finally, make sure the request is signed by the appropriate level commander.
- **Analysis.** The analysis must support the requirement. For example, if asking for non-tactical vehicles (NTV), one would need to show what Military Table of Equipment (MTOE) or other NTV vehicles are assigned to the unit, how they are being used, and how they cannot meet the unit's mission requirement. In addition, the justification must show how the unit's mission requires the number and type being requested. In other words, treat this analysis like a "troop to task" analysis.
- **Staffing, staffing, staffing.** As one goes up the chain of command, each level has a "bigger" picture of available assets and capabilities. Somewhere between the FP officer and the highest level, someone may be able to solve the problem without contracting for it in the manner requested. Solving the problem this way meets the requirement and the mission without needless paperwork and expense. So, follow proper staffing procedures and give the staffs the chance to do their jobs.
- **Funding Documentation.** There are basically two types of funding documents that can be used to allocate funds. The requester needs to include the proper document, properly filled out and signed as a part of the package. Sometimes there is a fine line between which funding documents should be used. The supporting Resource Management Office and contracting folks can determine which one is appropriate, and make sure it is filled out properly.
    - PR&C: (Purchase Request and Commitment – DA Form 3953). As described above, this is the form to use if buying something through local purchase or a new contract. For example, if the FP officer wants to lease an NTV or a bus, he should use a PR&C as

the obligation document because it is a new purchase from a commercial source. The PR&C lists what one is trying to buy and the cost.

- MIPR: (Military Interdepartmental Purchase Requests – DD Form 448). This is the form to use if purchasing something from a contract that already exists somewhere else in DoD. For example, if an Army agency already has a contract in place for technical support, and the FP officer wants to get some of the same type support for the unit, funds go (via a MIPR) to the Army contracting agency that owns the contract. The contracting agency buys it under its contract.

□ **Statement of Work (SOW) and Independent Government Cost Estimate (IGCE).** These documents are critical when trying to hire contractor support or labor. The SOW specifies the tasks to be performed, to what standard, and what the unit, as the government sponsor, is going to provide them. Without this information, contractors won't know how to properly bid for the contract. Writing a SOW is not normally a part of military training. On the other hand, no one else can define the requirements as well as the one who needs the service or product. The most important thing to remember is that the supporting contracting folks can help. The IGCE is what the requester thinks is a fair and reasonable price for what is to be obtained. The word "independent" is fairly self-explanatory, but also the most ignored. It is not "independent" if one asks a contractor what he would charge, then puts that in the package as the government estimate. There are some guidelines on how one can develop an IGE, and the local contracting folks can help one through it.

FISCAL CONSTRAINTS AND FUNDING SOURCES

When seeking funding for a particular project, the FP officer should obtain advice and assistance from the servicing Command or Staff Judge Advocate on appropriate funding sources for the current and coming year, as well as any fiscal restraints upon the proposed project. Fiscal law, as it is known, is an ever-changing body of law that defines how money can be spent. More than perhaps any other area of the law, Commanders should expect and demand a structure in the context of Fiscal Law that guarantees independent legal advice; such independence and access by judge advocates keeps Commanders out of trouble and is also required by statute. *Accord* 10 U.S.C. §§ 3037, 5148, 5046, and 8037 (as amended by Section 584 of the 2005 DoD Appropriations Act).

FISCAL CONSTRAINTS

Perhaps the greatest opportunity to end a Commander's or Comptroller's career is in failure to comply with fiscal limitations. Given this, it is important to understand the fact that fiscal law operates like no other law. The usual question by Commanders to the Staff Judge Advocate is: "Well Judge, does anything prohibit me from doing this?" In the context of fiscal

law, this is the wrong question. Rather, the right question is: "Well Judge, is there any law that authorizes me to spend this money in this way at the time I want to do this project?" This question is always the most important one to ask, and sets up the buzz phrase that is used to analyze fiscal problems: **PURPOSE, TIME,** and **AMOUNT**. Money appropriated by Congress is never indefinite. It is always appropriate for a certain purpose, for a limited time, and in a limited sum. If one is asked why, the simple answer is: "Congress likes it that way because it serves as their check and balance on Executive power."

It is also important to understand that there are routinely two primary types of appropriated monies immediately available for a COMJTF during contingency operations. The first is contingency operations or "CONOPS" money, and the other is humanitarian assistance money, the bulk of which in Iraq and Afghanistan is currently found in the Commander's Emergency Response Program (CERP). "CONOPS" money is generally a form of operations and maintenance (O&M) money that is appropriated for mission-essential operations in a particular contingency theater. Proper mission related-expenses are any supplies, services, or authorized construction projects in theater that are needed to perform the mission or to support personnel performing the mission. Proper services include: cleaning services, mess hall services, latrine services, utility services, power generation services, air condition services, porta-john services, tent services (includes set up, take down, and maintenance) and trash services. Supplies include: barriers, concertina wire, lumber, concrete, gravel (when used for maintenance and repair), batteries, radios, cell phones (air time is a service), generators, tents, paint, tools, spare parts, cots, furniture, air conditioning units (when installed as an integral part of real property), medical supplies, oil, and computers, just to name a few. CERP, in contrast, is money that can only be used by the COMJTF in OIF to fund certain high-impact high-visibility projects for the benefit of host nation people. With respect to the JARB and acquisition process, it is normally CONOPS money that funds most operations, but also carries with it the greatest restraints and pitfalls.

An FP officer's servicing judge advocate should be familiar with the types of money available and the purposes for which they can be used. This is detailed further below and is the easy part. The difficult part of meeting fiscal law requirements is asking the right questions to ensure that the project is appropriately classified and that the proper rule is applied. To help you do this, below is a "Fiscal Law Questionnaire." This questionnaire highlights the common issues, such as the $750,000 limitation on use of O&M money for construction ($1.5 million for a requirement needed for life, health or safety), the $3 million limit on repair, and the $250,000 limit on the purchase of individual items of supply. It also asks other questions, such as whether an item is centrally managed (*e.g.*, the HUMMV or the Kevlar Helmet), or whether a project or system (*e.g.*, equipment necessary to the operation of a computer network) has been split apart to stay within applicable thresholds. The answers to these questions determine whether OMA or CONOPS can be

used, or whether other types of money, such as Military Construction (MILCON) or Other Procurement Army (OPA) funds must be obtained.

It should come as no surprise that base camp preparation, including relocatable buildings, sprung structures and tents, portable generators, as well as the site preparation necessary for the installation, were constant sources of fiscal scrutiny during OIF. For an Army example, every engineer and judge advocate knows that AR 420-10 defines funded and unfunded costs, and that AR 415-15 governs MILCON. However, what is sometimes overlooked is that the Assistant Chief of Staff for Installation Management (ACSIM) and the Army Comptroller regularly issue policy guidance on how to interpret and apply the principles in these regulations, as well as how to ask for available funds. For example, on August 25, 2004, the Comptroller issued "Procedures for Approval of O&M Construction Projects in Support of GWOT." This document basically required a centralized DD Form 1391 (the form on which all MILCON money is sought) process managed by CENTCOM and the ACSIM. As a practical matter, it made it more difficult to request MILCON funds and heightened the importance of proper project classification for use of CONOPS money.

Consistent with this, a recurring fiscal issue during OIF was not so much which "color" money to use; as a practical matter it became obvious that CONOPS was the only real source available for mission-essential construction needs. Rather, the real issue, and where a judge advocate's advice and assistance were best employed, was in working with the engineers (C7) to assist the Command to properly classify projects within fiscal (construction) limitations. As an example, in the Army, the ACSIM sets policy in this area and current guidance should always be obtained when classifying a project for funding purposes. Other services should have similar policies.

An ancillary question to the issue of project classification and fiscal constraints is: What costs count against fiscal limits? Generally, use of CONOPS (O&M) funds can be used for projects if the approved cost of the project is $750,000 or less ($1.5 million if the project is intended solely to correct a deficiency that threatens life, health, or safety). *See* 10 U.S.C. 2805. The amounts for these limitations do apply to funded costs for the project. However, unfunded costs do not apply toward these limitations.

Funded costs (which are costs that **do apply** toward fiscal limitations/count against the thresholds) include, but are not necessarily limited to:

- Materials, supplies, and services applicable to the project
- Transportation costs for materials, supplies, and unit equipment
- Installed capital equipment
- Civilian labor costs
- Overhead and support costs (e.g., leasing and storing equipment)

- Supervision, inspection, and overhead costs charged when the Corps of Engineers, the Naval Facilities Engineering Command, or the Air Force serves as the design or construction agent
- Travel and per diem costs for military and civilian personnel
- Operation and maintenance costs for government-owned equipment (e.g., fuel and repair parts); and
- Demolition and site preparation costs

Unfunded costs (which are costs that do not apply toward the fiscal limitations/count against thresholds) include, but are not necessarily limited to:

- Military and civilian prisoner labor
- Depreciation of government-owned equipment
- Materials, supplies, and equipment obtained for the project on a non-reimbursable basis as excess distributions from another military department or federal agency
- Licenses, permits, and other fees chargeable under:
  - A State or local statute; or
  - A status of forces agreement (SOFA);
- Unfunded civilian fringe benefits
- Contract or in-house planning and design cost
- Gifts from private parties
- Donated labor and material contributed to the military construction project;
- Are chargeable to appropriations other than those available to fund the project; and are not reimbursed by appropriations available to fund the project.

Note that these fiscal limitations do not count against repair and maintenance work (IAW classification per DA PAM 420-11). The limitation for these projects is currently $3,000,000. Projects which exceed this must be approved by HQDA.

As stated above, the primary thing to remember is to involve the judge advocate as early as possible in this process. To obtain the best advice, however, the FP officer must provide the pertinent facts. The foregoing provides a summary of fiscal constraints; now, let's proceed to look at how to apply these rules and constraints.

FISCAL LAW QUESTIONNAIRE

During OIF, a questionnaire has been used by the Chief of Procurement and Fiscal Law for Multi-National Corps Iraq to analyze fiscal issues. While this questionnaire should be checked and updated prior to use, the form and content of it, for reference purposes, has been as follows:

Use this questionnaire to ask the pertinent questions relating to the fiscal limitations of acquisition requests. If unable to obtain the answers, the request is not ready. Each request should also be appropriately staffed. Failure to submit the requested information, failure to properly staff, or submitting incorrect information, will delay the action, and may result in an illegal acquisition.

GENERAL INFORMATION

- ☐ What is to be acquired (equipment, supplies, services, construction, etc.)?
- ☐ Who will supply the product or service (private contractor, the Army, another DoD agency, a non-DoD Federal agency, etc.)?
- ☐ What legal process will be used to acquire the service/supplies/equipment (existing contract, new contract, Economy Act order, Project Order, SCIA, GSA schedule, supply requisition or, as a last resort, LOGCAP.)?
- ☐ What contracting office/agency will process the acquisition?
- ☐ What kind of money will be spent? For example, Fiscal Year 2004 (FY04) Operations and Maintenance, Army (OMA); Other Procurement, Army (OPA), etc?

SUPPLIES / EQUIPMENT

- ☐ What is the estimated date that the funds will be obligated?
- ☐ On what estimated date will the items be delivered and/or installed?
- ☐ If the items will not be delivered/installed until the next fiscal year, please explain why.
- ☐ Has delivery, testing, installation, and contractor TDY costs been included in the total cost? If not, why not?
- ☐ Will any of the items be connected to equipment or systems already in the inventory? If so, please explain what function or capability the new equipment will add to the old?
- ☐ For acquisitions costing more than $250,000 (OPA Threshold):
    - ○ If there is more than one unit or component, is each component a separate end item or system? Is it something that can stand alone (e.g., mobile) or be used as part of a system?
    - ○ If some of the units will be connected to form a functional system, please describe the resulting system, its function, whether it will be temporary, how often it will be connected (whether it could later be reused for another purpose) and cost.
    - ○ If the connected system of components in b above has more than one function, please describe the primary function. What are the secondary functions and why are they secondary?

- ○ Can some of the costs be attributed to "installed building equipment" (IBE)? If so, what are those costs? You must also attach a written opinion from a C7, DPW or Army Corps of Engineers expert that the components at issue will be IBE.
- ○ If you are acquiring software, describe the general function of the software (software maintenance package, operating system software, etc.) What is the useful life of the software (i.e., will the software require a major update within 2 years to meet your changing requirements)?
- ○ Are any items centrally managed? This information can be obtained from the Program Manager for larger systems, such as aircraft, vehicles, weapons, communications systems, etc. Some centrally managed items have "SSN" numbers (standard study number, an 11-digit alphanumeric code maintained by AMC).
- ○ If the cost of each item is less than $250,000, O&M money can be used to purchase centrally-managed items if an appropriate waiver is obtained from the program manager (PM) for that item stating that the PM recognizes the requirement yet cannot support the item in theater.
- ○ For items priced at over $250,000, OPA funds must be used.

SERVICES

- □ Please describe all the services that the contractor will supply. Attach a copy of the relevant portions of the contract (if already in place) or a copy of the SOW.
- □ If funds are approved, when will funds be obligated?
- □ When will the services begin? End?
- □ If the services also involve acquisition of supplies or equipment, what estimated percentage of the total cost may be attributable to supplies and/or equipment?
- □ Please describe why the services are non-personal services (contract employees are not supervised by government employees, are responsible for producing a product or result unrelated to how it is produced, do not have an employer-employee relationship with the Army, etc. See the Federal Acquisition Regulation (FAR), Part 37).
- □ Please describe why the services do not involve inherently governmental functions, such as supervising soldiers, making policy decisions, intelligence gathering, contract formation, etc.? See FAR, Part 7.5.
- □ Does the total cost include an estimated amount for increased costs when contract employees do not qualify as technical experts under the SOFA, or is there a clause in the contract shifting this burden to the contractor?

CONSTRUCTION/REAL PROPERTY MAINTENANCE AND REPAIR

- ☐ When will funds be obligated?
- ☐ When will actual performance begin? End?
- ☐ If the total cost is more than $650,000, has a reasonable estimate (10% or more) been included for unexpected contingencies?
- ☐ If the total cost of the project exceeds $750,000 (MILCON threshold):
  - ○ What is the "project?" Are structures permanent (one project) or does it consist of many relocatable and reusable structures (arguably separate projects)?
  - ○ What portion of the project, if any, qualifies as "construction"? Construction includes building a new facility, alterations improving use of an existing facility, relocation of an existing facility, conversion of a facility to different use, etc.)? Local DPW or Engineer should be able to explain this and provide independent estimate.
  - ○ Is the project necessary to protect the life, health, or safety of coalition forces? If yes, then up to $1.5 million can be spent of O&M funds.
  - ○ What portion of the project, if any, qualifies as repair and/or maintenance? Maintenance is the preservation of an existing structure for day to day use. Repair is the restoration of an existing structure and the correcting of deficiencies. Please break out the repair costs and the maintenance costs separately. The local DPW or ACE should have this data. If the project is better characterized as a repair or maintenance, then the threshold for use of O&M money is up to $3 million.
  - ○ If the project exceeds O&M thresholds, is vital to national security or life, health and safety of troops, and deferral to the next consideration by Congress of MILCON projects would be inconsistent with either national security or life, health and safety, then the Secretary of the Army may proceed using unobligated MILCON money after providing notice to Congress and waiting 15 days.

TYPES OF FUNDS AND FUNDING SOURCES

No discussion of fiscal law would be complete without a general understanding of the common types of funds and their uses. As with everything in this Chapter, current appropriations bills and DoD policies should be reviewed to ensure that no change in applicable law or regulation has occurred. Fund types include:

- Operations and Maintenance (O&M).
- Military Construction (MILCON).
- Combating Terrorism Readiness Initiatives Fund (CbT-RIF).
- Unfunded Requirements (UFRs).
- Combatant Commander Initiative Fund (CCIF).
- Security Assistance Funds (State Department-supplied).

Operation and Maintenance (O&M)

Generally, operations and maintenance funds, of which CONOPS are a subset, are used to pre-deploy, deploy, and re-deploy. These funds are used to purchase fuel, barriers, forklifts, bulldozers, sensors and warning equipment; pay utility bills, hire custodial services, etc. Generally, these funds can be used to make the JFOB more secure.

Services are authorized to use annual operation and maintenance (O&M) funds for construction projects costing less than $750,000 ($1.5 million to correct a life threatening condition or for new construction and $3 million for maintenance and repair of existing facilities). This is a peacetime provision, applicable during contingencies and emergencies; however, a designation of a condition as “life threatening” is generally considered a safety issue instead of an emergency in the context of contingency operations. During combat or designated contingency operations, O&M may be used to fund construction projects exceeding these thresholds under certain circumstances, but the Commander must consult with the servicing judge advocate before making a determination to use O&M in such a case.

Military Construction (MILCON)

As noted above, military construction funds are obtained through a formal process using a DD Form 1391 and must be approved by Congress under applicable procedures. These funds are used to prepare ground for construction; purchase bricks, mortar, concrete, and other construction materials; pay construction labor, crane rental, and other expenses related to the construction of buildings, locks, dams, and roadways. Additionally, for the JFOB these funds could be used to build major buildings and structures, including concrete building, complex entry control points, or certain phased projects.

Combating Terrorism – Readiness Initiatives Funds (CbT-RIF)

The purpose of the CbT-RIF is to fund emergency and emergent high-priority combating terrorism requirements in the year of execution. The funds provide a means for combatant commanders (COCOMs) to react to unforeseen requirements from changes in a terrorist threat, threat levels, force protection doctrine/standards, as well as unanticipated requirements identified as a result of vulnerability assessments, tactical operations, and exercising AT plans. CbT-RIF can be used to fund maintenance costs for CbT-RIF-funded items during the year of purchase and the subsequent year as a stop-gap measure. This permits Services adequate time to program life-cycle costs if maintenance funds are not programmed and provided from the parent Service. The funds are not intended to subsidize ongoing projects, supplement budget shortfalls, or support routine activities, which are Service responsibilities.

Unfunded Requirements (UFRs)

Unfunded requirements are the needs for which there are insufficient or no funds during the current fiscal year and which may have only insufficient funds or no funds for the next fiscal year. Use the Program Planning and Budgeting Execution (PPBE) process to identify and justify requests to fulfill requirements. This is a longer process compared to most activities. Requested funds that are approved by higher headquarters will not arrive for two years at the earliest through this process. The JFOB may turn into a permanent base, so use this to request funds for equipment and construction that are not available through O&M, CbT-RIF, or other local and service funds. Work with the budget, program control, comptroller, or resource management office to identify deadlines and their data request formats in order to participate in this process. Develop a working relationship with the judge advocate, budget analysts, comptroller staff, and resource management personnel. They are the experts, so follow their instructions closely.

Combatant Commander Initiative Fund (CCIF)

The primary focus of the Combatant Commander Initiative Fund (CCIF) is to support unforeseen contingency requirements critical to combatant commands' joint warfighting readiness and national security interests. The strongest candidates for approval are initiatives that support combatant command activities and functions, enhance interoperability, and yield high benefit at low cost.

Force protection on the JFOB should be a strong candidate because of its high benefit, low cost, and its support of combatant command activities and functions.

These funds are not intended to subsidize ongoing projects, supplement budget shortfalls, or support Service component expenses that are normally the responsibility of the parent Service.

Initiatives considered by the Chairman of the Joint Chiefs of Staff in any fiscal year are not eligible for resubmission or follow-on funding in subsequent years. Because all funds are in the O&M appropriation, all funding provided for approved projects must be obligated before the end of the fiscal year for bona fide needs of that fiscal year.

Combatant command projects must be nominated for consideration at the combatant commander or deputy combatant commander level. The Chairman of the Joint Chiefs of Staff is the final approval authority for CCIF requests.

CJCSI 7401.01B provides details regarding restrictions on the use of the CCIF funds.

Initiatives submitted for funding under this program MUST qualify within one of the following authorized activities:

- Joint Exercises and Force Training
- Contingencies and Selected Operations
- Humanitarian and Civil Assistance
- Command and Control
- Military Education and Training for Military and Related Civilian Personnel of Foreign Countries
- Personnel Expense of Defense Personnel for Bilateral or Regional Cooperation Programs

Key questions to answer in the submission for these funds:

□ Why is this request considered unforeseen or emergent?

□ Would funding for this request subsidize an ongoing project, supplement a budget shortfall, or support a Service component expense that is normally the responsibility of the parent Service? If so, describe why.

□ Are there other funding sources for the request that fit the following? If so, why aren't they being used?

  ○ Initiatives already funded by combatant commander's executive agent or components.

  ○ Normal Service operating costs (including O&M costs)

  ○ Initiatives that have other available funding sources such as annual humanitarian and civic assistance submissions or command and control projects.

□ Does the request have an effect on the war on terrorism, strengthen joint warfighting capability, or aid in transforming the joint force?

□ What is the realistic impact of failure to fund the effort?

□ Is there a liaison or subject matter expert on the Joint Staff for this effort? If so, identify the point of contact and office.

- ☐ Can you provide a clear statement of need?
- ☐ Can you provide detailed cost estimates that include TDY requirements, contractual services, and equipment purchases to include unit costs, rates, and descriptions of contractual vehicles to be used?

If you make a submission, do it by letter. Submissions are not limited to one page. Adequate information is required for the Joint Staff to assess each initiative. Answer all the requests for data in the submission format.

Website for this document:
http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm

CONTRACTING AUTHORITY AND METHODS

The joint mission of resource management and contracting is to fairly allocate scarce resources across a theater of operations. With command approval, and as described above, resource management allocates funds to contracting, enabling it to obtain those supplies, services, and construction that the unit must have to perform its mission and that it does not currently possess. Consistent with this, there were fragmentary orders (FRAGOs) in OIF which defined what services could be purchased for base camps, perhaps the largest continuing expense, that differentiate between base camps with less than 600 personnel and those with more than 600 personnel. This same FRAGO also stated a preference for using the Logistics Civil Augmentation Program (LOGCAP) contract only "as a last resort."

Most discussion in Iraq about contract type devolved into a discussion about whether or not to use LOGCAP. As the influence of the Joint Contracting Command increases in Iraq and Afghanistan and available funds decrease, the discussion about whether to use a cheaper method of contracting may resolve itself. At present, it remains an issue for every JARB and a consideration for every FP officer on which contracting method to use for major requirements.

CONTRACTING AUTHORITY

No one can contract for the government without authority. It is critical to remember that contracting authority is not derived from the same place or in the same manner as command authority. In the CENTCOM AOR, for example, the Army is in charge of contracting, through the Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASAALT). The bottom line is that before a contract is signed, the person signing it should ensure that he or she has adequate authority in writing (through a warrant of written appointment) to sign. Contracts entered into without authority must be ratified by the contracting chain of command (or the offending person may pay out of pocket). So, if authority is unclear, contact contracting or the servicing judge advocate for guidance. These different lines of authority may be illustrated as shown in Figure 12-4.

Figure 12-4. Different Lines of Authority

Given proper authority, contracts are the legal agreements between the government and individuals or businesses for delivery of services, products, and equipment. A contractor can be one individual or a large company employing many individuals. Contractors may be U.S. citizens, foreign nationals and/or host nation personnel.

Always ensure consideration of force protection in all contracts for services and materials.

CONTRACTING TEAM

For the JFOB, all contracts are to incorporate force protection and antiterrorism (AT) considerations. (Antiterrorism is a subset of force protection.) To effectively do this, the JFOB needs a contracting team or needs to place the FP Officer on the JFOB contracting team. The following key personnel should be on the team:

- ☐ Director of Logistics Division, Director of Contracting, or similar.
- ☐ Force Protection Officer
- ☐ Servicing Judge Advocate or Legal Officer
- ☐ Contracting Officer (KO) or Field Ordering Officer (FOO) – These are the only people who can legally obligate the government to pay for materials and services.
- ☐ Contracting Officer Representative (COR) or Contracting Officer Technical Representative (COTR). – This person cannot legally obligate the government to pay. This person often writes the SOW and acts as a technical point of contact for the contracting officer who

may not be familiar with technology, materials, tactics, techniques, or procedures

- □ Task Monitors (This could also be the COR or COTR.) These personnel represent the unit initiating the contractual requirement.
- □ Comptroller (RM)/Disbursing Officer or Pay Agent – These are the only people who can legally certify and deliver funds for payment to a vendor.

FORCE PROTECTION (FP) – RELATED TASKS IN CONTRACTING

DOD Instruction 2000.16 provides tasks to accomplish with regard to contracting while considering antiterrorism measures. These are as follows:

- □ Implement a verification process, whether through background checks or other similar processes, that enables the U.S. Government to attest to the trustworthiness of DoD contractors and sub-contractors (U.S. citizens and host-nation personnel), including those personnel having direct or indirect involvement in the delivery or provision of services related to mail, supplies, food, water, or other materiel and equipment intended for use by DoD personnel. This vetting of trustworthiness shall include husbanding agents and crews on contracted ships, planes, trains, and overland vehicles.
- □ Develop and implement site-specific risk mitigation measures to maintain positive control of DoD contractor and sub-contractor access to and within installations, sensitive facilities, and classified areas.
- □ Develop and implement site-specific risk mitigation measures to screen contractor or sub-contractor transportation conveyances for chemical, biological, radiological, nuclear, and explosive (CBRNE) hazards before entry into or adjacent to areas with DoD personnel and mission-essential assets.
- □ Ensure that contracts comply with the AT provisions of the Defense Federal Acquisition Regulation Supplement (reference (k)).

TYPES OF CONTRACTS

There are various types of contracts to use. Each has its own advantages and disadvantages. Consult the contracting officer for the type of contract best suited to the requirements regarding force protection. Understand how the contract affects force protection. If there are any changes, the FP officer needs to know the effects on his mission and the JFOB whether they are small or large. Examples of the general types of contracts are below:

- Firm, fixed price (FFP).
- Cost-plus fixed fee (CPFF).
- Cost-plus award fee (CPAF).

- Time and materials (T&M).

Contracts can be modified using change orders. A change order adds, deletes, or changes tasks in the statement of work. The change order provides flexibility when requirements change and the contract needs to be modified.

Task orders are usually added to time and materials contracts. Task orders are often placed on contracts when specific efforts such as studies, analyses, and professional support services are needed for a specified period of time. The task orders provide flexibility as needs change.

Some examples of the products and services most likely acquired under contract are:

☐ Local Transportation Services (if any).

☐ Lodging on local economy (if any).

☐ Security Services outside JFOB (if allowed by applicable law).

☐ Fire Department Services.

☐ Potable Water Delivery.

☐ Electricity Production/Delivery using JFOB generators or host nation system.

☐ Natural Gas, Propane, Butane Delivery.

☐ Sewer.

☐ Garbage Collection and Disposal.

☐ Medical and Hazardous Material Disposal.

☐ Mortuary Services.

☐ Petroleum, Oil, Lubricants (POL).

☐ Meals.

☐ Toolkits – carpenters, plumbers, electricians, etc.

☐ Construction materials – wood, brick, concrete, wallboard, nails, screws, etc.

☐ Construction services – laborers, tradesmen, craftsmen.

☐ Earth materials – sand, gravel, topsoil.

☐ Earth-moving equipment-bulldozers, graders, scrapers, dump trucks.

CONTRACTING METHODS

In a contingency environment, there are generally two levels of individuals that possess authority to contract, and their methods differ. The first is the Field Ordering Officer (FOO), appointed by the unit. The second is a warranted contracting officer, appointed by the Principal Assistant Responsible for Contracting (PARC) in theater. Both derive their authority from the contracting chain of command in theater. However, the primary difference is the amount of money for which each can contract

and the formalities that must be followed for each. The FOO generally uses an SF 44 to contract and only has authority for contracts of $2500 or less. Depending upon the terms of his or her warrant, a KO may have unlimited authority, but must generally follow strict procedures contained in the Federal Acquisition Regulation (FAR) or other applicable guidance.

Field Ordering Officer (FOO) and the SF 44 Method

FOO contracting with an SF 44 is the simplest form of contracting. For an FOO to be able to contract for goods or services, all of the following must be true about the goods or services to be acquired:

- ☐ Not immediately available through military supply channels
- ☐ Emergency or Mission Critical
- ☐ At or below $2,500; no split requirements
- ☐ Sufficient funds are available from PR&C, DA Form 3953
- ☐ Immediately available from local vendor (on-the-spot purchase)
- ☐ One Delivery (Over the Counter) with One Payment
- ☐ Fair and Reasonable Price; Rotate Vendors

To properly contract and execute payment, there are several procedures that a FOO and his or her accompanying Pay Agent must follow:

- ☐ Receive requirement from Unit Commander
- ☐ Ensure funds are available on DA 3953
- ☐ Locate Vendor; Inspect Item
- ☐ Determine Fair and Reasonable Price
- ☐ Prepare SF 44
- ☐ Execute purchase; Class A Pay Agent pays
- ☐ Receive an itemized Vendor's Receipt

Completing the SF 44 properly is a key part of the process. Figure 12-5 shows a sample SF 44 with instructions for completion. Figure 12-6 depicts the FOO process from start to finish.

Warranted Contracting Officer (KO) Methods

As noted above, a KO must generally follow the formalities and competition requirements contained in the FAR. However, during contingency operations, with the approval of either the PARC or Head of Contracting Activity (HCA), these requirements may be relaxed under certain specified circumstances. These circumstances require a written justification and approval describing unusual or compelling urgency, and must be reviewed by a judge advocate prior to approval by the appropriate level of the contracting chain of command. In Iraq, for example, the HCA possessed the statutory authority to make competition and FAR exceptions

for acquisitions up to $75 million. However, such exceptions by the HCA are not the norm. This is because there are a host of other procurement flexibilities in a contingency environment designed to meet the needs of Commanders.

Whatever the method used, the process for the KO follows generally the same path. This process can be depicted as shown in Figure 12-7.

During contingency operations, there are several simplified acquisition methods in the KO's arsenal. These methods vary in complexity and approval requirements, but FP officers should feel free to consult with their servicing judge advocate and contracting officer to select the best method. They include:

- Purchase Orders. offer to buy supplies, services, and construction. Contract occurs when written acceptance is received. Forms used: DD 1155, SF 33 or SF 44
- Government Purchase Card
- Accommodation/Purchase Card Checks
- Blanket Purchase Agreements (BPA) offer to repetitively use supplies or services. Advance agreements for future contracts. Sets price, terms, and clauses to rapidly acquire items. Does not mean we will always use the same contractor. Form used: DD 1155
- Imprest fund. petty cash fund established by disbursing officer for cashiers. Funds are specifically identified for certain use.
  - Maximum amount advanced to units/cashiers $10,000
  - Cash used to pay for micropurchases (limit $2,500 each)
  - Used for immature theaters/countries
  - Appropriated funds reimburse Imprest fund
  - Each purchase must be validated and authorized
  - Cashiers cannot be ordering officers: separation of duty
- Existing contracts. sister services or agencies that meet unit requirements may already exist. KO can amend or use existing contracts
- LOGCAP (Logistics Civil Augmentation Program). ALC has several contracts for support world wide.
- AFCAP (Air Force Civil Augmentation Program) is used primarily for civil engineering
- Acquisition & Cross-Servicing Agreements. DoD has authority to acquire logistic support within itself, NATO countries, UN, and other State Department approved countries.

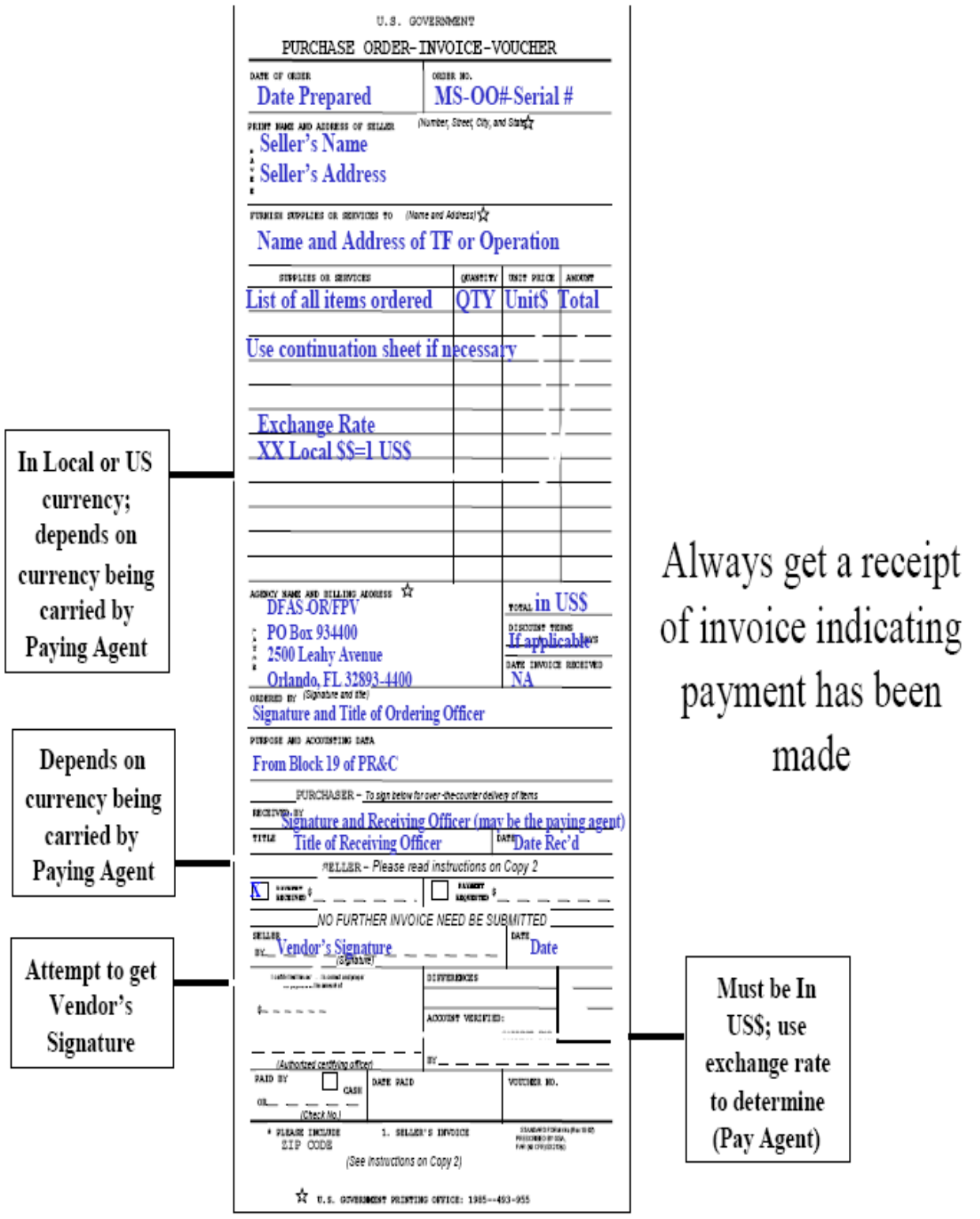


Figure 12-5. Sample SF 44 with Instructions

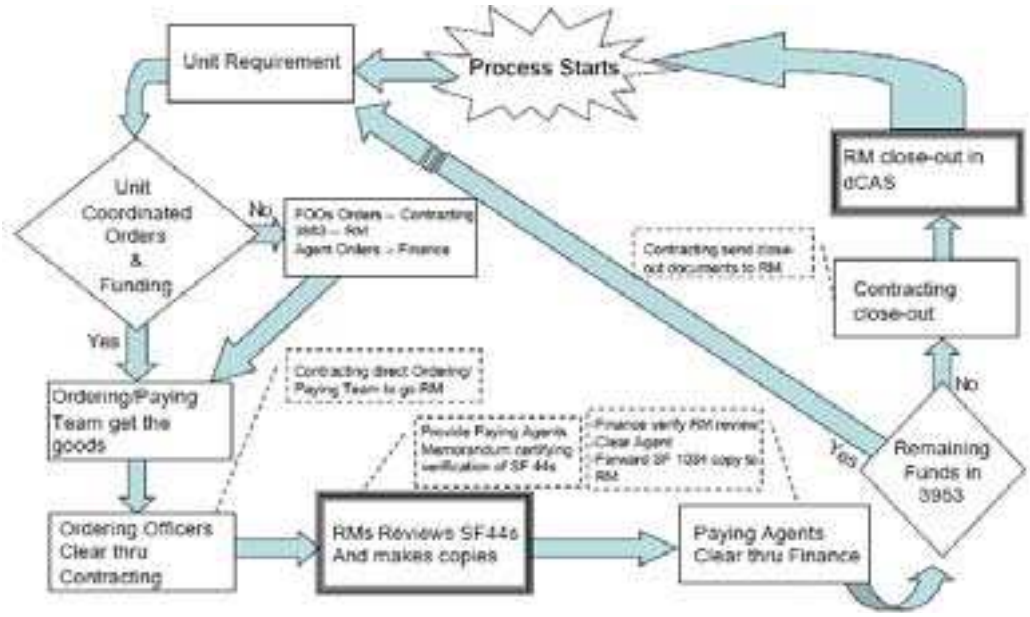


Figure 12-6. Actual Acquisition Flow

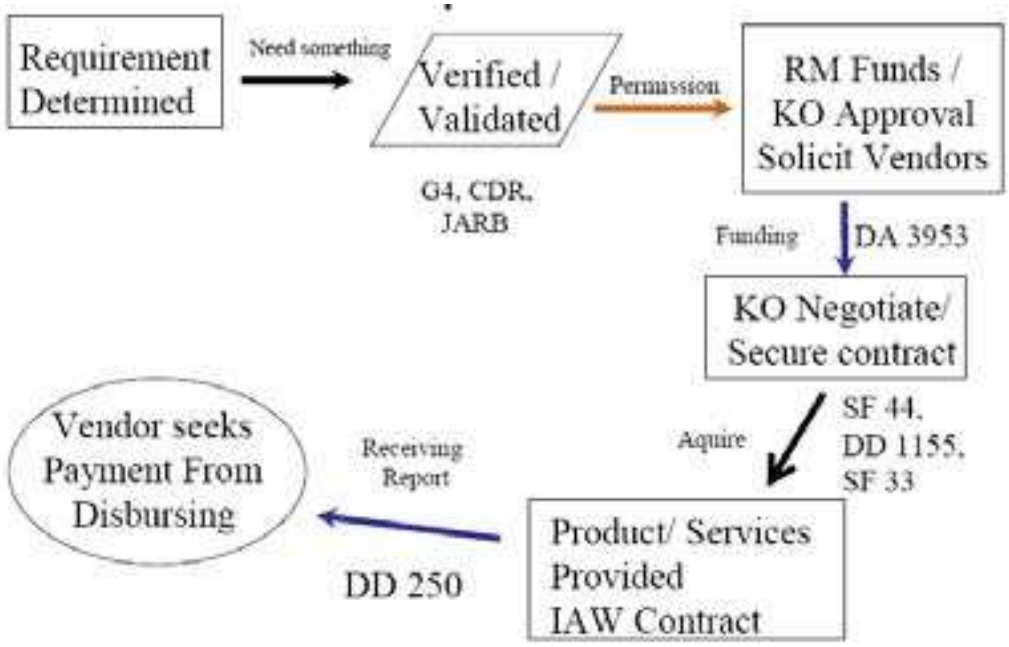


Figure 12-7. Contingency Contracting Officer Acquisition Process

RESOURCING-FUNDS AND CONTRACTING CHECKLIST

- ☐ Define the exact requirement for specific support service or product required
- ☐ Identify alternatives to contracting for the service or support
- ☐ Determine if local vendors/contractors accept the IMPAC card
- ☐ Determine if local vendors/contractors accept payment in local currency
- ☐ Determine if local lodging providers accept payment in local currency or the IMPAC card
- ☐ Determine if payments to local contractors will be in cash or by check
- ☐ Identify who will provide security for the funds before and during disbursement if payments are made in cash
- ☐ Identify who will provide security for disbursement personnel traveling to and from the forward operations base
- ☐ Estimate the amount of cash needed to pay local vendors and contractors for FP-related products and services
- ☐ Determine if the contracting task managers need translators
- ☐ Identify how translators will be paid – cash, check, electronic banking
- ☐ Determine if escorts for local contractors will be needed
- ☐ Develop and obtain approval for a method for letting local contractors onto the base
- ☐ Determine if enough real estate been obtained through status-of-forces agreement (SOFA) or other means to provide adequate standoff protection from vehicle-borne improvised explosive devices (VBIEDs)
- ☐ Determine if there is a current Threat/Vulnerability Assessment (VA) for the location
  - ○ Identify date of last threat and vulnerability assessments
  - ○ Identify threat
  - ○ Identify vulnerabilities
  - ○ Use the threat assessment and vulnerability assessment to determine contractual requirements

Identify the local capabilities for security and AT physical security measures that need to be considered if host nation contractors are employed on the JFOB

- ☐ Designate a contractor entry point
- ☐ Identify additional security measures that the contractor can provide during the service/support
- ☐ Identify what specifically the contractor can do to augment existing security arrangements

- ☐ Determine if the contractor can properly appraise or examine expertly (vet) the security clearance for all employees
- ☐ Determine what measures of uncertainty still exist after vetting the contractor's employees
- ☐ Determine if the unit/command considered asking for periods of support/service that are not routine or predictable in order to reduce risk of exposure
- ☐ Determine if coordination with the contractor ensures a more predictable time period of coverage
- ☐ Determine if local agencies can provide extra assistance if the contractor is unable to provide additional operations security (OPSEC) or FP physical security measures
- ☐ Determine if the unit/command can add extra FP physical security measures as needed
- ☐ Where vetting cannot be achieved or additional FP physical security measures cannot be contracted, identify what specific FP physical security measures can the unit/command implement to narrow operational risk
- ☐ Determine if the reason for the service or support requirement is really needed after all
- ☐ Determine if the operational benefit of receiving the service or support outweighs the identified security shortfalls
- ☐ Determine if the support tasks are mandated or can operational flexibility be employed to mitigate the overall risk
- ☐ For support contracts, determine if the unit/command incorporated the following AT considerations, if needed, into the contract:
    - ○ Conduct background checks of all contractor/sub-contractor employees.
    - ○ Establish a process for positively identifying all contractor/sub-contractor employees and consider the use of the following:
        - Photo IDs
        - Official IDs
        - U.S. Government Issue IDs (only after background checks)
        - Company-issued IDs as last resort
        - Limiting vehicle access.
        - Furnishing daily personnel access list w/photos to security personnel.
        - Furnishing daily vehicle access list to security personnel.
        - Identifying all watercraft being utilized.
        - Identifying all food and water sources being utilized.

- ☐ Determine if procedures and measures have been established and followed to ensure the contractor understands, acknowledges, fully supports and briefs appropriate company and sub-contractor personnel on the AT physical security measures to be implemented
- ☐ Determine if the measures been coordinated/approved with local agencies as needed
- ☐ Considerations for support to aircraft:
  - ○ Determine if there is a reliance on local contracts for services and support
  - ○ Identify the local security procedures at the selected airfields that contractors must follow
  - ○ Determine if there is a means to identify and approve contractors to work at the airfields

REFERENCES

Antiterrorism Enterprise Portal (https://atep.dtic.mil or https://atep.smil.mil)

AMC Website. "Contingency Contracting and Contractor on the Battlefield Policy, Guidance, Doctrine and Other Relevant Information" (available at http://www.amc.army.mil/amc/rda/rda-ac/ck/ck-source.htm)

Banes, Bryant S. "Best Practices Note: Procurement and Fiscal Law in a Deployed Environment," Center for Law and Military Operations, The Judge Advocate General's Legal Center and School, 25 June 2005.

CJCSI 3470.01. Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution, 15 July 2005

CJCSI 5261-01C. Combating Terrorism-Readiness Initiative Fund (CbT-RIF), 1 July 2003

CJCSI 7401.01B. Combatant Commander Initiative Fund, 15 Aug 03

FM 3-100.21. Contractors on the Battlefield, 1 March 2003.

FM 100-10-2. Contracting Support on the Battlefield, 8 April 1999.

JP 1-02. Department of Defense Dictionary of Military and Associated Terms, 12 April 2001 (As Amended Through 9 May 2005)

"Operational Contracting in Support of Operation Iraqi Freedom," PowerPoint briefing, U.S. Army Contingency Contracting Conference, 20 April 2005.

The Joint Antiterrorism (JAT) Guide, Version 1.2.1, April 2000

Chapter 13

TRAINING AND EXERCISES

Contents

INTRODUCTION

The U.S. military faces an asymmetric threat in Iraq. This threat frequently employs a broad range of military, paramilitary, and information operations specifically targeting our weaknesses and vulnerabilities. The current insurgents regard JFOBs comprised of a variety of logistics and support activities as desirable targets. Consequently, the JFOB commander must ensure units and service members are adequately trained in force protection (FP) and security measures. An effective training program for all Department of Defense (DoD) personnel is therefore essential to ensure personal safety and security.

TRAINING AND DOCTRINE

The doctrinal basis for training establishes fundamental principles that guide the employment of U.S. military forces in coordinated action toward a common objective. Joint doctrine contained in joint publications also includes terms, tactics, techniques, and procedures (TTP). Doctrine is authoritative but requires judgment in application. Each Service has a doctrinal agency responsible for establishing training standards and guidelines.

The **U.S. JOINT FORCES COMMAND** (USJFCOM) Joint Warfighting Center (JWFC) leads joint warfighter capability improvement through joint training. With emphasis on the Global War on Terrorism and military transformation, the JWFC works to ensure that America's military is the most advanced and powerful force in the world. The military will maintain this level of superiority

through strengthening and developing new capabilities and changing the way forces are trained - all supporting a new warfighting strategy. The web site is http://www.jwfc.jfcom.mil.

The **ARMY TRAINING AND DOCTRINE COMMAND** (TRADOC) operates 33 schools and centers at 16 Army installations. Training is the primary mission. TRADOC establishes the standards and requirements for training and developments for the Army. TRADOC develops competent and adaptive leaders while ensuring currency in Army doctrine and looks to the future while maintaining a firm grasp on today. The web site is http://www-tradoc.army.mil.

The **MARINE CORPS COMBAT DEVELOPMENT COMMAND** (MCCDC) Expeditionary Force Development System is a process that encompasses all activities and organizations required to produce, improve and sustain combat-ready, Marine Air Ground Task Forces for current and future deployments. Focusing on fundamental concepts (Marine Corps & Joint Operations), this process integrates doctrinal, organizational, structural, training and education, facilities and support, and materiel into a seamless process. MCCDC is made up of the Marine Corps Warfighting Laboratory, Expeditionary Force Development Center, Training and Education Command and Marine Corps Base Quantico. The web site is http://www.mccdc.usmc.mil.

The **NAVY WARFARE DEVELOPMENT COMMAND** (NWDC) Doctrine Department coordinates develops, publishes, and maintains Joint, Allied and Navy doctrine. To this end, the NWDC Doctrine Department promotes Navy and Joint doctrine awareness and manages the rigorous doctrine development process that moves the Navy and Marine Corps from conception and vision to practice. The web site is http://www.nwdc.navy.mil/Doctrine/.

The **AIR FORCE DOCTRINE CENTER** (AFDC) is the single voice for all doctrinal matters within the Air Force and to the joint community. The center researches, develops, and produces Air Force basic and operational doctrine, as well as joint and multinational doctrine. It coordinates with the major commands on their development of tactical doctrine and assists other Services' doctrinal development efforts. The web site is http://www.doctrine.af.mil.

MISSION ESSENTIAL TASK LISTS

The Mission Essential Task Lists (METLs) provide the foundation for an organization's training plans. The commander is responsible for developing a training strategy that will maintain unit proficiency for all tasks designated as mission essential. After mission essential tasks are selected, commanders identify supporting training objectives for each task. The conditions and standards for many major collective training tasks are identified in applicable Mission Training Plans.

The **UNIVERSAL JOINT TASK LIST** (UJTL) manual (CJCSM 3500.04C) provides a standardized tool for describing requirements for planning, conducting, evaluating, and assessing joint and multinational training. It is the basic language for development of a joint mission essential task list (JMETL) or agency mission essential task list (AMETL) that identifies required capabilities for mission success. The UJTL, when augmented with the Service task lists, is a

comprehensive integrated menu of functional tasks, conditions, measures, and criteria supporting all levels of the DoD in executing the National Military Strategy. The UJTL is available at www.dtic.mil/cjcs_directives/cdata/unlimit/m350004.pdf.

The **ARMY UNIVERSAL TASK LIST** (AUTL) manual (FM 7-15) describes the structure and content of the AUTL. For each task, the AUTL provides a definition, a numeric reference hierarchy, and the measures of performance for evaluating the task. As a catalog, it captures doctrine as it existed on the date of its publication. This publication is available at Army Knowledge Online (www.us.army.mil) and the General Dennis J. Reimer Training and Doctrine Digital Library at (www.adtdl.army.mil).

The **UNIVERSAL NAVAL TASK LIST** (UNTL) is a combined Navy, Marine Corps, and Coast Guard document and includes the Universal Joint Task List (UJTL) and the Naval Tactical Task List (NTTL). Once the level and scope of required mission capabilities is quantified, commanders can design a training program and focus planning efforts on developing training objectives that test subordinate commanders' ability to support the overall effort. It is available at the Navy Electronic Directives System (http://neds.nebt.daps.mil/directives/dirindex.html) and the Naval Warfare Development Command web site (http://nwdc.navy.mil/untl_nmetl/untl_nmetl.htm and also at the secure site http://nwdc.navy.smil.mil).

The **AIR FORCE TASK LIST** (AFTL) provides a comprehensive framework for all of the tasks that the Air Force performs in contribution to national defense. These tasks include Air Force capabilities provided in support of the joint force commander (JFC) across the spectrum of conflict and operations, as well as the tasks required of the Air Force to organize, train, equip, and provide capable aerospace forces. The document establishes general doctrinal guidance for the development of mission essential tasks (MET) using the AFTL and related conditions and measures. The manual (AFDD 1-1) is available at the Air Force Publishing website (http://www.e-publishing.af.mil).

ANTITERRORISM (AT) TRAINING

AT awareness training begins immediately upon entry into DoD service. Thereafter, Combatant Commanders, Service Commanders, and/or DoD Agencies provide AT Awareness Training annually. DoD Instruction 2000.16 requires all Combatant Commands, Services, and/or DoD Agencies to ensure every military Service member, DoD employee, and local national (LN) hired by the DoD, regardless of rank, is made aware of the need to maintain vigilance for possible terrorist actions and employ AT TTP. Additional details are provided in DoD O-2000.12-H and Joint Pub 3-07.2. There are four levels of DoD AT Training:

LEVEL I. This is the initial level of AT Awareness training. Personnel identified to receive Level I AT training will normally do so by viewing the Service or Combatant Command-selected personal awareness video provided under the instruction of a qualified Level I AT Awareness instructor and/or

DoD-sponsored, and Service or Combatant Command-certified, computer-based and/or distance learning program (Online AT Awareness training is available at http://at-awareness.org.). The following personnel are required to receive Level I training.

- All outside the United States (OCONUS)-based DoD personnel.
- All active uniformed Continental United States (CONUS)-based personnel assigned to a Combatant Command or Service command.
- All CONUS-based DoD personnel eligible for official OCONUS travel on Government orders.
- All CONUS-based DoD personnel, including civilian employees and DoD employed contractors, when the CONUS Terrorism Threat Level is set to "MODERATE" or above.
- All DoD family members, age 14 and above, deploying or traveling OCONUS on government orders.
- DoD Components will offer Level I AT Awareness Training to contractor employees, under terms and conditions as specified in their contract.
- Family members 14 years and older traveling beyond CONUS on official business shall receive Level I AT Awareness Training as part of their pre-departure requirements.

LEVEL II. Each installation and/or deploying unit must have at least one assigned Antiterrorism Officer (ATO). Personnel identified as unit ATOs are responsible for managing the AT program, advising the commander on AT issues, and providing Level I Awareness Training. Individuals administering Level I training are normally qualified to do so by attending a formal Service-approved Level II ATO training course that incorporates the minimum training standards outlined in DoD Instruction 2000.16 into the program of instruction. Graduates will have requisite knowledge and materials necessary to manage a comprehensive Base/Installation AT Program. This level of training will enable them to serve as the commander's principal advisor in all AT areas.

LEVEL III. The Services conduct Level III AT training for commanders at the O-5 and O-6 level in conjunction with pre-command training. The focus of this training is on the responsibilities discussed in the related DoD 2000 series publications, Service publications, and associated Joint Doctrine. Graduates will have requisite knowledge and materials necessary to supervise a comprehensive Base/Installation AT Program and manage AT issues.

LEVEL IV. The Joint Staff conducts Chairman of the Joint Chiefs of Staff (CJCS) Level IV Antiterrorism Executive Seminars. These seminars provide current updates, briefings, and discussion topics related to an AT program. This training provides senior commanders and managers with knowledge and materials to provide oversight to AT programs and policies. The seminars are tailored for an O-6 to O-8 audience. Graduates shall have requisite knowledge and materials to provide oversight to AT Programs and Policies.

AREA OF RESPONSIBILITY (AOR)-SPECIFIC AT TRAINING

Geographic Combatant Commanders are responsible for protecting all assigned personnel within their AOR. All individuals assigned outside the 50 United States for either permanent or temporary duty will complete the prescribed general AT awareness training and specific AOR training within three months prior to assuming assigned duties.

All AT Officers assigned within a Geographic Combatant Commander's AOR will coordinate closely with AT representatives from the Component and Subordinate Commands to develop training materials that address AOR-specific issues. The following topics should be addressed:

- ☐ Specific terrorist groups, their histories, tactics and techniques, and methods of operation
- ☐ Self-protection measures for individuals while on a DoD or U.S. Government facility or installation
- ☐ Self-protection measures for individuals while away from a DoD or U.S. Government installation
- ☐ Self protection measures for individuals while in transit from domicile to duty stations (for those living off an installation) or from one locale to another while on official business
- ☐ Improvised explosive device (IED) recognition
- ☐ Physical security measures for residents of single or multiple family housing units located off a DoD installation
- ☐ Security measures for executives and their immediate staff
- ☐ Family security measures
- ☐ Other topics as specifically mandated by the Combatant Commanders

TRAINING TASK CHECKLIST

FORSCOM Message R 091409Z SEP 04 (Change 4 to Training Guidance for Follow-On Forces Deploying in support of Operation Iraqi Freedom (OIF)) provides training guidance for forces deploying after 20 September 2004 in support of OIF. The training guidance identifies individual, leader, and collective training requirements for combat arms, combat support, and combat service support units by echelon from squad/section/crew through division and includes training for combat and stability operations. This message also clarifies training requirements for units that are deploying in support of echelons above division and corps (EAD/EAC) and supporting units. This is not an all-inclusive list and commanders at any level may add additional tasks to this list to ensure their units are trained. Units should use the Center for Army Lessons Learned (CALL) websites to refine their training as required. Major training topics are listed below.

THEATER SPECIFIC INDIVIDUAL TRAINING

- ☐ Complete a Country Orientation Brief to include a general overview of the political, military, cultural, religious, and economic conditions in the specific country. Information for this brief is available at the Central Intelligence Agency (CIA) World Fact Book website (www.cia.gov/cia/publications/factbook/ index.html).
- ☐ Complete AT/FP training Level 1 Category 2 (medium to high threat area) in accordance with and to the standards stated in AR 525-13 Appendix F (available at www.usapa.army.mil/).
- ☐ Complete Rules of Engagement (ROE) training IAW TC 7-98-1 (available at www.adtdl.army.mil/cgi-bin/adtdl.dll/tc/7-98-1/toc.htm). Specific ROE and specific instructions on use of deadly force will also be trained in theater.
- ☐ C omplete Combined Force Land Component Command (CFLCC) Rules for use of force training for all deploying units (http://www.swa.arcent.army.smil.mil/sections/sja/) and Multinational Forces Iraq (MNF-I) Rules for use of force http://www.iraq.centcom.smil.mil/sipr.cfm).
- ☐ Complete Media Awareness training IAW TC 7-98-1.
- ☐ Complete Weapons Qualification with assigned weapon IAW DA Pamphlet 350-38 (Standards available at www.atsc.army.mil/atmd/strac).
- ☐ Complete Nuclear, Biological, and Chemical Protective Measures training.
- ☐ Complete First Aid training.
- ☐ Complete Unexploded Ordnance (UXO) and IED training.
- ☐ Complete Common Task Training (CTT) on all CTT tasks identified in the Army Training Support center (ATSC) Test Bulletin for the current training year (available at www.atsc.army.mil/itsc/ctt.asp).
- ☐ Complete Land Navigation training.
- ☐ Complete Individual Movement Techniques training.
- ☐ Complete Combat Lifesaver (CLS) training. The goal is to have one CLS trained soldier assigned for each squad, section, or team.
- ☐ Complete Combat Stress and Suicide Prevention training.
- ☐ Complete an Introduction to Detainee Operations IAW U.S. Army Military Police School (USAMPS) Detainee Operations Training Support Package (located at http://www.us.army.mil under the Knowledge Collaboration Center for Army Training and Doctrine Command (TRADOC), USAMPS, Military Police (MP) Doctrine, Detainee OPS).
- ☐ Complete all regulatory briefings specified in applicable Army publications.
- ☐ Complete the Law of Land Warfare and the Geneva and Hague Conventions training.

- ☐ Demonstrate Army Battle Command Systems proficiency. Soldiers in maneuver elements must demonstrate individual and collective proficiency on battle command systems and understand their employment.
- ☐ Complete Code of Conduct (COC) training. The austere, capricious, and threatening nature of the USCENTCOM AOR requires that all deploying forces be trained to a minimum of Level B COC. Deploying high-risk-of-capture personnel are required to be trained to COC Level C and receive survival, evasion, resistance, and escape (SERE) theater preparation training prior to deployment.
- ☐ Complete Basic Iraqi Language training. All soldiers will receive training on basic Iraqi language commands normally used during operations. At a minimum the Defense Language Institute developed training on CD-ROM "Iraqi Familiarization" will be used to develop training.

THEATER SPECIFIC LEADER TRAINING

- ☐ Complete Military, Political, Cultural, Economic, and Religious Environment training. All leaders are required to be trained in understanding these areas.
- ☐ Utilize an Interpreter IAW the CALL Handbook #04-7 (Interpreter Operations).
- ☐ Perform Negotiations IAW TC 7-98-1.
- ☐ Supervise Convoy Operations IAW TC 7-98-1.
- ☐ Employ Non-Lethal Capabilities IAW TC 7-98-1.
- ☐ Plan and Conduct Urban Operations IAW FM 3-06.11.
- ☐ Supervise the Application of the ROE and use the Graduated Response Matrix IAW TC 7-98-1.
- ☐ Conduct Casualty and Medical Evacuation IAW FM 8-10-6.
- ☐ Perform Risk Management in Support of Mission IAW FM 100-14.
- ☐ Supervise Traffic Control IAW TC 7-98-1.
- ☐ Conduct Cordon and Search operations IAW TC 7-98-1.
- ☐ Understand and/or Develop Unit SOPs that address FP postures, graduated response matrix, weapon readiness levels and security postures.
- ☐ Complete UXO and IED training.
- ☐ Complete Crowd Control training IAW FM 19-15 Chapter 6 (Control Force Operations) and Chapter 8 (Crowd Control Operations) **[FM 19-15 replaced by FM 3-19.15, Civil Disturbance Operations, 18 April 2005]**.
- ☐ Complete Combat Stress training IAW FM 22-51 Chapter 2, and Suicide Prevention Training IAW DA Pam 600-24.
- ☐ Conduct Wheeled Vehicle Operator training IAW AR 385-55 and TC 21-305.

- ☐ Enforce the Law of War and the Geneva and Hague Conventions.
- ☐ Supervise the Handling of Enemy Personnel and Equipment at the Squad Level.

Units should be trained to a proficient level in competencies that are general in nature and inherent in a unit's normal duties and responsibilities. This requirement enables units to transition to offensive and defensive operations if needed.

EXERCISES

Exercises will help the JFOB Commander and staff develop, refine, and test various FP procedures. A good exercise program will validate the FP plan, identify weaknesses, synchronize the FP plan with other plans, and develop corrective actions. JFOB Commanders should conduct an FP exercise at least annually and maintain a written after-action review (AAR). A JFOB FP exercise should test the following areas:

- ☐ Force protection condition (FPCON) Implementation
- ☐ Initial response and consequence management capabilities
- ☐ Weapons of mass destruction (WMD) defense, incident response and consequence management
- ☐ Attack warning systems
- ☐ Medical mass casualty (MASCAL) handling

EXERCISE TASK CHECKLIST

DETERMINE EXERCISES AND RESOURCES

- ☐ Use the force protection working group (FPWG) to recommend exercise training objectives and tasks to the JFOB Commander
- ☐ Review training assessment(s) and determine specific training tasks. Consider the following:
  - ○ React/respond to IED discovery
  - ○ Control belligerent personnel
  - ○ React/respond to sniper attack
  - ○ React/respond to indirect fire attack
  - ○ React/respond to mass casualty event
  - ○ React/respond to Level I (small arms ambush, IED) attack
  - ○ React/respond to WMD/CBRNE (chemical, biological, radiological, Nuclear, or high-yield explosives) attack.
  - ○ React/respond to hazardous material contamination
- ☐ Review training assessment(s) and determine target audience

- ☐ Review training assessment(s) and determine current level of training proficiency
- ☐ Determine required level of training proficiency (acquire new skills, familiarize skills, practice and sustain skills, or validate skills)
- ☐ Determine exercise approach (crawl, walk, or run)
- ☐ Define desired level of realism (live, virtual, or constructive)
- ☐ Select exercise(s)
- ☐ Schedule FP scenario-driven exercises on the JFOB long-range calendar
- ☐ Include first responders in the planning process
- ☐ Take appropriate operations security (OPSEC) measures to prevent disclosure of vulnerabilities during exercise planning, conduct, and evaluation
- ☐ Consider the impact on mission, costs, and availability of personnel and resources
  - ○ Confirm training areas and locations
  - ○ Determine training ammunition allocations
  - ○ Determine availability of required training support packages and terrain databases
  - ○ Determine availability of training simulations and simulators
  - ○ Identify transportation requirements
  - ○ Identify support items
  - ○ Conduct exercise risk management/assessment
- ☐ Use small and concise scenarios to exercise a specific part of the FP program.

DEVELOP EVALUATION CRITERIA

- ☐ Select the type of evaluation (informal, formal, internal, external, or any combination)
- ☐ Develop an evaluation plan. Ensure that:
  - ○ Evaluators are trained and prepared to assume those duties for FORMAL evaluations
  - ○ Training plans prepare subordinate leaders to evaluate their units for INFORMAL evaluations
- ☐ Prepare evaluation and control plan. Be sure to address:
  - ○ Intent of the exercise and the evaluation
  - ○ Evaluation procedures
  - ○ Exercise scenario

- Training objectives
- Resource guidance
- Required coordination
- ROE
- Safety considerations
- Exercise operating procedures
- References—SMs, FMs, MTPs, and SOPs
- Evaluation checklists and training and evaluation outlines (T&EOs)
- Guidance on conduct of AARs

CONDUCT THE EXERCISE

☐ Ensure leaders conduct pre-combat checks

☐ Conduct safety and exercise briefings

☐ Supervise, evaluate, and implement hazard controls

☐ Execute training. Ensure the exercise is well-structured, realistic, safe, and effective

EXAMINE AND EVALUATE RESULTS

☐ Examine and evaluate results based on:

- FP incident response plan
- Written comments captured during the exercise

☐ Conduct an exercise AAR. Ensure the AAR covers the following:

- Review what was supposed to happen (training plan)
- Establish what happened
- Determine what was right or wrong with what happened
- Determine how the task(s) should be done differently next time

DEVELOP A STRATEGY FOR IMPROVEMENTS

☐ Insert adjustments into the FP plan

☐ Establish timelines for completing action items

☐ Track action items to completion

☐ Plan for and conduct retraining, if required

RESOURCES

All links to non-U.S. Government sites or services are provided solely for convenience. Use of these links is not an endorsement of or warranty of services provided. The DoD does not exercise any responsibility over the content at such sites. NOTE: A comprehensive list of web links is available on the accompanying JFOB Handbook CD

The **Joint Improvised Explosive Device (IED) Defeat Task Force** [JIED DTF] provides multi-echelon training and seminars that address pre-deployment training. The team provides information that allows unit leaders to decide how to best approach preparing the unit and its leadership for conditions found in the operational theaters of Iraq and Afghanistan. Units should schedule this training as early as possible in the preparation period so that leaders can reinforce the adaptation necessary throughout pre-deployment training. Contact Mr. Jack Silvers, IED Task Force, at 913-684-9534, or 913-593-3930. NIPR email is jack.silvers@leavenworth.army.mil. The SIPR website is located at http://iedtaskforce.army.smil.mil. Available training seminars include:

- Counter-IED TTP
- Company Commander/First Sergeant Seminar
- Brigade/Battalion Commander/Command Sergeant Major Seminar
- Senior Leaders Briefing

The Joint Staff has produced **Joint Staff Guide 5260**, *Antiterrorism Personal Protection Guide: A Self-Help Guide to Antiterrorism*. Each service member should become familiar with its contents and incorporate those protective measures that are applicable to his/her particular situation. The **Joint Staff Pocket Card 5260**, *Antiterrorism Individual Protective Measures* is a pocket-sized reference for AT awareness. Both are available at http://www.dtic.mil/cjcs_directives.

The **Unit and Battle Command Training** website provides the Army's leaders with self-development, unit operational, and institutional Battle Command digital training products and resources. It also provides comprehensive and current points of contact, links, and resources for Battle Command digital systems training. The web site is at https://www.warrior-t.army.mil.

The **Defense Security Service** Antiterrorism and Force Protection web site is a good resource. http://www.dss.mil/search-dir/training/csg/security/T5terror/Intro.htm#Introduction

The **Center for Army Lessons Learned** (CALL) has a large collection of information resources, documents, and search tools available on-line. Web links specific to OIF include:

- Iraq Operational Environment (https://call2.army.mil/focus/ctc/docs/DCSINT/OE_IRAQ/)
- Combat Identification/Fratricide products (https://call2.army.mil/products/fratricide.asp)

- Urban Operation page, loaded with articles, lessons, TTP's and doctrine (https://call2.army.mil/products/urban-ops.asp)
- OIF Newsletters (https://call2.army.mil/focus/ctc/iframe/docs/call/ied_tf/OIF/newsletters)
- OIF Products (AAR's, Smart Cards, Initial Impression Reports, Other Documents) (https://call2.army.mil/focus/oif/products.asp)
- IED Task Force Newsletters (https://call2.army.mil/focus/ctc/iframe/docs/call/ied_tf/OIF/newsletters/)
- Stability and Support Operations (CALL Handbook No. 03-20) (https://call2.army.mil/products/handbooks/asp/03-20/)
- CALL Newsletter, No. 05-24, Sept 05, Forward Operating Base Tactics, Techniques, and procedures (a copy is provided on the JFOB Handbook CD)
- Joint IED Defeat Task Force newsletters, written for all service members (https://call2.army.mil/focus/ctc/iframe/ied_tf/articles.asp)

Multi-National Corps/Multi-National Forces Iraq information is available at http://www.mnf-iraq.com/. Specific information includes policy memoranda and general orders.

PS Magazine (Preventive Maintenance Monthly) is available online**.** The web page is at https://www.logsa.army.mil/psmag/psonline.htm

Innovative Technology Application (**ITA**) has produced The AT/FP Exercises Computer-based Training CD-ROM Set. This CD set provides the JFOB Commander, staff, and emergency responders with interactive scenarios to exercise and practice their responses to incidents. Scenarios include high explosives, chemical, biological, and radiological events. Contact ITA at www.itapages.com/ cm_wmd/wmdprojects/DODEX.htm.

The Antiterrorism Enterprise Portal (**ATEP**) is located at https://www.atep.smil.mil. Menu items to the left of the main page include a Training section.

The U.S. Army Materiel Command **Logistics Support Activity (LOGSA)** provides logistics intelligence, life-cycle support, and technical advice and assistance to the current and future force. LOGSA's Electronic Manual Online website (registration required) is located at https://www.logsa.army.mil/etms/online.htm.

The U.S. Central Command (**CENTCOM**) web site provides news releases, news letters, features, and information on current operations. The web site is at http://www.centcom.mil

The **Soldier's Manual of Common Tasks** (SMCT) contains the common tasks that are essential to the Army's ability to fight and win on the modern battlefield. The U.S. Army Training Support Center provides an online training package for many of the tasks at https://atiam.train.army.mil/soldierPortal.

REFERENCES

AFI 10-245. *Air Force Antiterrorism (AT) Standards*, 21 June 2002. (available at www.e-publishing.af.mil)

AFI 36-2209. *Survival and Code of Conduct Training*, 28 February 1994. (available at www.e-publishing.af.mil)

AFR 64-4V1. *Survival Training*, 1 July 1985. (available at http://www.e-publishing.af.mil/)

AR 385-55. *Prevention of Motor Vehicle Accidents*, 12 March 1987. (available at www.apd.army.mil)

AR 525-13. *Antiterrorism*, 4 January 2002. (available at www.usapa.army.mil)

DA PAM 350-38. *Standards in Weapons Training*, 1 October 2002. (available at www.apd.army.mil)

DA PAM 600-24. *Suicide Prevention and Psychological Autopsy*, 30 September 1988. (available at www.apd.army.mil)

DoD Instruction 2000.16. *DOD Antiterrorism Standards*, 4 June 2001. (available at www.dtic.mil/whs/directives/corres/html/200016.htm)

DoD O-2000.12-H. *DOD Antiterrorism Handbook*, February 2004. (available at www.dtic.mil/whs/directives/corres/html/o200012h.htm)

FM 3-05.70. *Survival*. 17 May 2002. (available from www.adtdl.army.mil)

FM 3-06.11. *Combined Arms Operations in Urban Terrain*, 28 February 2002. (available from www.train.army.mil)

FM 3-19.15. *Civil Disturbance Operations*, 18 April 2005. (available from www.apd.army.mil)

FM 3-25.26. *Map Reading and Land Navigation*, 18 January 2005. (available from www.adtdl.army.mil)

FM 7-0 (FM 25-100). *Training the Force*, 22 October 2002. (available from www.adtdl.army.mil)

FM 7-1 (FM 25-101). *Battle Focused Training*, 15 September 2003. (available from www.adtdl.army.mil)

FM 7-98. *Operations in a Low Intensity Conflict*, 19 October 1992. (available from www.train.army.mil)

FM 8-10-6. *Medical Evacuation in a Theater of Operations Tactics*, 14 April 2000. (available from www.adtdl.army.mil)

FM 20-32. *Mine/Countermine Operations*, 29 May 1998. (available from www.train.army.mil)

FM 21-16 [FMFM 13-8-1]. *Unexploded Ordinance (UXO) Procedures*, 30 August 1994. (available from www.train.army.mil)

FM 22-51. *Leaders' Manual for Combat Stress Control*, 29 September 1994. (available from www.adtdl.army.mil)

FM 100-14. *Risk Management*, 23 April 1998. (available from www.adtdl.army.mil)

FORSCOM Message R 091409Z SEP 04 *SUBJECT: Change 4 to Training Guidance for Follow-On Forces Deploying ISO Operation Iraqi Freedom* (available at https://call2.army.mil/ctcask/oifmsgCHG4.asp)

"Iraq." *The World Factbook* (Washington DC: Central Intelligence Agency, 2005). (Available from www.cia.gov/cia/publications/factbook/ index.html)

JP 3-07.2. *Joint Tactics, Techniques, and Procedures for Antiterrorism*, 17 March 2002. (available from www.dtic.mil/doctrine)

Kolodze, Michael L. "Commentary: The Asymmetric Threat" *Army Logistician*, July-August 2001, pp. 16-17.

STP 21-1-SMCT. *Soldier's Manual of Common Tasks Skill Level 1*, 31 August 2003. (available from www.adtdl.army.mil)

STP 21-24-SMCT, *Soldier's Manual of Common Tasks Skill Level 2, 3, and 4*, 31 August 2003. (available from www.adtdl.army.mil)

TC 7-98-1. *Stability and Support Operations Training Support Package*, 5 June 1997. (available from www.adtdl.army.mil)

TC 21-305. *Training Program for Wheeled Vehicle Accident Avoidance*, 19 August 1996. (available from www.adtdl.army.mil)

Chapter 14

PLANS FOR FORCE PROTECTION

Contents

INTRODUCTION

The force protection (FP) plan is necessary for the development and implementation of a comprehensive, integrated FP Program. The FP plan compiles specific measures taken to establish and maintain an FP program. The Joint Forward Operation Base (JFOB) FP plan should accomplish the following:

- Provide a clear, concise mission statement
- Convey the JFOB 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 templates presented in this chapter are samples of FP plans and standing operating procedures (SOPs). The FP plan itself should not be an end state. Instead, the plan should focus efforts to adequately plan and resource all aspects of the JFOB FP mission.

FP PLAN DEVELOPMENT PROCESS

The JFOB commander is responsible for the development of a comprehensive, integrated and executable FP plan. The JFOB operations staff should take the lead in the development of the FP plan. No one individual should have the sole responsibility for developing an FP plan. Instead, having a cross-functional working group, such as the JFOB FP Working Group to develop the plan ensures the participation, input, and "buy-in" of necessary subject-matter experts (SME).

□ Step 1: **Compile Information.** The planning staff should use all information developed during the planning process for plan documentation. The various sections of the plan should comprise related FP data that can be "cut" and "pasted" into the plan format. Relevant information includes, but is not limited to, the following:

- Mission Statement
- Threat Assessment
- Vulnerability/Risk Analysis
- Incident Response Measures and Drills
- Course of Action (COA) Development
- Resource Documentation

□ Step 2: **Select Plan Format.** The FP plan format follows the standard operation plan (OPLAN) and five-paragraph operations order (OPORD) format. However, the format should be tailored to meet the unique requirements of the JFOB and should capture the elements of a comprehensive FP program.

□ Step 3: **Produce Plan Summary and Basic Plan.** The plan summary provides a concise synopsis of the scope and purpose of the plan. The basic plan provides the basis for all amplifying sections (Annexes/Appendices) and is produced prior to their documentation.

□ Step 4: **Assign Responsibility for Annex/Appendix Development.** Annexes/Appendices provide the details not readily incorporated into the basic plan. The number of annexes or appendices will vary according to the necessity to increase the clarity and usefulness of the basic plan. Each annex relates to a specific aspect of the FP operation. FP Working Group members with related expertise or area responsibility should develop and document individual annexes or appendices. For example, the Public Affairs representative should supervise the development of the Public Affairs Annex.

□ Step 5: **Establish a Plan of Action and Suspense Dates.** FP plan development and documentation requires a comprehensive, integrated approach and a strong, clear vision of FP program requirements. A realistic plan of action, with suspense dates, drives the efficient development and documentation of the FP Plan.

- ☐ Step 6: **Coordinate Staff Development and Review of the Plan.** The Operations Officer coordinates the staff's work in developing the FP Plan and reviewing the drafts. He should ensure that all parties have ample time to review drafts but should not let the process drag on indefinitely.
- ☐ Step 7: **Finalize the Plan.** The finalized plan is submitted to the commander for review and approval. Upon execution, the FP Plan becomes an OPORD. The finalized plan should meet the following criteria:
    - Be consistent with the JFOB's mission and responsibilities
    - Be oriented to a tactical perspective
    - Be adequately detailed to provide specific actions to be taken
    - Be easily understood
    - Be capable of quick and decisive execution if required
- ☐ Step 8: **Publish the Plan and Develop Supporting Plans.** Once the FP plan is published, the next planning cycle begins. The FP plan cannot remain static; rather, as the situation changes, the plan must also change. Consequently, the plan must remain under constant review – a "living document," so to speak. Each subordinate and supporting commander who is assigned a task in the FP Plan must also prepare a supporting plan. Supporting plans should be consistent with the supporting commander's mission and responsibilities.

JFOB FP PLAN TEMPLATE

The FP Plan is usually included as part of a comprehensive OPLAN. This template is not intended to be all inclusive. Although the following plan template is presented in five-paragraph OPORD format, planners can modify the format and contents to meet the needs of the JFOB, site, or other location.

1. **SITUATION**.

a. **Threat**. The following subparagraphs discuss the areas to be discussed in a threat analysis:

(1) Threat Assessment. Briefly describe the threat to U.S. military members, including any activities, capabilities (weapons, tactics, techniques, and methods of attack, including (WMDs)), high incidence of crime, or any other physical threat to the JFOB. Utilize the DoD Threat Methodology Factors (operational capability, intent, activity, and operating environment) in the examination of the threat. The threat assessment is normally provided by local or command intelligence (CC-J2, joint intelligence support element (JISE), G-2, etc.) or by other DoD and federal agencies (Naval Criminal Investigative Service (NCIS), Air Force Office of Special Investigation (AFOSI), Criminal Investigation Division (CID), Department of State (DOS), Defense Intelligence Agency (DIA), etc.). Parts of this paragraph may be classified and under separate cover.

(2) Threat Level. Identify the current DIA threat level. The current threat level can be obtained on the USCENTCOM Joint Security

Directorates (JSD) Secret Internet Protocol Router Network (SIPRNET) homepage: http://recluse.centcom.smil.mil/ccjs/jsd.htm

(3) Vulnerability Assessment. Identify exploitable vulnerabilities and suggest options that may eliminate or mitigate those vulnerabilities. This paragraph(s) should indicate the JFOB's susceptibility to attack and should identify those vulnerabilities that form the basis for determining FP measures. Likewise, for units deploying to the area of responsibility (AOR), this paragraph(s) should discuss vulnerabilities identified from pre-deployment site surveys. Information derived from the vulnerability assessment will be classified in accordance with the Defense Threat Reduction Agency (DTRA) Security Classification Guide.

(4) Risk Assessment. Examine risks to determine possible event likelihood and consequences based upon the threat assessment; asset criticality; vulnerability assessments; and the ability to deter, defend, mitigate, and recover from an incident.

(5) FP condition (FPCON) (if applicable). Identify the current FPCON, if applicable (DoD FPCONs are normally not applicable in combat zones). The current FPCON can be obtained on the USCENTCOM JSD SIPRNET homepage.

b. **Friendly**. The following subparagraphs list the units, ships, personnel, and locations covered by the JFOB FP plan.

(1) Location of local U.S. forces. List all units at the JFOB or deployment location(s) within the JFOB AOR. Include major weapon system types and numbers and troop numbers-on the JFOB, ashore, in port, and at sea.

(2) Location(s) of other U.S. organizations/agencies. List any U.S. Government organizations, agencies, or facilities located nearby. Include emergency contact phone numbers.

(3) Type and number of security personnel and equipment. List the number of U.S. security forces, weapons, ammunition/explosives, and equipment. List any specific situations that might affect security capabilities (host nation (HN) storage, concealed weapons requirements, etc.). Also, include any other U.S. forces that are armed or have explosives (aircrew, explosive ordnance disposal (EOD), Marine expeditionary unit (MEU), AFOSI, Patriot missile batteries, etc.).

(4) Response Forces. In the following subparagraphs, explain response force composition, capabilities and responsibilities:

(a) Police/Security Forces

(b) Quick Reaction Forces (QRF)

(c) Fire/Rescue

(d) Medical

(e) EOD

(f) Chemical, biological, radiological, nuclear, or high explosives (CBRNE)

(g) Engineer/Public Works

(h) Attachments and Detachments. List here or refer to an annex.

(i) Other Agencies. This list would include other U.S. or HN entities not in direct control of the JFOB commander (e.g. Central Intelligence Agency (CIA), ISF, DoS). Include coordinating instructions as necessary.

(5) HN/allied security capability. List all HN or allied security capabilities. When available, include numbers of troops and weapons carried. This paragraph should also discuss/summarize any Memorandums of Understanding (MOUs) and Memorandums of Agreement (MOAs) that have been established with the HN or local authorities to complement and enhance the overall FP plan.

c. **General**. Provide any details that may clarify the current FP situation, if needed. Include considerations, such as the following, that would directly affect the situation:

(1) Tactical Situation Possibilities. The commander's planning guidance may provide details for this paragraph.

(2) Personnel Situation. The personnel officer may provide details for this paragraph.

(3) Logistic Situation. The logistics officer may provide details for this paragraph, which should address the general incident response logistics situation and not simply be a restatement of the ADMINISTRATION AND LOGISTICS section of this plan.

(4) Legal Situation Possibilities. The staff judge advocate may provide details for this paragraph.

(5) Public Affairs Considerations. The Public Affairs Office (PAO) may provide details for this paragraph.

(6) Civil Affairs Considerations. Civil Affairs/J-5 or equivalent may provide details for this paragraph.

(7) Cultural Considerations. The Chaplain or Civil Affairs Officer may provide details for this paragraph.

d. **Assumptions**. Provide assumptions used as a basis for this plan (e.g., strength of response force to be supported, support available from other agencies).

2. **MISSION**. Describe the JFOB FP mission scope and requirements.

3. **EXECUTION**. The following subparagraphs discuss the factors that affect the implementation of the JFOB FP:

a. **Commander's Intent**. List the JFOB commander's intentions, goals, and objectives concerning the JFOB FP mission.

b. **Key Tasks and Responsibilities**. List the key tasks and the sections responsible for those tasks. Be sure to address both the development and execution of the JFOB FP plan. For example, if the JFOB is divided into security sectors or zones, then list the unit/commanders responsible for those sectors or zones.

c. **Concept of FP**. The following subparagraphs should provide the plan specifics:

(1) **Intelligence.** Identify the methods used to integrate all sources of information concerning threats to U.S. personnel into the JFOB continuous planning and assessment process. This discussion should include how threat information flows up and down the chain of command.

(2) **Counter surveillance/Counterintelligence.** Identify associated CS/CI assets and explain how these assets will be incorporated into the JFOB FP mission. The integration of these proactive assets and techniques provides an essential means to detect and deter adversaries. Commanders must incorporate CS/CI assets into their FP plan, particularly for high threat level areas and in support of in-transit units.

(3) **Deployment/travel security measures.** List specific measures a unit will follow during deployment to the final bed-down/exercise/operations site. Consider command and control, emergency contact numbers and communications, procedures for intermediate stops, and threat notification procedures when transitioning through different AORs or countries.

(4) **Security at aerial ports of debarkation (APODs)/seaports of debarkation (SPODs).** List specific measures to follow at the air/sea ports where passengers are on/off loaded. Also consider cargo loading/unloading security measures when U.S. personnel would be at risk.

(5) **Site Specific FP measures.** List site-specific FP measures and procedures. If the DoD FPCON system is applicable, then list site-specific FPCON measures. Also describe the FPCON transition procedures. Transition procedures are required to ensure that measures are properly disseminated and implemented throughout the JFOB.

(6) **Access control/entry-control procedures.** The following subparagraphs should include the measures and procedures used to control access to the JFOB, HN controlled areas, or U.S. controlled areas/facilities.

(a) **Personnel access procedures.** Describe the procedures for personnel access into controlled or restricted areas. These areas could include the entire JFOB, restricted areas, flight lines, etc.

Address access procedures for all categories of personnel, including U.S., U.S. security forces, third country nationals (TCNs), contractors, HN, HN security, allied security, etc. This paragraph should also discuss identification badges.

(b) **Materiel access.** Describe the procedures for materiel access into the JFOB or a U.S. controlled site or facility, to include any HN requirements or procedures. The procedures should outline which vehicles and cargos are allowed into the restricted areas and what procedures are in place to control the access.

(c) **Vehicle access/search area procedures.** Describe the procedures, including any HN requirements or procedures followed at the search areas, gates, and entry control points (ECPs), if not included in a paragraph above. Discuss vehicle/personal search requirements (random, 100 percent, incoming and outgoing, etc.), methods of searching (U.S. security, addition of MWD, transmission/backscatter x-ray, vapor sensors, etc.), responsible parties (U.S. security forces, HN security, host/responsible unit, etc.), required equipment (lights, poles, ladders, ramps, creepers, SCBA, etc.), security requirements (driver segregation, overwatch, etc.) and required facilities (overhead protection, segregation walls, blast berms, air conditioning for MWDs, etc.).

(7) **Physical Security:** The following subparagraphs describe the physical security measures at JFOBs, deployment site(s), ports, and exercise areas. Include site maps in Annex C of this plan.

(a) **JFOB perimeter.** Include the physical characteristics of the JFOB or controlled-area perimeter. Discuss fence construction, physical barriers, vehicle restriction capability, security sensor systems, patrol requirements, etc. Include all perimeters (U.S. controlled perimeter, HN controlled, hedgehog barriers, vehicle berms, concertina wire, etc.). If security zones exist, discuss the zones, responsible command/unit, and measures to be implemented in each. Include site maps in Annex C of this plan.

(b) **Critical facilities.** Include the physical characteristics and entry procedures for critical or unique facilities. Discuss unique construction that impacts FP, sensor systems, access limitations, etc.

(c) **Off-site residential locations (if applicable).** Describe and list all off-site residential locations, construction, FP modifications, and any FP procedures or measures used. Include local area maps with residence locations in Annex E of this OPORD.

(8) **Random antiterrorism measures (RAMs).** List the RAMs that the JFOB will employ. The basic approach to implementing RAMs is to identify individual, site-specific FP measures that can be

randomly employed. If the list of RAMs is extensive, include it as a separate annex to this OPORD.

(9) **Off-site travel and convoy security.** Describe the procedures for all off-site travel. Discuss uniform and clothing policy, arming policy, communication requirements, minimum/maximum number of personnel, and any vehicle restrictions or issues.

(10) **Subsistence security.** The following subparagraphs address the procedures required to ensure safe food and water sources. If contract subsistence is used, address FP considerations for contracting operations.

(a) **Food.** List the FP measures used to ensure a safe food supply.

(b) **Water.** List the FP measures used to ensure a safe water supply. If potable water is not available, then include requirements for water treatment; for example, use of a reverse osmosis water purification unit (ROWPU).

(c) **Waste.** List the required FP procedures that allow for removal of waste products (waste water treatment, food waste, and septic waste). Procedures may also be included in the material access paragraphs above. Also consider site infrastructure issues and failure procedures.

(11) **Plan for arming personnel.** Describe the arming plan for the security forces. Include specific post or position requirements (i.e., M-60s at the ECPs, main gate armed with 9mm, etc.). Also include all JFOB unique requirements or changes from Service standards (i.e., weapons must be concealed; only shotguns may be used, etc).

(12) **Rules of Engagement (ROE).** Include guidance concerning the ROE for weapons use. Typically, this paragraph will reference Service specific regulations or instructions that govern ROE. Discuss any deviation from Service standards.

(13) **Use of deadly force training for security and law enforcement personnel.** Include guidance concerning the use of deadly force training for security forces.

(14) **Incident response measures.** SEE INCIDENT RESPONSE ANNEX.

(15) **Consequence management measures.** SEE CONSEQUENCE MANAGEMENT ANNEX.

(16) **Antiterrorism** (**AT) training.** The following subparagraphs include the JFOB specific training requirements. The subparagraphs are not a restatement of the training requirements, but the plan or measures used to accomplish the training.

(a) **Formal training.** List the requirements and the plan to accomplish all formal AT training (Level I, Level II, and Level III).

(b) **Initial training.** List the JFOB-specific FP or AT training required for personnel upon their arrival in the AOR and outline the plan to accomplish the training. Discuss cultural training, additional security training, local threat issues, etc.

(c) **FP Exercise.** Describe the plan to exercise the FP mission. Identify specific communication and coordination requirements between organizations on the JFOB, specifically U.S., allied, and HN security forces. FP exercises can be part of the JFOB overall exercise program.

(17) **Weapons of Mass Destruction (WMD) measures.** Describe the WMD measures the JFOB will follow. List the equipment present and the methods used for storage and distribution.

(18) **Site infrastructure issues and failure procedures.** The following subparagraphs list some of the measures used to ensure the required FP posture in the event of a system failure. These paragraphs define what is required to support the JFOB FP mission and identify facilities, areas, or sites that will require additional FP measures in the event of an infrastructure or primary system failure. The information might also be contained in the consequence management annex.

(a) **Water distribution.** List the measures security forces and utilities personnel use to maintain the required FP posture during a water distribution failure.

(b) **Power and secondary power systems.** List the measures security forces and utilities/power production personnel use to maintain the required FP posture during a power failure. Include specific details concerning the continued operations of electric power security, alarm, and detection systems

(c) **Lighting systems.** List the measures security forces and utilities personnel use to maintain the required FP posture during a lighting system failure. Include specific details about continuing FP operations without primary lighting systems.

(d) **Communications network.** List the measures security forces and utilities personnel use to maintain the required FP posture during a communication system failure. Include specific details about conducting FP operations without primary communication systems.

(19) **Post deployment requirements.** List the post deployment requirements for personnel returning to the continental United States (CONUS) or leaving the USCENTCOM AOR. Include Customs requirements or restrictions in effect.

d. **Coordinating Instructions.** Include coordination and control measures applicable to two or more elements of the command, if not addressed elsewhere.

4. **ADMINISTRATION AND LOGISTICS**.

a. **Administration**. Describe the administrative requirements for the JFOB FP Plan. The following subparagraphs detail the specialized or unique administrative requirements for the JFOB FP mission:

(1) **Personnel.** Provide required information and instructions to supporting unit personnel.

(2) **Maintenance of Unit Strength.**

(a) **Strength Reports.** Provide instructions for submitting status reports. Include requirements for routine and special reports.

(b) **Replacements.** Address instructions for validating existing personnel requisitions, for submitting requisitions, and for processing and removing replacements.

(3) **Personnel Management.** Address FP related military and civilian personnel and civilian detainee management procedures.

(4) **Mortuary Affairs.** Include evacuation procedures and handling of personal effects. Note this information may also be included in Phase IV of the execution paragraph.

(5) **Maintenance of Discipline, Law, and Order.** Include information provided by military law enforcement authorities.

(6) **Miscellaneous.** Include personnel administrative matters not specifically assigned to another coordinating staff section or included in preceding subparagraphs. Provide special instructions or special reports not covered in preceding subparagraphs.

b. **Logistics**. The following subparagraphs detail the specialized or unique equipment and materials required for the JFOB FP mission.

(1) **FP equipment lists.** List specific equipment and materials required for JFOB FP operations. The lists need to be as detailed as possible. Include coordinating instructions with the agencies or units that provide the equipment or materials. This information can also be contained in Annex F of this plan.

(2) **Maintenance and storage of FP arms and equipment.** Describe the plan for the maintenance and storage of FP equipment items and weapons/ammunition storage. Also, include any restriction or limitations concerning weapons storage (HN armory with U.S. security, no storage facility, etc.).

(3) **Off-site transportation of weapons and explosives.** Describe the plan for any restrictions and measures used for the transport of weapons and explosives while outside of U.S. controlled areas. Discuss concealment of weapons, use of explosive placards, vehicle restrictions, maximum number of weapons transported, etc.

(4) **Storage of medical supplies and materials.** Describe the plan for storage of medical supplies, materials, and chemical, biological, radiological, and nuclear (CBRN) protective equipment. Storage

and/or distribution of CBRN items may also be included in the WMD paragraph above.

(5) **FP measures in the contracting process.** Identify the measures taken to ensure that FP concerns are addressed in all aspects of the contracting process.

(6) **Materiel and Services.** Address supply, transportation, labor (e.g., location of facilities, collection points, maintenance priority), and services (e.g., type of service available, designation and location of the unit, schedule of service) required.

(7) **Medical Evacuation and Hospitalization.** Provide the plan for evacuation and hospitalization of sick, wounded, or injured personnel. Address evacuation responsibilities and air evacuation policy. Note this information may also be covered in Phase IV of the execution paragraph.

5. **COMMAND AND SIGNAL**.

a. **Command**. The following subparagraphs detail instructions regarding subordinate and higher unit command and control functions required to support the JFOB FP mission.

(1) **Command and control (C2) for JFOB FP.** Identify the C2 relationship of the forces responsible for the JFOB FP mission. Discuss security forces, command center personnel, emergency response personnel, tenant unit command and staff, etc.

(2) **Component/support agency chain of command and responsibilities.** Describe the command relationship with the JFOB, tenant units, deployed units and the higher headquarters.

(3) **FP command relationship during transit to and from deployment location.** Describe the command relationship with personnel in transit to and from a JFOB within the USCENTCOM AOR. Include requirements and responsibilities of the responsible higher headquarters.

(4) **FP Working Group composition.** List the members of the FP working group. Include meeting schedules and any other relevant administrative procedures.

b. **Signal**. The following subparagraphs detail equipment and measures required to ensure communications support to the JFOB FP mission.

(1) **Internal FP notification procedures.** Describe the plan to provide information and ensure secure communications between security and emergency response forces. Include required equipment and dedicated frequency requirements. If not contained in the incident response annex, also include incident notification guidelines and procedures.

(2) **Mass notification system.** Describe the equipment and procedures to be used to provide mass notification in the event of an attack or emergency.

(3) **External communications capabilities.** List the equipment and the capabilities required to communicate to higher headquarters and other outside agencies.

(4) **Suspicious Incident Report (SPOTREP) procedures.** List the procedures and format used to report a suspicious incident or activity.

Annex A, References. This annex contains all the references used in the development of the JFOB FP plan. If a website reference (for example, for threat information) is used, include the website URL.

Annex B, Intelligence. This annex contains all of the intelligence information used to develop the JFOB FP Plan. Normally, this information is summarized for inclusion in the plan. This annex may be classified and under separate cover.

Annex C, Site Layout/Diagram. This annex contains all of the maps and charts for the JFOB, including all barrier (fences, bollards, gates, etc.) locations and types. Indicate any exclusion zones or restricted areas.

Annex D, Barrier Plan. This annex contains the plan/measures for the storage, movement, and placement of JFOB mobile barrier systems (Jersey barriers, Bitburg barriers, HESCO barriers, etc.). Include maps displaying the barrier plan either here or in Annex C to this FP plan. Include coordination instructions for storage and transportation requirements between security forces and logistics or support personnel.

Annex E, Maps of Residential Locations. This annex contains a map of the local area surrounding the JFOB and shows all the residences of U.S. personnel.

Annex F, Lists and Locations of FP Equipment. This annex lists in detail all of the equipment and materials required for the JFOB FP mission and also storage and maintenance requirements.

Annex G, Evacuation and Assembly Procedures. This annex contains the plan for the controlled evacuation of the JFOB.

Annex H, JFOB Commander's Self-Assessments. This annex contains the JFOB commander's completed vulnerability/self-assessment checklist.

Annex I, Higher Headquarters' Vulnerability Assessments. This annex contains any higher headquarters (USCENTCOM JSD, JSIVA, etc.) vulnerability assessments. This annex may be classified and under separate cover.

Annex J, Exercise After-Action Reports (AARs). This annex contains any relevant FP exercise or operation AARs.

Annex K, FP Threat and Personal Security Briefings. This annex contains the briefings used for any JFOB FP training (formal, individual security, cultural, etc.) and the current threat briefing.

Annex L, Off-Site Residential Assessments. This annex contains the vulnerability assessment for off-site (U.S. controlled area) facilities and residences, if not included in Annex I to the FP Plan. This annex may be classified and under separate cover.

Annex M, Bomb Threat/Suspect Package Procedures. This annex contains the measures JFOB security forces and emergency response personnel follow in the event of a bomb threat or suspicious package/vehicle.

Annex N, Incident Response. ***See discussion in Incident Response Annex Template section of this chapter.***

Annex O, Consequence Management. This annex describes the consequence-management plan or measures used to mitigate casualties and damage to facilities. Include steps required to reconstitute the JFOB's ability to perform FP measures/mission. As with incident response, add instructions as needed to provide the detailed FP support requirements for consequence management functions and additional forces integration. This annex is not intended to list all requirements, but to define what is required to support the JFOB FP mission. Some information may also be contained in the incident response annex.

Annex P, BDOC SOP. ***See discussion in BDOC SOP Template section of this chapter.***

INCIDENT RESPONSE ANNEX TEMPLATE

The Incident Response Annex/Plan is a component of the overall Force Protection Program. The annex should highlight areas of concern in incident response planning. The annex is not meant to be all inclusive or followed rigidly. Planners can modify the plan format and contents to meet the needs of the JFOB, site, or other location.

JFOB FP PLAN ANNEX N: INCIDENT RESPONSE PLAN

1. **Introduction**. The Incident Response Plan is a component of the JFOB Force Protection Plan. The incident response plan is to be used for any hazard or threat to the JFOB, external emergencies, and any community emergency event that the JFOB may be asked to provide assistance. The incident response plan is structured to use the Incident Command System (ICS), and implement Standard Operating Procedures (SOPs).

2. **Purpose**. This plan describes how the JFOB will respond to emergency threats or events. The incident response plan addresses policy requirements and assumptions, and processes for a JFOB-wide response using ICS and SOPs. Procedures for coordinating security, fire, medical first responders, site-specific response measures and secondary incident concerns need to be included.

3. **Scope**. This incident response plan applies to all Service members and implements the JFOB strategy for responding to all emergency events. It is designed to respond and protect the well being of all occupants within the JFOB, protect the physical infrastructure, and allow for operational continuity to the fullest extent possible.

4. **Policy**. In the event of an emergency or disaster, the JFOB will implement the incident response plan. This action ensures that necessary services are provided to maintain a safe environment for all JFOB occupants. As required, the JFOB will work closely with tenant organizations to ensure effective interaction during response and recovery. This incident response plan and all related SOPs define the mitigation, preparedness, response, and recovery efforts necessary to minimize the potential adverse impact from all threats and events.

5. **Responsibilities**.

a. The JFOB Commander is responsible for the overall implementation of the incident response plan.

b. The base defense operations center (BDOC) officer in charge (OIC) or designated officer is responsible to act as the Incident Commander/Manager (IC), and is responsible for all JFOB response planning and actions.

c. The JFOB Emergency Program Coordinator is responsible to ensure that the incident response plan is current and assists the IC with internal (key operators) and external (community or agency) coordination.

d. The JFOB Chief of Staff is responsible for monitoring and ensuring JFOB operations and services are implemented or returned to working order.

e. The JFOB Safety Officer is responsible for monitoring and initiating actions to ensure safe actions are taken during the emergency event.

f. The JFOB Public Affairs Officer will act as the point of contact for the media and other governmental agencies that may request information concerning the incident and its impact.

g. The JFOB Security Officer (or Senior Law Enforcement Officer) ensures that lockdown and security procedures; traffic and crowd control; crime scene investigation; and perimeter control are implemented.

h. The JFOB Chief Engineer is responsible for protecting, repairing, and maintaining utility systems, communications, and equipment necessary for JFOB operation.

i. The JFOB Logistics Officer is responsible for logistical function as it relates to providing facilities, transportation, supplies, equipment, and services.

j. The JFOB Finance Officer is responsible for providing funding and tracking expenses that relate to JFOB incident response measures.

k. The JFOB Medical Officer is responsible for providing proper medical, health care, and treatment services.

l. The JFOB Fire/Rescue Chief is responsible for providing firefighting, emergency rescue, emergency medical (paramedic), and other emergency response capabilities related to fire protection and mitigation.

m. The JFOB EOD Officer is responsible for monitoring and providing first response and forensic capabilities related to bombs, IEDs, and other unexploded ordnance (UXOs).

6. **Procedures**. Whenever an emergency event or threat occurs that may require response, the IC will acquire information as to the type of event and potential impact to the JFOB (See Incident Response Report, Tab E). If the IC decides the emergency event will or may have an adverse impact to the JFOB, he or she will activate the incident response plan, which requires the following:

a. Implement the Response Checklist (See Tab C). This Checklist provides a framework to initiate assessment, planning and emergency response based on current information available.

b. Activate the EOC. The IC will contact the EOC members (See Tab A) and advise them to respond to the EOC.

c. Assess Incident Information and Evaluate. Depending upon the emergency, e.g., warning or real time event, the IC will determine the level of response based on the following:

(1) Type of event and impact to JFOB based on information received from affected operational units and/or agencies from outside the JFOB.

(a) Naturally occurring events (examples include earthquake, tornado, severe storm)

(b) Attack events (examples include rocket attack, mortar attack, sniper)

(c) Human related events (examples include bomb threat, civil disturbance, hostage/barricade situation, terrorist event)

(d) Hazardous materials events (examples include biological agents, chemical agents, radiation event, explosion)

(e) Operational continuity (examples include communications disruption, critical supplies shortage, computer system disruptions)

(f) Equipment plant and utilities (examples include alarm system failure, electrical power failure, roads and grounds blocked, water delivery/potability)

(g) Safety and security (examples include alerting and warning systems, facility access control, fire suppression systems)

(h) Health and medical (examples include evacuation, mass casualty incident, outreach)

(2) Event magnitude internally and externally

(3) Estimate likely duration.

(4) Determine potential secondary adverse events and impacts.

(5) Activate the ICS and use appropriate SOPs. [One option is to use the Key Activity Chart (See Tab D), determine which ICS units are needed (See Tab B) and which SOPs to use (See Tab I for local SOPs)].

d. Maintain current information and situation status of the emergency event.

e. Coordinate with operating units and outside agencies, as required.

f. If possible or required, consider additional EOC/incident response plan functions:

(1) Manage staff/support.

(2) Initiate hazard reduction strategies and resource issues. Use SOP key activities spreadsheet for guidance.

(3) Conduct pre-event planning.

(4) Conduct training, if applicable.

(5) Evaluate response actions and act accordingly.

(6) Initiate recovery actions when warranted.

(7) Complete situation reports (SITREPs) as required (See Tab F for format).

(8) Conduct critique of response actions and make changes as necessary.

7. **References**. Include applicable references here.

8. **Review**. Include instructions for review and revision of this plan.

Tabs:

A. EOC Membership and Contact Information

B. ICS Membership and Contact Information

C. Response Checklist

D. Key Activity Chart

E. Incident Report Format

F. SITREP Format

G. Operating Status Report Format

H. After Action Report Format

I. Incident Response Scenarios

1. Earthquake

2. Bomb Threat

3. Terrorist Event

4. [Add other tabs as required to develop incident response scenarios]

BDOC SOP TEMPLATE

The BDOC controls base defense operations within the JFOB, including incident response and consequence management functions. The BDOC SOP should focus efforts to adequately plan and resource all aspects of the BDOC mission. Planners can modify the format and contents to meet the needs of the JFOB. NOTE there is a complete sample BDOC SOP available on the accompanying JFOB Handbook CD.

JFOB FP PLAN ANNEX P: BDOC SOP

Purpose. This SOP establishes basic policy and procedures for conducting base defense operations within the JFOB AOR.

Scope. In this section explain the scope of the SOP.

Changes. This SOP is designed to be a living, working document. Explain how changes from the previous version of the SOP will be annotated and distributed (for example, red font and sent to subordinate units in the form of a G-3 fragmentary order (FRAGO)).

INTELLIGENCE SECTION

Purpose: This section provides and establishes responsibilities for planning and conducting intelligence operations in support of the BDOC.

Procedures: Explain BDOC specific Intelligence procedures here.

Responsibilities: Explain responsibilities by duty positions here. Include, at a minimum, Intelligence Officer, Intelligence non commissioned officer (NCO), and other key intelligence positions.

Battle Tasks: List specific battle tasks here. Battle tasks allow the senior commander to define tasks that integrate the battlefield operating systems, receive the highest priority for resources (such as ammunition, training areas and facilities, materiel, and funds), and receive emphasis during evaluations directed by higher headquarters.

OPERATIONS SECTION

Purpose: This section establishes responsibilities for the planning and conduct of the BDOC.

Procedures: Explain BDOC specific operations procedures here.

Responsibilities: Explain responsibilities by duty positions here. Include, at a minimum, Operations Officer, Operations NCO, and other key operations positions.

Battle Tasks: List specific battle tasks here.

PLANS SECTION

Purpose: This section provides and establishes responsibilities for the planning of future base defense and force protection operations.

Procedures: Explain BDOC specific plans for procedures here.

Responsibilities: Explain responsibilities by duty positions here. Include, at a minimum, Plans Officer, Plans NCO, and other key plans positions.

Battle Tasks: List specific battle tasks here.

LIAISON SECTION

Purpose: This section outlines the duties and responsibilities of the BDOC Liaison Section, liaison teams and liaison officers/NCOs.

Procedures: Explain BDOC specific liaison procedures here.

Responsibilities: Explain responsibilities by duty positions here. Include, at a minimum, Liaison Officer, Liaison NCO, and other key liaison positions.

Battle Tasks: List specific battle tasks here.

AREA DAMAGE CONTROL SECTION

Purpose: This section outlines duties and responsibilities necessary to maintain current operational data concerning terrain management, force protection infrastructure and engineering operations on the base complex.

Procedures: Explain BDOC specific area damage control procedures here. Include engineer asset management, terrain management, lines of communication, and infrastructure priorities. If these topics are not covered in this SOP, explain where they are located.

Responsibilities: Explain responsibilities by duty positions here.

Battle Tasks: List specific battle tasks here. At a minimum, the section should provide information related to current and future operations.

[LIST OTHER APPLICABLE BDOC SECTIONS AS REQUIRED]

EXCEPTIONS TO POLICY. List any exceptions to policy that affect BDOC Operations here.

TABS

A: Operational Graphics

B: Acronyms and Abbreviations

C: Site Layout Diagrams and Maps

D: Battle Drills

E: Forms

F: S-2/Intelligence Diagrams

G: S-3/Operations Diagrams

H: EOD reports

I: Access Control Rosters and Worksheets

J: Traffic Flow Diagrams

[Add other tabs as required to develop incident response scenarios]

RESOURCES

All links to non-U.S. Government sites or services are provided solely for convenience. Use of these links is not an endorsement of or warranty of services provided. The DoD does not exercise any responsibility over the content at such sites. NOTE: A comprehensive list of web links is available on the accompanying JFOB Handbook CD.

Air Force publications are available at www.e-publishing.af.mil. Some publications that address force protection measures are the following:

- AFTTP 3-42.32, Home Station Medical Response to Chemical, Biological, Radiological, Nuclear, or High-Yield Explosive (CBRNE) Events
- AFDD 2-4.1, Force Protection
- AFPD 10-26, Counter-Nuclear, Biological, and Chemical Operational Preparedness
- AFI 10-2501, Full Spectrum Threat Response (FSTR) Planning and Operations
- AFI 10-2502, USAF WMD Threat Planning and Response Handbook
- AFPD 32-40, Disaster Preparedness
- AFI 32-4001, Disaster Preparedness Planning and Operations
- AFI 32-4002, Hazardous Material Emergency Planning and Response Program
- AFMAN 32-4004, Emergency Response Operations
- AFMAN 32-4005, Personnel Protection and Attack Actions
- AFMAN 32-4013, Hazardous Material Emergency Planning and Response Guide

DoD Instruction 2000.18, Department of Defense Installation Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Emergency Response Guidelines, provides guidance for the establishment of a CBRNE preparedness program for emergency responders at all DoD installations. The document is available at http://www.dtic.mil/whs/directives/corres/html/200018.htm.

The **Emergency Management Institute** (EMI) serves as the national focal point for the development and delivery of emergency management training. EMI curricula are structured to meet the needs of a diverse audience with an emphasis on how the various elements work together in emergencies to save lives and protect property. There are various self-study programs available at http://training.fema.gov/EMIWeb/.

The **Emergency Response Guidebook,** developed jointly by the U.S. Department of Transportation, Transport Canada, and the Secretariat of Communications and Transportation of Mexico, is for use by firefighters, police, and other emergency services personnel who may be the first to arrive at the scene of a transportation incident involving a hazardous material. This reference is located at http://hazmat.dot.gov/pubs/erg/ gydebook.htm.

The **Federal Emergency Management Agency** (FEMA) is responsible for disaster plan, response, recovery, and mitigation functions. FEMA's Online Library has incident response reference materials, publications, maps, photographs, audio and video clips. The site is available at http://www.fema.gov/library/.

The **JAT Guide**, the only Office of the Secretary of Defense (OSD) and Joint Staff approved antiterrorism (AT) software planning tool, contains incident response and consequence management plan templates. The JAT Guide is available through Antiterrorism Enterprise Portal (ATEP) (https://www.atep.smil.mil) or contact JATguide@erdc.usace.army.mil to obtain a copy.

The Department of Homeland Security (DHS) **Lessons Learned Information Sharing** system (https:// www.llis.gov/) is the national network of lessons learned and best practices for emergency response providers and homeland security officials. The site requires registration.

The **National Response Plan** incorporates best practices and procedures from incident management disciplines and integrates them into a unified structure. Although a comprehensive all-hazards approach to U.S. federal domestic incident management, the plan provides a good overview of incident response organization and measures. The plan is located on the DHS website at http://www.dhs.gov/ dhspublic/theme_home2.jsp.

The **Office of Emergency Transportation** (OET), in the Research and Special Programs Administration (RSPA) of the Department of Transportation (DOT), performs coordinated crisis management functions for multimodal transportation emergencies. Their web site is http://www.dot.gov/ost/oet/.

REFERENCES

AFMAN 10-401 V2. *Planning Formats and Guidance*, 1 May 1998. (available at www.e-publishing.af.mil)

AR 525-13. *Antiterrorism*, 4 January 2002.

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. (available at www.dtic.mil)

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. (available at www.dtic.mil)

CJCSM 3122.03A. *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance*, 31 December 1999 w/Change 1, 6 September 2000. (available at www.dtic.mil)

DoD Instruction 2000.16, *DOD Antiterrorism Standards*, 4 June 2001. (available at www.dtic.mil/whs/directives/corres/html/200016.htm)

DoD O-2000.12-H, *DOD Antiterrorism Handbook*, February 2004. (available at www.dtic.mil/whs/directives/corres/html/o200012h.htm)

FM 5-0. *Army Planning and Orders Production*, 20 January 2005. (available at www.adtdl.army.mil)

FM 6-0. *Mission Command: Command and Control of Army Forces*, 11 August 2003. (available at www.adtdl.army.mil)

FM 101-5-2. *U.S. Army Report and Message Formats*, 29 June 1999. (available at www.adtdl.army.mil)

JP 3-10.1. *Joint Tactics, Techniques, and Procedures for Base Defense*, 23 July 1996. (available from www.dtic.mil/doctrine)

JP 3-31. *Command and Control for Joint Land Operations*, 23 March 2004. (available at www.dtic.mil/doctrine)

MCWP 5-1. *Marine Corps Planning Process*, 5 January 2000 w/Change 1, 24 September 2001. (available at www.doctrine.usmc.mil)

NWP 5-01. *Naval Operational Planning*, 1 May 1998. (available at www.nwdc.navy.smil.mil)

This page intentionally blank

Chapter 15

ACRONYMS / TOOLS

Contents

ACRONYMS

* A-B *

AAR……After Action Report
AASHTO……American Association of State Highway and Transportation Officials
ABCS.....Army Battle Command System
ABD.....Air Base Defense
ABM/UBM.....Automated Building Machine/Ultimate Building Machine
AC……..Active Component
ACP……Access Control Point
ADCON.....Administrative Control
ADVON.....Advanced Echelon
AFCEE .....Air Force Center for Environmental Excellence
AFCESA.....Air Force Civil Engineer Support Agency
AFCS .....Army Facilities Component System
AFDC .....Air Force Doctrine Center
AFMAN.....Air Force Manual
AFOSH.....Air Force Occupational Safety & Health
AFOSI.....Air Force Office of Special Investigations
AFRC.....Air Force Reserve Command
AFS.....Air Force Station
AFSC .....Air Force Specialty Codes
AFSOC .....Air Force Special Operations Command
AFTL .....Air Force Task List
AIF.....Anti Iraqi forces
ALO……Air Liaison Officer
AM.....Amplitude Modulation
AMETL .....Agency Mission Essential Task List

AO .....Area of Operation
AOI.....Area of Influence
AOR.....Area of Responsibility
APCO .....Association of Public Safety Communications Officials
APOD .....Aerial Port Of Debarkation
ARC.....Air Reserve Component
ARFF .....Aircraft Rescue Fire Fighting
ASAALT .....Assistant Secretary of the Army for Acquisition, Logistics, and Technology
ASCC.....Army Service Component Commander
ASDIA.....All Source Document Index
ASG .....Area Support Group
ASOC…….Air Support Operations Center
AT……..Antiterrorism
ATEP .....Antiterrorism Enterprise Portal
ATO.....Antiterrorism Officer
ATWG .....Antiterrorism Working Group
AUTL .....Army Universal Task List
AVS……Automated Video Surveillance
AWS……...Alert Warning System

BASOPS .....Base Operations
BCOC .....Base Cluster Operations Center
BDOC .....Base Defense Operations Center
BDT .....Base Development Team
BOS .....Base Operating Support

* C-D *

C2 .....Command and Control
C4I…….Command, Control, Communications, Computers, and Intelligence
CALL.....Center for Army Lessons Learned\
CAT .....Crisis Action Team
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
CCA.....Contract Construction Agents
CCIR.....Commanders Critical Information Requirement
CCTV .....Closed Circuit Television
CD.....Chemical Defense / Compact Disc
CDM .....Chemical Downwind Message
CDR.....Commander
CE .....Civil Engineer
CEA .....Captured Enemy Ammunition

CES.....Civil Engineering Squadron
CFLCC .....Combined Force Land Component Command
CHS……Combat Support Hospital
CI .....Counterintelligence
CIA……Central Intelligence Agency
CIB .....Compressed Image Base (also Command Information Bureau)
CID .....Criminal Investigation Division
CIP.....Critical Infrastructure Protection
CIR .....Critical Information Requirements
CJCS .....Chairman, Joint Chiefs of Staff
CJTF .....Combined Joint Task Force
CLS.....Combat Lifesaver
CM.....Consequence Management
CMU .....Concrete Masonry Unit
COA.....Courses Of Action
COB.....Collocated Operations Base
COC.....Combat Operations Center
COCOM .....Combatant Commander
COLISEUM.....Community On-Line Intelligence System for End Users and Managers
COMSEC.....Communications Security
CONOPS .....Concept of Operations
CONUS.....Continental United States
COP .....Common Operating Picture
COR.....Contracting Officer Representative
COSC……Combat Operational Stress Control
COTR .....Contracting Officer Technical Representative
COTS.....Commercial Off-The-Shelf
CPA .....Coalition Provisional Authority
CREST.....Corps of Engineers Real Estate Teams
CRREL.....Cold Regions Research & Engineering Lab
CSB.....Corps Support Battalion
CS/CI .....Counter-Surveillance and Counterintelligence
CSD .....Command Supply Discipline
CSG .....Corps Support Group
CSIL .....Commercial Satellite Imagery Library
CTCSS.....Continuous Tone Coded Squelch System
CTT.....Complete Common Task Training
CVAMP.....Core Vulnerability Assessment Management Program
CWDE……Chemical Warfare Defense Equipment

DCSENGR .....Deputy Chief of Staff, Engineer
DEPSECDEF.....Deputy Secretary of Defense
DERF.....Defense Emergency Response Funds
DES.....Data Encryption Standard
DFAC .....Dining Facility
DHS……Department of Homeland Security
DIA.....Defense Intelligence Agency

DoD .....Department of Defense
DON .....Department of the Navy
DONCIP.....Department of the Navy Critical Infrastructure Protection
DOQ .....Digital Orthophoto Quad
DOS .....Department of State
DOT.....Department of Transportation
DPW .....Director of Public Works
DSN .....Defense Switched Network
DTRA .....Defense Threat Reduction Agency

* E-F-G *

EAC .....Echelon Above Corps
EAD.....Echelons Above Division
ECP.....Entry Control Point
ECR……Effective Casualty radius
EDD.....Explosive Detector Dog
EEI.....Essential Elements of Information
EEFI.....Essential Elements of Friendly Information
EMI……Emergency Management Institute
ENVST .....Environment Support Team
EOC .....Emergency Operations Center
EOD.....Explosive Ordnance Disposal
FPL……Final Protective Line
EPW.....Enemy Prisoner of War
ERDC .....U.S. Army Engineer Research and Development Center
EW.....Electronic Warfare

FCC.....Federal Communications Commission
FEMA .....Federal Emergency Management Agency
FEST.....Forward engineer support team
FEST-A.....Forward engineer support team-augmentation
FEST-M.....Forward engineer support team-main
FET .....Field Engineering Team
FFE .....Field Force Engineering
FFIR.....Friendly Forces Intelligence
FFP .....Firm, Fixed Price
FM .....Factory Mutual / Field Manual / Frequency Modulation / Financial Management
FOO .....Field Ordering Officer
FOB .....Forward Operations Base
FP……..Force Protection
FPCON .....Force Protection Condition
FPTAS .....Flight Path Threat Analysis Simulation
FPWG.....Force Protection Working Group
FRAGO.....Fragmentary Order
FRAGOs.....Fragmentary Orders
FRS.....Family Radio Service

FSCC .....Fire Support Coordination Center
FSCCRD……Fire Support Coordinator
FSE .....Fire Support Element
FT .....Feet
FUSB .....Facilities Utilization and Support Board

G-2.....Intelligence Staff (hyphen may be omitted, as in G2)
G-3……..Operations, Plans, and Training Staff
GPS.....Global Positioning System
GPTO…….General Purpose Tape Obstacle
GS .....General Support
GSA .....General Services Administration
GSR……Ground Surveillance Radar

* H-I-J *

HAZMAT .....Hazardous Material
HF .....High Frequency
HHQ AT .....Higher Headquarters Antiterrorism
HID .....High Intensity Discharge
HMMWV……..High-Mobility, Multipurpose, Wheeled Vehicle
HN .....Host Nation
HPAC .....Hazard Prediction and Assessment Capability
HQ AMC .....Headquarters, Air Mobility Command
HSS……Health Service Support
HRB.....High Risk Billet
HRP .....High Risk Personnel
HRT .....High Risk Target
HUMINT .....Human Intelligence
HVAC.....Heating, Ventilation, and Air Conditioning

IAT .....Infrastructure assessment team
IAW .....In Accordance With
IC……. .....Incident Commander
ICP…….Incident Command Post
ICR .....Intelligence Collection Requirements
ICS…….Incident Command System
IDS.....Intrusion Detection System
IED .....Improvised Explosive Devices
IIG.....Interim Iraqi Government
IJQS .....Initial Job Qualification Standard
INFOSEC…… ..Information Security
INMARSAT .....International Marine/Maritime Satellite
INTEL.....Intelligence
IPB.....Intelligence Preparation of the Battlespace
IPDS .....Inland Petroleum Distribution System
IR .....Incident Response
IRC…….Incident Response Center
IRISA.....Intelligence Report Index Summary File

IS.....Intrinsically Safe
ISO.....International Standards Organization
ISR.....Intelligence, Surveillance, Reconnaissance

JAT Guide .....Joint Antiterrorism Manager's Guide
JCS.....Joint Chiefs of Staff
JFC.....Joint Force Commander
JFOB.....Joint Forward Operations Base
JIEDDTF .....Joint Improvised Explosive Device Defeat Task Force
JIPB .....Joint Intelligence Preparation of the Battlespace
JISE.....Joint Intelligence Support Element
JOC…….Joint Operations Center
JSD…….Joint Security Directorate
JSIVA .....Joint Service Integrated Vulnerability Assessment
JSLNBCRS.....Joint Service Lightweight NBC Recon System
JTRS .....Joint Tactical Radio System
JTTP .....Joint, Tactics, Techniques, and Procedures
JWFC.....Joint Warfighting Center

* K-L-M-N *

LAN.....Local Area Network
LCD .....Liquid Crystal Display
LE……..Law Enforcement
LEP .....Locally Employee Personnel
LIC.....Low-Intensity Conflict
LMR .....Land Mobile Radio
LN.....Local National
LNCP.....Local National Control Point
LNO……..Liaison Officer
LOC .....Lines Of Communications
LOGCAP .....Logistics Civilian Augmentation Program
LOGSA.....Logistics Support Activity
LOP.....Levels Of Protection
LP .....Listening Post
LPI/LPD .....Low Probability of Intercept/Low Probability of Detection
LSA.....Logistics Support Area

MAJCOM .....Major Command
MANPAD.....Man-Portable Air Defense
MCCDC.....Marine Corps Combat Development Command
MCP.....Mobile Command Post
MCV .....Munitions Clearance Vehicle
MDITDS.....Modernized Defense Intelligence Threat Data System
MDMP.....Military Decision-Making Process
MET.....Mission Essential Tasks
METL .....Mission Essential Task Lists

METT-TC……..Mission, Enemy, Terrain and Weather, Troops Available and Civilian
MEU……..Marine Expeditionary Unit
MEVA .....Mission Essential Vulnerable Asset
METL .....Mission Essential Task List
MHE .....Materials Handling Equipment
MHz.....Megahertz
MIL……Military
MILCON .....Military Construction
MNC-I .....Multinational Corps-Iraq
MNF .....Multinational Forces
MNSTC-I.....Multinational Security Transition Corps-Iraq
MOA.....Memorandum Of Agreement
MOB.....Main Operating Base
MOOTW.....Military Operations Other Than War
MOU.....Memorandum of Understanding
MP .....Military Police
MSA……...Munitions Storage Area
MSC……...Major Subordinate Command
MSHARPP .....Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
MSR.....Main Supply Routes
MTOE……Modified Table of Organization and Equipment
MTW .....Major Theater War
MWD.....Military Working Dog
MWR.....Moral, Welfare, and Recreation

NAVFAC.....Naval Facilities and Engineer Command
NBC.....Nuclear, Biological, Chemical
NBCC .....Nuclear, Biological, Chemical, and Conventional
NBCCC.....NBC Control Center
NCD……...Net Control Device
NCIS .....Naval Criminal Investigative Service
NEC .....National Electrical Code
NEO.....Noncombatant evacuation operation
NES.....NIMA National Exploitation System
NFPA.....National Fire Protection Association
NGA .....National Geospatial-Intelligence Agency
NGO .....Non Governmental Organization
NIMA.....National Imagery and Mapping Agency
NIPRNET .....Non-Classified Internet Protocol Router Network
NIST .....National Institute of Standards and Technology
NSA .....National Security Agency
NTIA.....National Telecommunications and Information Administration
NTTL.....Naval Tactical Task List
NVD……...Night Vision Device
NWDC.....Navy Warfare Development Command

* O-P-Q-R *

O&M.....Operations and Maintenance
OCONUS.....Outside the Continental United States
OET……Office of Emergency Transportation
OFDA .....Office of Foreign Disaster Assistance
OIC……Officer in Charge
OIF.....Operation Iraqi Freedom
OIS…….Officer Information System
ONC.....Operational navigational charts
OP……..Observation Post
OPCON……..Operational Control
OPLAN……..Operations Plan
OPORD.....Operations Order
OP .....Observation Post
OPS.....Operations
OPSEC.....Operations Security
OSD……Office of the Secretary of Defense

PAO .....Public Affairs Office
PDC .....Protective Design Center
PDF……Principal Direction of Fire
PIDS .....Perimeter Intruder Detection System
PIR.....Priority Intelligence Requirements
PKO .....Peacekeeping Operations
POD .....Port Of Debarkation
POL.....Petroleum, Oils, and Lubricants
PPBE.....Program Planning and Budgeting Execution
PPE……Personal Protective Equipment
Prime BEEF.....Prime Base Engineer Emergency Force
PVNTMED……Preventive Medicine Program
PX .....Post Exchange

QRF .....Quick Reaction Force
QRT……Quick Reaction Test

RA.....Risk Assessment
R&D .....Research and Development
RAM .....Rockets, Artillery, Mortars
RAMP.....Return fire, Anticipate attack, Measure, and Protect
RAMs .....Random Antiterrorism Measures
RAOC .....Rear Area Operations Center
RED HORSE .....Rapid Engineer Deployable Heavy Operation Repair Squadron Engineer
RFF .....Request For Forces
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
RSPA…….Research and Special Programs Administration
RSTA.....Reconnaissance, Surveillance, and Target Acquisition
RTOC .....Rear Tactical Operations Center

* S-T *

SAF.....Secretary of the Air Force
SAFE .....Secure Analyst File Environment
SAM .....Surface to Air Missile
SAR……Search And Rescue
SASO.....Stability And Support Operations
SBU .....Sensitive But Unclassified
SCBA…….Self-Contained Breathing Apparatus
SDR .....Software-Defined Radio
SECDEF .....Secretary of Defense
SECSTATE .....Secretary of State
SFI…….Security Force Instructions
SIGINT.....Signals Intelligence
SINCGARS .....Single Channel Ground to Air Radio System
SIPRNET.....Secret Internet Protocol Router Network
SITREPS.....Situation Reports
SJA .....Staff Judge Advocate
SLUDGEM……Salivation, Lacrimination, Urination, Defecation, Gastric Emesis, Miosis
SMCT .....Soldier's Manual of Common Tasks
SME……Subject Matter Expert
SOC .....Special Operations Command
SOFA.....Status Of Forces Agreement
SOG .....Sergeant Of the Guard
SOLIS.....Signals Intelligence On-line Information System
SOP.....Standing Operation Procedure
SOW .....Statement Of Work
SPL…… ....Sound Pressure Level
SPOD.....Sea Port Of Debarkation
SRC.....Survival Recovery Center
SRG .....Special Republican Guard
SSA.....Simplified Survivability Assessment
SSI……..Special Security Instructions
SSO……Special Security Orders
STDTT…….....Security Technology Decision Tree Tool
STE.....Secure Telephone Equipment
SWA .....Southwest Asia
SWEAT .....Sewer, Water, Electricity, Academics, Trash

TA.....Threat Assessment
T&E……Traversing and Elevation
T&M.....Time and Materials
TACON……..Tactical Control

TALCE .....Tanker Airlift Control Element
TCE.....TeleEngineering Communication Equipment
TCF……Tactical Combat Force
TCM .....Terrorist Consequence Management
TCMS .....Theater Construction Management System
TCN .....Third Country National
TCP……Traffic Control Points
TEOC.....TeleEngineering Operations Center
TETK.....TeleEngineering Toolkit
TL .....Threat Likelihood
TOC .....Tactical Operations Center
TOE……Table of Organization and Equipment
TPC.....Tactical Pilotage Charts
TRADOC.....Army Training and Doctrine Command
TTP .....Tactics, Techniques, and Procedures
TWG.....Threat Working Group

* U-V-W-X-Y-Z *

UFC .....Unified Facilities Criteria
UFR .....Unfunded Requirements
UGS……Unattended Ground Sensors
UHF .....Ultra-High Frequency
UJTL.....Universal Joint Task List
UN .....United Nations
UNTL .....Universal Naval Task List
UPS.....Uninterrupted Power Supply
USACE.....U.S. Army Corps of Engineers
USARUER .....United States Army, Europe
USCENTCOM .....United States Central Command
USCENTCOM AOR.....United States Central Command Area of Responsibility
USG .....United States Government
USGS.....U.S. Geological Survey
USJFCOM .....U.S. Joint Forces Command
US&P.....United States and Possessions
USSOCOM.....United States Special Operations Command
UTC .....Unit Type Code
UTM .....Universal Transverse Mercator
UXO .....Unexploded Ordinance

VA .....Vulnerability Assessment
VBIED.....Vehicle-Borne Improvised Explosive Devices
VET……Verbal Test
VETTED……Background Check Conducted
VHF .....Very High Frequency
VMD……..Video Motion Detection
VUL.....Vulnerability

WMD.....Weapons of Mass Destruction

WMP-1 .....War Mobilization Plan Volume 1
WVAT……Weather Vulnerability Assessment Tool

TOOLS

The following tools are useful in developing an effective force protection (FP) Program. Most of these tools are furnished on the JAT Guide Program CD and the Joint Antiterrorism (JAT) Guide Tools CD. Since the JAT Guide is available on the Antiterrorism Enterprise Portal (ATEP), the tools can be downloaded from the Secret Internet Protocol Router Network (SIPRNET) or Non-Classified Internet Protocol Router Network (NIPRNET) ATEP site. A few tools are available from originating agencies.

CAUTION: When data specific to the JFOB are used with some of these tools, the resulting electronic files or hard copy documents may be classified. Check the "DTRA Force Protection Security Classification Guidelines" and service guidelines and with your security manager for proper classification level. In general, if the data or information would assist an attack, they are classified. For example, classification would occur if the data or information reveals specific risks, vulnerabilities, attack tactics that could succeed, times when an attack could produce maximum consequences, or the level of concern about such an attack.

PRE-DEPLOYMENT SITE SURVEY

A pre-deployment site survey is used to develop a significant amount of information needed in planning for deployment. Much of the survey can be completed prior to a boots-on-the-ground site survey and a list of required information developed for the visit.

General
☐ What is the JFOB name?
☐ Any previous JFOB names or identifiers?
☐ What is the JFOB mission?
☐ Location? (Northern Iraq, Southern Iraq, Eastern Iraq, Western Iraq, Sunni Triangle area, Other)
☐ Have you consulted the OPORD from the Combatant Commander?
☐ Has a country clearance been granted to all members of the PDSS team, if required?
☐ Is there a Status of Forces Agreement (SOFA) to review before the PDSS occurs?
☐ Which Service is responsible for antiterrorism at the JFOB?
☐ Has the U.S. Embassy been contacted, if required, with regard to conducting a pre-deployment site survey?
☐ Has the JFOB's current FP officer been contacted for essential data such as threat, maps, imagery, vulnerability, risk assessments, etc. for the PDSS? Has that data been assembled for members of the PDSS team?
☐ What is the status of the JFOB FPWG-active, inactive, non-existent? Is it experienced, inexperienced?
☐ Does the FPWG have the proper composition? Have the following functions been included in the FPWG - Installation and unit FP officer (FPO), engineer, resource management, provost marshal, medical, intelligence, public affairs, logistics, legal, explosive ordnance disposal (EOD), safety, tenant, and certain functions in other agencies as requested?
☐ If needed, has the host (HN) nation been contacted with regard to a pre-deployment site survey?

☐ Are there civil/political considerations that affect force protection? Who will handle them?
☐ Are there HN agreements, international agreements, or treaties that specify U.S. involvement in operations? If so, where are they referenced for consultation?
☐ Is a Base Defense Operations Center (BDOC) planned or already in place on the site? If not, what will be the central point for base defense operations?
Pre-Deployment Site Survey Team
☐ Has the PDSS team been selected with recommended functions (FPO, engineer, military police, etc.)?
☐ Is site-related FP data being collected and assembled for future users?
☐ Has someone been identified as the PDSS data keeper? In what form(s) (paper or electronic) is the data stored? Is another location being used as an alternate site or backup for storage of the data? If so, where? Who is the point of contact at the other location?
☐ Who has/will be tasked to assemble a Continuity of Operations book?
☐ Who are the primary and alternate coordinators between the PDSS team and the FPWG?
☐ Has the PDSS team assembled plans and recommendations? Where are those data available?
Existing Site Situation (if deployment is to an existing JFOB)
☐ What is HN role in JFOB security and what is its capability?
☐ Is AT training provided to all personnel before arrival on the site?
☐ Have vulnerability assessments been completed on the Iraqi police stations?
☐ Has the U.S. obtained diagrams and pictures from the roofs and ground around the police stations?
☐ What emergency evacuation measures, site improvements, and physical security actions need to be planned and implemented at Iraqi police stations?
☐ Are various drills such as bomb threat drills conducted?
☐ Are defensive driving briefings and training conducted particularly for offsite travel?
☐ Is off-street secure parking available?
☐ What is the site population?
☐ What units are on the site - logistics, security forces, engineering, infantry, armor, artillery, aviation, maintenance, etc?
☐ What is the site population count of government civilians: U.S., HN, or coalition?
☐ What is the site population count of non-government civilian contractors: U.S., HN, or coalition?
☐ What is the command and control structure/relationships between units?
☐ What units (to include tenants) has the JFOB commander designated responsible for FP and what are their roles and areas for protection?
☐ Have the following products been produced?
☐ Threat Assessment
☐ Vulnerability Assessment
☐ Risk Assessment
☐ If the products have not been produced, what is the schedule for their completion?
☐ Have the results of the assessments been used for planning and implementation of FP activities?
☐ Have vulnerability and associated data been entered into Core Vulnerability Assessment Program (CVAMP)?
☐ Have personnel received cultural awareness training or its equivalent in order to work better with the local culture?
☐ Are local transportation services used to get on and off the JFOB? If so, what force protection measures are used to guarantee security?

Site Selection and Layout
☐ Has the PDSS team obtained maps and imagery of the location of the PDSS? Recommended minimum imagery resolution is 1 meter. Use commercial and government-provided imagery of the appropriate security classification level as needed.
☐ Have maps and imagery been made available to all members of the team either electronically or on paper?
☐ If the site is a port, are the necessary coastline, depth, and port data available to ships, small boats, and other watercraft to avoid mines or attacks from small watercraft?
☐ What critical assets will be placed or are already on the site?
☐ Have plans been made for the placement of assets with regard to standoff and dispersion?
☐ Are there nearby levees or dams which should be considered for their effects on FP if they break due to natural forces or enemy action?
☐ Has the terrain been evaluated to consider flooding, snowfall, shifting sand, or other difficult environmental conditions with the associated impact on FP?
☐ Is there nearby geological activity that could affect FP due to its consequences, i.e., earthquake, volcano?
☐ Have assembly or rally points been designated in case of emergency evacuation ? Have these points been designated on maps/imagery for quick reference?
☐ What areas with obstacles, terrain, and vegetation have been identified that could be hiding places for enemy forces prior to or during an attack and are identified on a map or imagery?
☐ Are there planned efforts to remove obstacles and vegetation and/or modify terrain to reduce potential hiding places by the enemy?
☐ What man-made obstacles or buildings in the vicinity of the airfield could be used by the enemy to attack aircraft, vehicles or personnel and are designated on a map or imagery?
☐ Have potential enemy areas of approach been identified on maps or imagery of the site?
☐ Have areas of enemy support in the local population or enemy locations been identified on maps and imagery?
☐ Are nearby minefields, if any, marked on a map or imagery for avoidance by all personnel?
☐ Does the layout of the site conform to the concept of a layered defense-in-depth?
☐ What is the expected population of the JFOB - U.S. personnel, HN personnel, and contractors?
☐ Have locations been selected for installation of mass notification systems?
☐ Does the layout of the site provide roadways of sufficient width for emergency vehicles to travel quickly from their stations to all parts of the site?
☐ Has a layout for placement of FP-related equipment been noted on a map or image? (Barriers, watch towers, etc.) Has this data been given to the FPO and FPWG for review, analysis, and coordination?
☐ Have security zones been planned? Have those security zones been marked on a map or image of the site?
☐ Have the threat, vulnerability, and risk analysis results been used to guide the placement of critical assets onsite?
☐ Have these results been used to guide the placement of protective equipment and material (barriers, window glazing, towers) to mitigate risk?
☐ Are emergency evacuation procedures in place?
☐ Have off-limits areas related to FP been marked on maps/imagery for easier location and identification?

☐ Are locations for communications antennas identified and marked on maps/imagery?
☐ If the threat assessment includes a MANPADS attack against aircraft, have illustrations of the "SAM Footprint" (Surface-to-air missile footprint) been included on maps or imagery for review, analysis, and planning? (The tool Flight Path Threat Analysis Simulation is helpful here.)
☐ Have maps and imagery been marked either electronically or on paper to show entrances, exits, evacuation routes, placement of housing, critical infrastructure points (1phone, sewage, electricity, etc.), major supply routes, lines of communication, security zones, etc.?
☐ Have the locations for sensor systems/intrusion detection systems, etc. been pre-planned and marked on maps/imagery for placement?
☐ Were the sensor/intrusion detection systems tested to ensure they work at the times of day and under the conditions you expect to occur when they are needed? Were the sensors locations analyzed for maximum effectiveness?
☐ Are streams, drainage ditches, and tunnels that enter the perimeter marked on maps or imagery for FP planning use?
☐ Have lighted areas been identified? Has this been coordinated with other members of the team?
☐ Have the characteristics of existing buildings been assembled for the vulnerability assessment and risk analysis? These include the type of construction-concrete, wood frame, etc.
Threat
☐ Has a threat assessment for the site been conducted?
☐ Has the threat assessment been given to team members for their individual and the team's collective planning?
☐ What information does the threat assessment provide with regard to groups, tactics, weapons, and targets?
☐ Has a communications channel for threat data been established between the U.S. Embassy, the COCOM, ships (if applicable), local police stations and other local forces?
☐ Have potential enemy areas of approach been identified on maps or imagery of the site?
☐ Have areas of enemy support in the local population or enemy locations been identified on maps and imagery?
☐ How will updated/modified threat information be transmitted to FP personnel?
☐ Are counter-surveillance and counter-intelligence activities built into the AT plan?
☐ Have enemy tactics and weapons been analyzed for potential use against the site? If so, what were those tactics and weapons?
Risk Analysis
☐ Have the results of the following products been used in the risk analysis?
☐ Threat Assessment
☐ Vulnerability Assessment, including Incident Response Capability
☐ Risk Assessment
☐ If the products have not been produced yet, what is the schedule for their completion?
☐ Has a vulnerability assessment been conducted? What were the results? Have the results been given to all members of the team?
☐ Has vulnerability and associated data been entered into Core Vulnerability Assessment Program (CVAMP)?
☐ Are vehicles parked near buildings? Has an analysis been completed regarding potential explosive effects against the building and its occupants? Has a minimum distance from the building for parked vehicles been determined and enforced?
☐ Have analytical tools such as AT Planner, Hazard Prediction and Assessment Capability (HPAC), and Flight Path Threat Analysis Simulation (FPTAS) been used to predict weapons effects against the critical assets (personnel, equipment, etc.)?

☐ Has an analysis been conducted regarding aircraft entering or departing the site's airfield?
☐ Has an analysis been conducted regarding ships or other vessels entering, docked, or departing the port?
☐ If a Joint Staff Installation Vulnerability Assessment (JSIVA) was completed within the last year, has it been reviewed for identification of vulnerabilities and a reduction in the number and kind of vulnerabilities?
☐ Are briefings supplemented with use of deadly force/scenario based training for all personnel required to perform law enforcement and security duty?
☐ Are all personnel aware of the local Rules of Engagement (ROE)?
☐ Who is responsible for coordinating relief efforts with government and international agencies?
☐ Are established control areas coordinated with HN to minimize interference, misunderstandings, and collateral damage?
☐ Have safe havens been identified in offices and residences?
☐ Are visits of high risk personnel identified, tracked, and coordinated, i.e., name, date of visit, travel mode, accompanying personnel, dignitaries, baggage handling?
Perimeter Security
☐ What avenues of approach or departure outside the perimeter are available in case of emergency or natural disaster?
☐ What road conditions to and from the site will impede personnel transport and subject them to danger from the threat?
☐ Have enemy avenues of approach been identified?
☐ What nearby rail lines are subject to danger from the threat?
☐ What nearby bridges are subject to danger from the threat?
☐ What nearby airfields are subject to danger from the threat? Include boundaries, parking ramps, taxiways, etc.
☐ What nearby ports are subject to danger from the threat?
☐ What protective measures will be emplaced at the airfield boundaries for security of aircrews and aircraft?
☐ What transportation vehicles will be needed for transportation outside the perimeter, i.e., humvees, tractor trailers, sedans, pickups, etc.?
☐ What types of up-armored vehicles will be needed?
☐ What types of armored vehicles will be needed, i.e., tanks, fighting vehicles, etc.?
☐ Have fields of fire been identified and evaluated from a force protection perspective?
☐ What barriers and/or protective devices on the perimeter are available to mitigate the consequences of an attack - barriers, protective film, detection and warning systems, etc?
☐ How many and what type of traffic barriers will be used for traffic control, inspection, and entry control?
☐ What type of guard positions will be used - ground level guard building, elevated tower, fixed fighting position, and/or bunker?
☐ Has the placement of watch towers for overwatch been evaluated for effectiveness? How many watch towers will be emplaced?
☐ Are earthen berms needed as barriers?
☐ Is there a truck/bulk/commercial delivery entrance separate from personnel carrier entrance(s)?
☐ Are entry control points (ECP) configured so attackers cannot run the entrance(s)?
☐ Are ECP configured so attackers cannot run the exit lane(s)?
☐ Are intrusion detection systems in use for the JFOB perimeter? What types are they?
☐ What sensor systems (radiation detectors, x-ray machines, metal detectors, etc.) will be emplaced for alert and warning before vehicles or personnel enter the site?
☐ Is emergency power backup available for communications and monitoring systems at

	the perimeter?
☐	How will FP equipment (barriers, sensor systems, etc.) be moved to the site if needed, i.e. pickup, tractor-trailer rig, aircraft, ship, etc.?
☐	What construction equipment will be needed to construct berms, watch towers, entry control points as needed - forklifts, dozers, graders, etc.?
☐	Will the site perimeter and/or flight line be patrolled or monitored electronically? If monitored electronically, what monitoring equipment will be used? Is monitoring being done continuously?
☐	Is the entire perimeter fence line in view of patrolling guards?
☐	Have "No Trespassing" or other types of warning signs been placed on the fence?
☐	Have no fire areas been designated to protect civilians, prevent disruption of operations, and protect combat outposts and patrols been designated and updated?
☐	Will private vehicles be allowed onsite? If so, how will they be checked and registered?
☐	What are the procedures for detecting personnel wearing or carrying improvised explosive devices (IEDs) in packages?
☐	What type of hands-on or similar inspection tools are available - mirrors, ladders lights, ramps, mechanic's creepers, etc. for vehicle inspection?
☐	Are military working dogs available for explosive detection at the gate?
☐	What random AT measures are considered for use at the site? Are they actively implemented?
☐	If the site is a port, have defensive measures against swimmers and small craft been considered and prepared?
☐	How will the area around ships be monitored and protected?
☐	Will inspection of visitors and their parcels be conducted?
☐	What type of inspections before entry onsite will be conducted of vehicles and watercraft?
☐	Do you have procedures for dealing with a situation where a suspected IED is discovered (vehicle or person)?
☐	What measures have been put in place (permanent and procedural) to minimize casualties and damage if a VBIED driver is detected or delayed or loses his/her nerve, and detonates?
☐	Is there a HN restriction on the use of air defense systems?
☐	Are alternate airfields planned for use in case the risk for the JFOB airfield and aircraft becomes too great?
☐	Do security zones include waterways and ports? If not, when will they be included?
☐	Are there any breaches in fences or other barriers? If so, are they marked on maps or electronically marked and identified for repair? Who is responsible for monitoring the breaches until repaired?
☐	Are there any places where streams and/ or drainage ditches and tunnels enter the perimeter barrier? If so, where?
☐	Are streams, drainage ditches, and tunnels that enter the perimeter monitored for intrusion?
☐	Are air operations susceptible to MANPADS attack? If so, explain countermeasures, i.e., threat surveillance, external perimeter security, HN patrols etc.
☐	What measures have been implemented to provide security against a surface-to-air missile attack?
☐	What protective measures are in place for off-site transportation of weapons and explosives?
☐	Has a barrier plan been developed, and has it been implemented?
☐	Has dispersion and standoff been considered for risk mitigation? How will it be implemented?

☐ If the site is a port shared with commercial operations, will DoD material be segregated from commercial materials? If not, how will theft, pilferage, and contamination be prevented? How will the material be protected from placement of harmful materials or explosives?
☐ Who will inspect containers before departure from the site by air, land, or sea?
☐ Are standard operating procedures available for security forces?
☐ Has the Quick Reaction Force (QRF) or its equivalent exercised for an enemy's close assault on the perimeter?
☐ Are waterways protected from enemy mining operations? How are they monitored/protected?
☐ Are high speed approaches by IED-bearing vehicles prevented?
☐ Have close air support assets been identified for request if needed - who, what, where, and estimated arrival times?
☐ Who is responsible for FP convoys? How are rest sites/transfer points protected?
☐ Have maps and imagery been marked either electronically or on paper to show entrances, exits, evacuation routes, placement of housing, critical infrastructure points(phone, sewage, electricity, etc.), major supply routes, lines of communication, security zones, etc.?
☐ Are bridges, fords, tunnels, ferries, underpasses, and swim sites identified on maps/imagery? How are these monitored to prevent or detect enemy usage?
☐ What areas with obstacles, terrain, and vegetation have been identified that could be hiding places for enemy forces prior to or during an attack?
☐ What man-made obstacles or buildings in the vicinity of the airfield could be used by the enemy to attack aircraft, vehicles or personnel and are designated on a map or imagery?
☐ Are nearby minefields, if any, marked on a map or imagery for avoidance by all personnel?
☐ Are psychological operations coordinated with the FP officer?
Internal Security
☐ Has the AT plan for the site been reviewed and approved at least annually?
☐ What units are currently on the site?
☐ What is the site population? What is the population per unit?
☐ How many on the site are civilian (non-government personnel) contractors? How many are U.S. citizens and how many are Iraqi citizens?
☐ What is the command and control structure/relationships between units?
☐ What unit has the JFOB commander designated as responsible for FP?
☐ Have maps and imagery been marked either electronically or on paper to show entrances, exits, evacuation routes, placement of housing, critical infrastructure points(phone, sewage, electricity, etc.), major supply routes, lines of communication, security zones, etc.?
☐ Are sensor locations marked on maps or imagery?
☐ Have the following products been reviewed for use in internal security?
☐ Threat Assessment
☐ Vulnerability Assessment
☐ Risk Assessment
☐ What tenant units are expected to occupy the JFOB?
☐ Will every tenant unit have a representative/member on the JFOB FPWG?
☐ Has a contact list for FP coordination with other units been assembled? Have members of the list been contacted for early notification of FP issues/concerns/capabilities?
☐ Have those tenant unit members on the JFOB FPWG been identified and notified of their responsibilities?
☐ What types of weapons will be needed for security forces in addition to their normal complement of weapons?

☐ Are munitions support areas (MSAs) protected? How?
☐ Will explosive ordnance disposal (EOD) teams be on the site? If not, who will handle EOD issues that arise?
☐ Will the site have a quick reaction force (QRF)?
☐ How will restricted access areas be protected, i.e., badging system, fences, berms, card reader, etc.? Are these systems available immediately or will they be emplaced weeks after the site is occupied? If available later, what other means will be available to control access to restricted areas?
☐ Has the required number of FP personnel been considered and analyzed for effectiveness? What was the method for doing so?
☐ Assuming the airfield is interior to the site, who has security responsibility for it?
☐ Have bomb threat/suspect package procedures been developed and implemented?
☐ Are exposed ladder and fire escapes susceptible to use by the enemy? How are they secured from enemy use?
☐ Is an up-to-date map or image of the JFOB available to the QRF or its equivalent?
☐ Have internal security zones been established?
Occupied Structures-Subset of internal security
☐ Have the buildings and other structures been described - wood frame, brick and other masonry, steel frame with concrete walls, etc. - for blast effects analysis?
☐ Will high-occupancy structures be located near the perimeter? What does an analysis provide with regard to expected damage, injuries, and deaths from an attack?
☐ Have structures been prioritized based on concern for the effects of an attack on the people and equipment in each structure? (number possible casualties, JFOB mission degradation, equipment damage)
☐ Have at least the high priority structures been reviewed to determine if it is possible for an attacker in a vehicle to get beneath, get under some section of the structure, or crash into the structure before detonating a vehicle-borne improvised explosive device (VBIED)?
☐ What standoff measures can/will be emplaced to keep vehicles away from the structures, and is the distance sufficient?
☐ Will existing buildings need retrofitting to provide adequate protection against the threat? If so, what kind of retrofits will be needed and on how many buildings?
☐ Have the buildings and other structures been modified to include blast protection measures such as film on glass windows, blast doors, etc.?
☐ Are parking garages and elevators monitored?
☐ Are sensors/intrusion detection systems in place to alert security forces in case of attempted entry or unauthorized entry into restricted areas on site?
Local Law Enforcement/Fire Department/Medical Services-Subset of internal security
☐ Are there existing agreements with local law enforcement and fire departments for security outside the site?
☐ Will the site have its own fire-fighting/emergency personnel and their equipment for post-attack incident response and consequence management?
☐ Does the site have sufficient fire-fighting equipment for response to multiple attacks at one time?
☐ What communications systems are available for non-security forces, i.e., other DoD personnel?
☐ Are port fireboats available in case of emergency? Is an MOA needed for this capability? Will the HN provide this capability or will DoD provide it?
☐ Are emergency medical services available to treat injuries and casualties due to accident or attack?
☐ Who handles the response to hazardous material incidents? Is the proper protective gear immediately available to responders?

☐ Are pharmaceuticals secured to prevent unauthorized access?
☐ Is an up-to-date map or image of the JFOB available to the local law/fire/medical services?
☐ Have medical facilities been set up away from possible lucrative targets? If not, how are they protected from the threat?
☐ Does the HN plan to evacuate local personnel just outside the JFOB in case the JFOB itself has to be evacuated?
Contractors-Subset of Internal Security
☐ How many entrances will be approved for use by contractors? Have these entrances been marked on an image or map of the site?
☐ What methods will be used to approve entrance of offsite contractors onto the site?
☐ Will solid waste disposal contractors be allowed onsite for pickup?
☐ Will liquid waste (sewage) disposal contractors be allowed onsite for pickup?
☐ Will HN contractors be escorted at all times by security forces or other DoD personnel while onsite?
☐ What number of personnel will be contractor escorts? Are security forces expected to provide escorts to contractors? If not, who will provide escorts to contractors while they are on site?
☐ Are construction staging locations away from asset areas?
☐ What points have been selected for onsite and offsite commercial and service delivery of materials, products, mail, etc.?
☐ If deliveries must be made onsite, are the delivery offload/loading areas set a distance from critical assets/high-risk resources to reduce risk from IEDs and other enemy weapons? What does an analysis state for a recommended/required distance for standoff from critical assets?
☐ Is a badging system or another approved system in place for positive identification of contractors?
☐ Is a daily personnel access list provided to security force personnel at designated contractor entrances?
☐ Will local contractors be searched before entering the JFOB?
☐ Have procedures and measures been established to ensure the contractor understands, acknowledges, fully supports and briefs appropriate company and sub-contractor personnel on FP/AT measures?
☐ If local contractors are used, who provides translator services?
☐ How will local translators be approved for entry onto the site?
Command, Control, Communications, and Computers (C4)
☐ Has the FPO coordinated force protection/communications requirements with the JFOB Communications/ Information Systems Officer?
☐ Are C4 systems in place to support FP?
☐ Have critical nodes been analyzed for risk?
☐ Do the force protection contingency plans identify base communications capabilities and limitations?
☐ What is the primary means of communication for the security force?
☐ Is a contingency plan in place to reroute communications should any part of the communications systems become damaged or lost?
☐ Are communication systems capable of being used to transmit instructions to all key posts simultaneously in a rapid and timely manner?
☐ Does the JFOB 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 capability back to other security forces?
☐ Does the security force use a duress code for emergency situations?
☐ Are communications systems encrypted? If so, identify which ones and which units use them.
☐ Are there procedures set in place to allow non-U.S. personnel, but yet they are coalition members, access to unclassified computer systems?
☐ Are primary and backup communications systems in place for emergency response units - fire, etc.?
☐ Is a mass notification system in place (Giant Voice, computer bulletin boards, emergency e-mail, sirens, flares, etc.) to warn personnel of impending attacks or for post-attack "All Clear"?
☐ Will alarm systems have a central point of notification?
☐ What reachback capability will be available for deployed forces?
☐ What types of mass notification systems will be used?
Critical Supplies/Infrastructure
☐ Will local sources of food be approved by veterinary personnel?
☐ How will food be protected from pilferage and contamination?
☐ How will water be protected from contamination - whether provided from inside or outside the JFOB?
☐ What alternate sources of water are available for quick access?
☐ What water treatment sources are in use - Reverse Osmosis Water Purification Unit (ROWPU), Harvest Eagle, Harvest Falcon, or other?
☐ What conservation measures are available in case of water supply disruption?
☐ How will petroleum, oil, and lubricants (POL) be protected from theft and contamination?
☐ How will POL be protected from destruction due to threat tactics?
☐ Are there storage facilities or alternate supplies and routes available in case of POL supply disruption?
☐ Is electrical power available? If not, how will it be provided?
☐ Based on the projected electrical load, will there be enough electrical power to operate all portions of the site without interruption?
☐ Is emergency power backup available for barrier locations, checkpoints, and warning systems?
☐ Is emergency power backup available for communications and emergency-related systems?
☐ Is sewage treatment/disposal available and in sufficient capacity to handle the waste from all site personnel? How will this capability be protected?
☐ Is garbage collection and disposal available in sufficient capacity for the site?
☐ Are POL tanks stored down slope from other facilities to reduce risk of enemy use as a weapon?
☐ Are plans available for protection of remediation and reconstitution activities for critical infrastructure for post-attack time?
☐ Are self-service food areas consistently monitored?
☐ Are self-service food areas limited to authorized patrons only?
☐ Has a comprehensive list of water assets, including personnel, treatment systems, transportation systems, storage facilities, and supply systems, etc. been developed?
☐ Are consequence management-related supplies available for the most likely threats?
Training and Exercises
☐ Have all JFOB occupants been given AT training before arrival?
☐ Have exercises emphasizing force protection been held and future ones scheduled? If so, which units will participate in the exercise?
Resourcing
☐ Are FP/AT practices integrated into contracts?

Real Estate-Subset of Resourcing
☐ What is the limit of DoD authority over the site?
☐ Will DoD lease the site?
☐ What FP measures are included in the lease of the site by the lessor, if any?
☐ Will DoD lease buildings near the site? Designate the buildings that will be leased if applicable.
☐ Will billeting be available onsite?
☐ Will billeting be offsite?
☐ How will billeting be protected from enemy attack?
☐ What FP measures will be available to personnel offsite- armed escorts, entry-controlled buildings, armored vehicles for transportation, etc.?
Resource Management-Subset of Resourcing
☐ Will existing structures require retrofits to reduce risk? What are the estimated costs for conducting those retrofits?
☐ Have vulnerability analyses, resource requirements, and justifications for force protection been documented?
☐ Has the Core Vulnerability Assessment Management Program (CVAMP) been used to document vulnerabilities?
☐ Have requirements for FP resources been coordinated with the resource manager?
☐ Have requests been made for funding to fix vulnerabilities?
☐ What fund types (O&M or MILCON) have been identified for use for new construction or retrofits to reduce risk?
☐ Has CbT-RIF as a source of funds been considered and requested?
Miscellaneous
☐ If it is necessary for visiting diplomats/high ranking personnel to enter the site, has this matter been coordinated with the State Department?
☐ If it is necessary for visiting diplomats/high ranking personnel to enter the site, what measures are in place to admit them quickly?
☐ If it is necessary for visiting diplomats/high ranking personnel to enter the site, who is responsible for their protection?
☐ Have certain locations or establishments - laundry, restaurants, hotels, etc.- been declared off-limits due to force protection concerns?
References:
Army Field Manual 5-114, 1992
AFI 31-104, Airfield Security Survey, 27 Dec 04
USCENTCOM Regulation 415-1, dated 1 Dec 04
DoD 2000.12H, DoD Antiterrorism Handbook, January 2004
Joint Forward Operations Base (JFOB) Force Protection Handbook (DRAFT), 23 August 2005
Center for Army Lessons Learned Newsletter, Forward Operations Base; Tactics, Techniques, Procedures; 05-24, September 2005
CENTCOM Operations Order 05-01, 10 August 2005

BASE DEFENSE OPERATIONS CENTER (BDOC) COLLABORATION PAGE

A collaboration site is essentially an automated bulletin board. Web collaboration provides an organization with the capability to collaborate externally or internally via the Internet in real time. Web collaboration can be used in an Internet Protocol (IP) environment or integrated with an organization's existing communication infrastructure to provide automated information for web-based inquiries. Use of the Internet allows rapid

dissemination of important information, such as points-of-contact, files and forms, tools, and uniform requirements. A sample BDOC collaboration page may look like Figure 15-1.

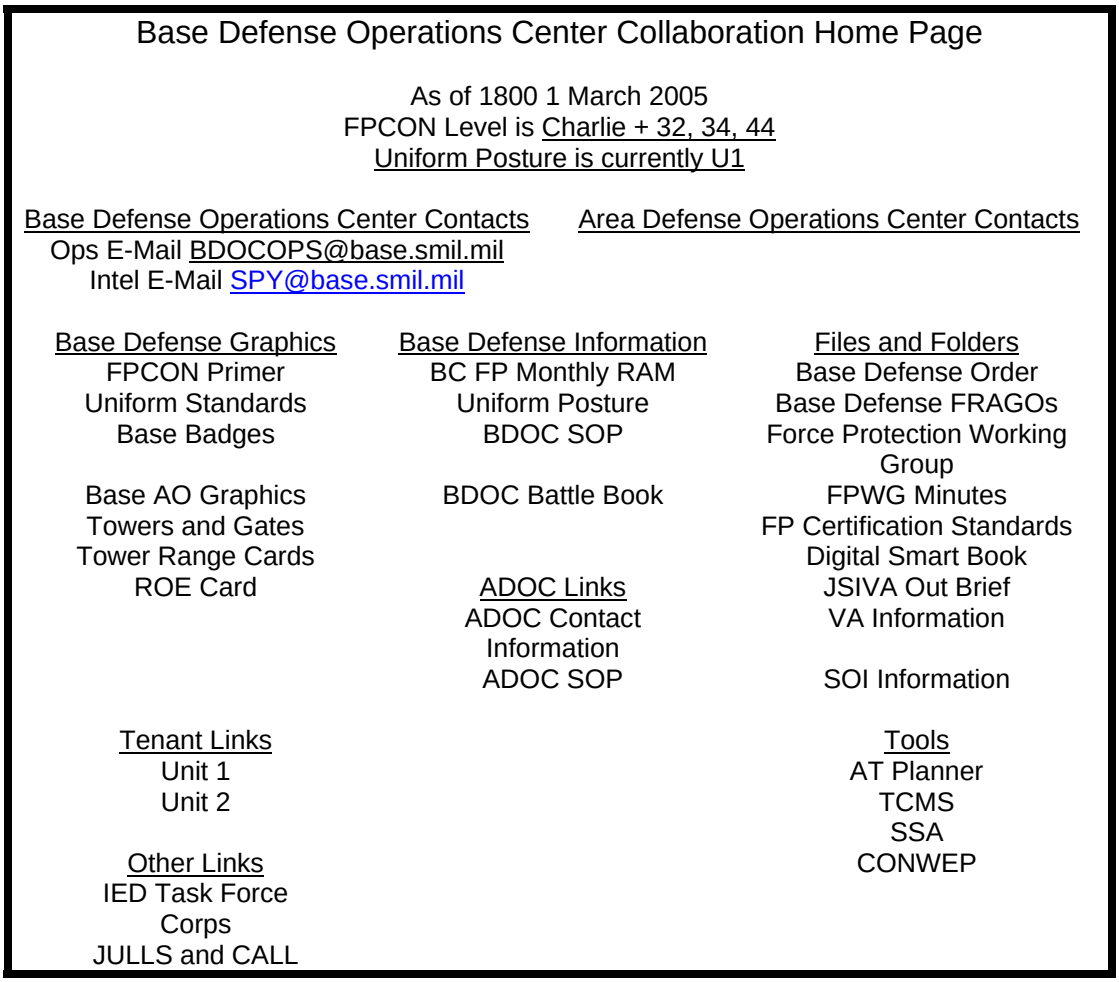


Figure 15-1. Sample BDOC Collaboration Page

DVD Summary Table of Contents

A DVD accompanies this JFOB Handbook. The DVD contains such information as:

- A digital copy of this Handbook in .pdf format.
- Digital copies of all Handbook chapters in Microsoft Word in case you want to capture checklists and make copies or modify for your use.
- Continuity of Operations Plan (COOP) information.
- More detail versions of selected information abbreviated in the Handbook, such as the BDOC SOP.
- References such as selected OPORDs.

- Selected construction plans and designs, templates for data collection and display, and tools.
- References including selected high-speed video of protective designs tests against threats.

CONTINUITY OF OPERATIONS (COOP)

The COOP is a record of information collected in planning and implementing FP. The COOP is also a record of findings and decisions. The primary purpose of the COOP is to maintain continuity of operations as personnel rotate in and out of the JFOB, and as the deployed force is preparing for redeployment and the follow-on force is performing pre-deployment planning.

A sample COOP is provided on the DVD included with this Handbook.

An example of the type information in the COOP is:

- Contact Information (for BDOC, ADOC, tenants, contractors, suppliers).
- Operations Orders (USCENTCOM AT OPORD 05-01, JFOB FP Plan, FRAGOS).
- FP Working Group (membership, meeting agendas, issues).
- Risk Management information (key asset inventory, current threat, self-assessment results, vulnerabilities, incident response capabilities).
- Pre Deployment Site Survey (PDSS).
- Base Defense Information (Base Master Plan, FP construction projects, BDOC SOP, equipment inventory, communications, graphics, maps).
- FP Plan Execution Records.
- Training (METL, Pre-Deployment training checklist, deployment training checklist, exercise tasks and records, USCENTCOM AT training requirements).
- Higher level assessments and JSIVAs.
- Resources and references.

JOINT ANTITERRORISM ENTERPRISE PORTAL (ATEP)

ATEP, the J-34 SIPRNET Portal is a one-stop shop for FP and antiterrorism (AT) officers and is active on both the NIPRNET (https://atep.dtic.mil) and the SIPRNET (http://www.atep.smil.mil). ATEP is your best source of personalized access to AT/FP information. It provides an integrated interface for current and planned tools; additional tools will be added as they become available. Numerous documents, recent briefings, and ongoing initiatives are available

ATEP is available to all military and federal employees. In addition, contractors working for the federal government may be given access providing they have a need for access and are sponsored by a military member.

DoD component members are invited to post information on ATEP because increased field participation ensures that ATEP will remain useful and accurate. For assistance in posting information to either ATEP page, contact LCDR Jeff Krusling at (703) 614-0083.

ATEP also provides direct access to the JAT Guide (including fixed installation and expeditionary modules). The JAT Guide provides a "how to" process for developing or modifying AT programs and includes templates and tools to support the planning process,

ATEP (SIPRNET) is also the venue for accessing the Core Vulnerability Assessment Management Program (CVAMP). CVAMP is the automated, Web-based means for managing command vulnerabilities and associated funding requests.

JOINT ANTITERRORISM PROGRAM MANAGER'S GUIDE (JAT GUIDE)

The JAT Guide is the only Joint Staff approved software tool/template for building DoD AT plans. It consists of 6 major elements that provide the "how to" for risk assessment, planning, resourcing, training, exercising, and reviewing that meet the requirements of DoDI 2000.16. It provides a comprehensive and consistent planning capability. The Guide has been widely distributed on CDs (3-CD box set) and DVDs within the Services. Most components of the JAT Guide can be run directly from the CDs or DVD, although the normal process is to install the JAT Guide on a personal computer so all features are available.

This JFOB Handbook directed to IRAQ is a subsection of the Military Operations section of the JAT Guide.

The Guide is on the ATEP on both SIPRNET and NIPRNET sites with automatic updates available.

POC: JAT Team email <http://www.lovej@wes.army.mil>; JS SIPRNET <http://www.atep.smil.mil>, NIPRNET <https://atep.dtic.mil>

TOOLS USED IN THE JAT GUIDE

JAT Database

This database is a series of three MS Excel workbooks written specifically for the JAT Guide and used extensively throughout the AT Assessment and Planning processes. The database can be used on any computer that has Microsoft Excel installed. It is the repository for information on threat, assets, vulnerabilities, incident response (IR), risk, course of actions, and cost/benefit. The workbook "CURRENT CONDITION" is used in developing a risk assessment (a prioritized list of installation current risks). The workbook "A" is used in developing a single course of action (COA), with resources

requirements, to mitigate the risks. A copy of the "A" workbook can be used to develop the data for each COA alternative. The workbook "COA MASTER LIST" is used to select among alternative COAs using a benefit-cost process or two other processes of a more subjective nature.

This tool must be downloaded to a PC, and the information becomes classified when populated with data for the JFOB.

Asset Value Rating Tool

This program returns an asset value rating number between 0 and 1 based on user answers to a set of questions. This value can be used to form an initial ranking and filtering of key assets for use in the risk assessment. This program can be downloaded to and used on practically any PC.

Threat Likelihood Tool

This program is used to estimate the likelihood of a given aggressor type targeting an asset using a specific threat tactic. It returns a number for threat likelihood between 0 and 1 that is used for calculating event likelihood. This program can be downloaded to and used on practically any PC.

Vulnerability Rating Tool

This program is used to develop threat-asset pair vulnerability ratings for an outside-in assessment: installation perimeter, facility perimeter, facility exterior, and facility interior. These individual ratings are combined to form an overall vulnerability rating for a threat-asset pair, which is used in calculating event likelihood. This program can be downloaded and used on practically any PC.

Preliminary Standoff Check Tool

This is a "javascript" tool that provides damage estimates for generic structures from specified vehicle bomb threats. The damage estimates are used to answer vulnerability questions relating to assets that are located inside a building.

AT Planner

The AT Planner software is a PC-based program, distributed with the JAT Guide that provides the user with a computerized analysis tool for evaluating the damage to buildings and occupants from terrorist threat scenarios using explosives.

Emphasis has been placed on the evaluation of structural components, windows, personnel, and limited other assets. Structural components are defined for columns, walls, and roofs, including common construction materials. Damage to the building components is calculated using algorithms from the Facility and Component Explosive Damage Assessment Program (FACEDAP) with the user providing the distance of the explosive charge from the building. The AT Planner can also calculate the required standoff to prevent damage for a given explosive charge. The calculation is based on expected explosive size and an acceptable level of building damage. The AT Planner then uses the required standoff to provide information on protective barriers and a vehicle velocity calculator to aid in barrier and obstacle selection. Extensive information is available on various types of obstacles and protective barriers in the "Help" file, and the information source is referenced. In addition, the AT Planner provides a

basis for design and analysis of wall and window retrofits. It also has the capability to view facility or site images, locate assets on the site image, and show building damage in 2-D and 3-D graphical formats. Blast walls can be placed in front of structures, and the resulting damage to a protected building calculated. Glass hazard calculations have been incorporated along with user-defined pressure-impulse curves to give structural engineers more flexibility in evaluating structures. The AT Planner is updated on a regular basis to include user feedback and recommendations.

AT Planner Version 2.1 was released in February 2005. The software distribution is limited to DoD and Federal Government employees and their contractors. Software distribution is password protected. During installation a hardware fingerprint is generated and displayed during the first use of the program. Also, a password is required. A request must be made to the POCs listed below.

POC. Ms. Sue Wolfe or Mr. William Hossley, U.S. Army Engineer Research & Development Center, Commercial Telephone: (601) 634-3225; Fax: (601) 634-2309; Email (preferred): <wgatplan@erdc.usace.army.mil>.

THIS SOFTWARE REQUIRES A SECURITY KEY TO ENABLE IT. If you have installed the software and wish to obtain a key, follow the instructions given on the webpage indicated below.

- Web Page: <https://atplanner.erdc.usace.army.mil. >
- Accept the certificate. Log in as follows:
- User Name: atpuser Password: 4u2plan

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.

CVAMP

This is a web-based program for tracking, prioritizing, and reporting vulnerabilities identified through vulnerability assessments. The program is available on the SIPRNET ATEP.

DON CIP SELF ASSESSMENT TOOL AND REFERENCE GUIDE

This tool is available on a CD issued by the Department of the Navy Chief Information Officer (Don CIO). It includes provisions and tools for identifying

critical infrastructure assets and performing vulnerability assessments as well as understanding the tools and practices available to improve security. It is not intended to be complete. It is a compilation of good information and should be used in conjunction with information obtained from other sources to develop and implement effective policies and capabilities for protecting critical infrastructure. See the Navy CIO website for availability: <http://www.doncio.navy.mil/>

FALCONVIEW

This is a Windows 95 and Windows NT mapping system that displays various types of maps and geographically referenced overlays. The program supports many types of maps, but the primary ones of interest to most users are aeronautical charts, satellite images and elevation maps. FalconView also supports a large number of overlay types that can be displayed over any map background. The current overlay set is targeted toward military mission planning users and is oriented towards aviators and aviation support personnel.

For JAT Guide purposes, this software application is used concurrently with the Flight Path Threat Analysis Simulation (FPTAS) to display probabilities of engagement and other scenarios from the threat of man-portable air defense systems (MANPADS).

See the FalconView website at <www.falconview.org> for availability.

FLIGHT PATH THREAT ANALYSIS SIMULATION

This PC-based software model allows the user to determine the most lethal locations in and around selected airports/airfields where potential threat systems could be deployed. The application can be acquired from the Defense Intelligence Agency (DIA) Missile and Space Intelligence Center. It is used with FalconView to display the most lethal locations on National Geospatial-Intelligence Agency (formerly National Imagery and Mapping Agency) maps and imagery.

HAZL (WINDOW FRAGMENT HAZARD LEVEL ANALYSIS)

This PC-based software is used to predict the hazard level and blast response of various window glazing types and to evaluate the benefits of a wide range of window retrofits. Most blast injuries result from window breakage shrapnel. This program, too, is available in the JAT Guide.

HAZARD PREDICTION AND ASSESSMENT CAPABILITY (HPAC)

This software application can predict the effects of hazardous material releases, including chemical, biological, radiological, and nuclear (CBRN) and toxic industrial chemicals/materials into the atmosphere and on humans. This

program is available from the Defense Threat Reduction Agency and requires training; the training materiel is provided with the software.

JAT COA SELECTION TOOL

This Microsoft Excel workbook contains a wide variety of example COAs organized according to threat tactic and strategy for risk reduction. These examples are taken from several sources and may be useful in developing site specific measures. The tool is useable within and is also downloadable from the JAT Guide website to any PC.

JAT GRAPHICS

This is geographic information system (GIS) software used for FP Planning. It is used to display maps/images and overlays for area of operations and interest, key assets, threat analysis, vulnerabilities and risk priorities, COAs, etc. This GIS accepts many types of map and imagery data and can be used with high resolution overhead imagery available from ENG. High resolution imagery permits zooming down to view objects and can be used to perform measurements directly from the imagery versus measurements on-the-ground. This GIS tool on the JAT Guide will operate on practically any PC and is no-cost. Training is required, and ENG and others use this system or something like it. Instructions and training materiel are part of the download.

SIMPLIFIED SURVIVABILITY ASSESSMENT (SSA) AND CONVENTIONAL WEAPONS (CONWEP) EFFECTS

This computer program can be used on practically any PC. SSA can be used to assist in the planning, design, and construction of survivability positions. SSA includes a customizable position database, a simplified overhead cover design wizard, and an optionally installed conventional weapons effects assessment tool.

SSA contains tools to plan, design, and construct standard survivability positions based on Army FM 5-103 “Survivability.” The positions are contained in a customizable database that can be browsed to view construction notes, design drawings, photos, bills of materials, required assets and construction time estimates. Users may edit the database to customize the positions, modify the construction time estimates and required assets or add additional drawings. SSA also includes the ability to import positions, plans, and equipment assets from other users’ SSA databases. Users may create new equipment assets and add them to the database or edit existing assets. Also, the database includes newly designed and accepted positions not yet in FM 5-103.

SSA addresses the cumbersome hand calculations in FM 5-103 for designing overhead cover with the addition of an overhead cover wizard that reduces designing overhead cover to a few steps and a few minutes of effort. The wizard includes built-in material types and properties and operates in four different design modes based on user-known information. The results are displayed in a

printable report that lists specific weapons for which the design provides and does not provide an acceptable level of protection.

SSA includes a planning tool for laying out the survivability plan and unit assets in tree format. The plan can be organized into missions and tasks, with user-specified priorities. Other user settings determine the effects of details such as soil type, night work, number of work hours per day, mission-oriented protective posture (MOPP) level, scheduled downtime, refueling, and more. Once a plan is built, construction time estimates can be made in a few moments and a Gantt chart of the estimated construction effort is displayed. Additional estimates can be quickly made, for example, to disable equipment, change priorities, or focus on a smaller portion of the plan. Any portion of a plan may be selected for viewing the bill of material requirements.

SSA comes bundled with ConWep, an optional application for calculating a variety of different conventional weapons effects such as air blast pressures, fragment and projectile penetration, loads on structures, cratering, and more. ConWep must be installed separately, and a separate password must be obtained prior to its use.

POC. Don Nelson or Speler Laird, email: <SSA@erdc.usace.army.mil>

On the first attempt to run SSA or ConWep, the user will encounter a window indicating that a software key is required to run the software. Due to the sensitivity of the material in SSA and ConWep, software keys (different keys from different sources for each) help to control unauthorized use of the software.

HOW TO GET A SOFTWARE KEY FOR SSA:

- Start the SSA software and when the window appears asking if a software key has been obtained, click OK.
- A new window will appear with entry boxes for the user's name and the software key. Do not enter anything into these boxes at this time. All that is needed at this point is the Hardware ID. At the top of this window is a unique Hardware ID for the machine on which SSA has been installed. Write down this number.
- Click Cancel to close the window and exit SSA; then email the following information to <SSA-Key@erdc.usace.army.mil> to get a software key:
  - User name.
  - Hardware ID.
  - Title/Rank.
  - Company/Unit.
  - Mailing Address.
  - Email Address.
  - Daytime Phone Number.
  - Statement of how/where SSA will be used.

- Upon approval, a software key will be emailed to the address provided.
- Upon receiving the software key, the user should restart SSA, and when the window appears asking if a software key has been obtained, click OK.
- A new window will appear. Type in the user name and hardware key exactly as given. If possible, copy and paste this information from the email for ease of entry.

IMPORTANT: The user name must be input exactly as it appears in the software key request because it is part of the encryption key.

After a valid user name and software key are input, the software will be unlocked and the main SSA screen will be displayed. SSA will not request the software key information during any successive program uses.

HOW TO GET A SOFTWARE KEY FOR CONWEP:

- Start the ConWep software from the Start Menu or from within.
- When the window appears asking if a software key has been obtained, click OK.
- A new window will appear with entry boxes for the user's name and the software key. At the top of this window is a unique Hardware ID for the machine on which ConWep has been installed. Write down this number.
- Follow the screen directions to obtain a software key for ConWep. ConWep has different approval requirements than SSA. The developers of SSA cannot provide a software key for ConWep. Users should follow the onscreen directions and provide the requested information to the ConWep email address provided onscreen.
- Once a software key is obtained for ConWep and is installed in a manner similar to that described for SSA, the key will no longer be required.

TELEENGINEERING OPERATIONS CENTER (TEOC)

Description. The TEOC provides a reachback 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 troops can be linked to subject matter experts (SMEs) 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.

TeleEngineering Communications Equipment (TCE). This is a satellite-based system that provides the capability to send (secure or non-secure) and receive data and conduct video teleconferences.

There are two versions of the TCE, a fixed-site (TCE-F) version that is used in garrison and a deployable (TCE-D) version ruggedized for field use. The systems consist of a Polycom ViewStation capable of H.320 based conferencing

(with non-secure IP functionality supported), a Panasonic Toughbook (designed using MIL-STD-810F), an encryption device, external hand-held camera, and other miscellaneous pieces. The fixed-site version is connected to an ISDN line and the deployable system connects through an M-4 satellite terminal. The deployable system uses auto-switching dual voltage power supplies and can operate from 110V to 220V AC. The deployable system can also operate on vehicle battery power.

Depending on configuration, the systems can communicate point-to-point or connected through a multipoint video teleconferencing (VTC) bridge at the ERDC TEOC to allow up to forty-four users in a secure VTC at a time. The data transfer rate and video connection for the deployable system is typically 64 kbps (this can be increased by adding additional satellite terminals) and the fixed-site version typically has a transfer rate of 128 kbps (can be increased to 512 kbps by upgrading the IMUX and adding additional ISDN lines). The system can also be used to send and receive non-secure email traffic.

Automated Route Reconnaissance Kit (ARRK). This is a hardware and software package used to automatically, continuously collect route reconnaissance (or other activity) information without requiring the vehicle to stop or personnel to leave the ground or air vehicle for routine calculations. Time, security, and accuracy concerns normally associated with a route reconnaissance are reduced. The ARRK collects photographs or video, voice recordings, global positioning system (GPS) locations, accelerometer data, and gyroscope data streams in three dimensions (switch data collection on/off, mix and match). Unlike traditional, manually recorded route reconnaissance efforts, the ARRK allows an operator with minimum training and experience to collect, process, and export the route information. Data can be overlaid on digital maps using a GIS and sent through TCE. Reconnaissance data collected by the ARRK can be quickly converted to a pre-formatted report in accordance with the requirements of FM 5-170.

POC. Voice: (601) 634-2735/3485 or 1-877-223-8322; DSN 446-2735/3485.
E-mail: TEOC@usace.army.mil; Fax: (601) 634-2764.

THEATER CONSTRUCTION MANAGEMENT SYSTEM (TCMS)

TCMS is a PC based construction planning, design, management, and reporting system that is used by military engineers for contingency construction activities. Its primary purpose is to support Engineer planners with facilities design information for outside the continental United States (OCONUS) mission requirements. It is intended to be used at all levels of engineer units from engineer command (ENCOM) down to engineer company level.

- **Planning**. Develop facility and installation plans to satisfy mission construction requirements using TCMS computer routines. Plans include estimates for material and construction requirements.

- **Design**. Prepare site specific and new design/construction drawings, or use existing Army Facilities components System (AFCS) designs within TCMS, or modify as required to site adapt or to fit mission requirements using the TCMS computer aided design and drafting capability.

- **Management**. Setup and manage the construction progress and the construction resource allocation and utilization throughout the construction time frame.
- **Reporting/Communication**. Develop and transmit the necessary reports up the engineer chain of command to facilitate the decision making process using inter computer electronic and direct entry.

TCMS is the approved method for distributing the AFCS Designs and related information in accordance with AR 415-16. Army Technical Manuals TM 5-301, TM5-302, and TM 5-303 will no longer be distributed in hard copy. TCMS is updated and distributed annually.

Detailed project descriptions and related construction estimates.

- Real estate requirements.
- Design and construction drawings and plans.
- Bills of materials for individual facility or complete project.
- Construction resource estimates as related to Army Engineer unit construction capability.
- Theater oriented Construction Guide Specifications.
- Construction Directives.
- DD form 1391 process initiation.
- Project and Unit Construction Status Reports.

Distribution of TCMS is available, upon request, to all U.S. Military engineer units including all Active Component, USAR and Army National Guard. Huntsville Center of the U.S. Army Corps of Engineers provides active TCMS support and will train TCMS users in the basic operation of the system.

To take full advantage of the system, users must know how to use AutoCAD and Microsoft Project.

Program Operation and Support information:

U.S. Army Engineer Support Center, Huntsville
ATTN: CEHNC-ED-SY-F
4820 University Square
Huntsville, AL 35816-1822
Phone: (256) 895-1781 DSN: 760-1781
FAX: (256) 895-1798
http://ww.tcms.net

SATELLITE AND OTHER MAP TYPE DIGITAL DATA

This is a specialized area related mostly to data used in GIS-type tools such as JAT Graphics and FalconView mentioned in this JFOB Handbook, as well as numerous other GIS-type tools in use within all Services, and the systems in use typically at DIV level and higher in IRAQ. This section does not include

alternatives to or variations on non-GIS use, such as digital photos taken from a helicopter and used as-is in briefings or documents or marked up with overlay symbols, boundaries, and notation using Microsoft Word or PowerPoint or pencil.

Unclassified low–to-high resolution data adequate for planning is available from several sources. The unclassified data resolution and contents may be better, or the same as, or may be exactly the same data as the classified imagery used in the INTEL and ENG shops.

Contact the INTEL and ENG staffs for imagery availability. Check that the data format is appropriate for use (check the GIS tool instructions) and the security clearance level.

The National Geospatial-Intelligence Agency (NGA) is a major data source. It is highly likely that someone at the JFOB or another larger JFOB will have an account and procedures for ordering imagery.

Generally, the three types of NGA-source maps and imagery needed are operational navigational charts (ONC), tactical pilotage charts (TPC), and compressed image base (CIB) format imagery at 1m or 0.6m resolution. Other types of maps and other imagery resolutions are available as well.

For FalconView, the maps and imagery needed are TPC maps and CIB format imagery at 5m resolution. The 5m resolution permits ready identification of ground features while reducing the file sizes needed for viewing the region around airfields. However, 1m can be used.

If the required data are not already available or there is a problem locating a local source, go to <http://www.nga.mil/portal/site/nga01/> and contact the military support/service representative for instructions on how to obtain maps and imagery for your JFOB or area of interest.

NGA provides classified and unclassified data.

- Using SIPRNET, you can download maps and imagery from the NGA Gateway Data Navigator page. Estimate the SIPRNET download time and assess possible challenges before using this method. (This is NOT the personal computer company known as Gateway.)
  - Go to <http://www.nga.smil.mil> on the SIPRNET.
  - Click on the “Gateway Data Navigator” tab.
  - Click on the geographical area of interest or the alphabetically listed country pages.
  - Use the functions to find your selection of data.
  - Download the file to your PC via http and save the zip file as the default .rpf.
  - Unzip the file.
  - Follow the instructions in the JAT Graphics Users Guide to load the unzipped data file into a data depot. If you are using FalconView, follow

the instructions, starting with the unzipped data file to load the data into the FalconView data manager.

- Unclassified commercially-available imagery is available on DVD or CD from NGA but cannot be downloaded.

– Go to <http://www.nga.smil.mil> on the SIPRNET.

– Go to the country or state pages of interest.

– Left click on “Services” on the left side of the screen. This displays a hyperlink called “Commercial Satellite Imagery Library” (CSIL). Left click on this CSIL hyperlink.

– Follow the instructions to set up an account. This will take a few minutes.

– Once you receive a password, log in as a registered user. (Passwords expire every 90 days.)

– Click on the Search Scenes hyperlink.

– Use the standard search options and CSIL Archive Metadata Search.

– Request data and platform type. Examples for use in JAT Graphics are as follows:

- IKONOS.
- Quickbird.

– Be aware that this only sets the format and not the projection of the image. JAT Graphics only uses the UTM projection. Some data provided by NGA is in a different projection and will not work in JAT Graphics or FalconView.

– Select the sensor type. Use “Panchromatic.”

– Choose country of interest.

– Input the coordinates for the location of interest in degrees, minutes, seconds.

– Place your order for the imagery data to be delivered on DVD or CD.

NOTE: Some U.S. Geological Survey (USGS) Digital Orthophoto Quad (DOQ) imagery is in Mr. SID format. (Mr. SID is a commercial software application). Run a GOOGLE search for a free conversion utility package to convert it to a GeoTIFF file with UTM projection to use it in JAT Graphics.

Chapter 16

FORCE PROTECTION PROGRAM ASSESSMENT BENCHMARKS

Contents

INTRODUCTION

The benchmarks provided are examples to assist the commander in developing a force protection assessment checklist for a JFOB. The benchmarks are referenced to chapters in the JFOB Handbook and are designed to be used as a field checklist with notes on the status of the benchmark item as it is reviewed. These benchmarks are intended to provide Commanders a starting point to develop a comprehensive checklist for their force protection program (FP) review.

JFOB PROGRAM MANAGEMENT BENCHMARKS

BM #	Benchmark	Refer to Page	Notes
	Chapter 1: C2 and the Base Defense System		
1	□ Are tenant units located on the JFOB assigned defensive responsibilities commensurate with their capabilities?	1-2	
	Chapter 2: Force Protection Planning		
2	□ Does the Commander have a clear and concise mission statement in the JFOB defensive order that supports and complies with MNC-I OPORD 05-02?	2-6	

3	☐ Is there an established Master Plan for the JFOB that includes long-term efforts for mitigation of vulnerabilities that require continuity, such as future construction, ECP improvement, Perimeter Security improvements, FP specific construction projects?	2-5	
4	☐ Does the Commander's FP execution checklist include continuous reassessment of Threat, Vulnerability and Criticality and structural hardening (dispersion, full-height sidewall protection, compartmentalization, etc)?	2-10	
	Chapter 3: Threat Analysis		
5	☐ Does the Commander's threat analysis identify the primary weapons threat against coalition forces (currently rockets, artillery, mortars and vehicle-borne improvised explosive devices (RAMs and VBIEDs); the enemy's tactics, techniques, and procedures (TTPs); the probability of attack, and the enemy capability to launch an attack?	3-14	
	Chapter 4: Risk Assessment		
6	☐ Has the Commander analyzed the risks of attack to personnel assigned to the JFOB and prioritized the risks?	4-6	
7	☐ Does Operations lead the Force Protection Working Group (FPWG) to focus their efforts in developing courses of action (COA) to mitigate risks?	4-22	
	Chapter 5: JFOB Site Selection and Layout		
8	☐ Is the JFOB located on Key Terrain that provides the line of site advantage to the JFOB; i.e., does the JFOB overlook surrounding terrain versus giving the advantage to the enemy? In Urban areas, are JFOBs located to prevent observation from nearby high-rise buildings?	5-3	

	Chapter 6: Perimeter Security		
9	☐ Does the JFOB have a perimeter that permits security forces to detect, warn, assess, deny, and defeat attackers?	6-1	
10	☐ Do physical barriers optimize the use of security forces?	6-2	
11	☐ Does the perimeter allow adequate standoff? Is there a clear zone with no occupancy inside the perimeter (standoff area to protect from blast/frags)?	6-2	
12	☐ Does the JFOB use Explosive Detection Military Working Dogs to screen for explosives at entry control points (ECPs)?	6-28	
13	☐ Are ECPs adequate to mitigate potential for access with VBIEDs as well as suicide/homicide bombers?	6-33	
14	☐ Are search areas at ECPs concealed from view and are persons being searched concealed from view?	6-42	
15	☐ Does the JFOB use MVACIS to screen delivery trucks?	6-29	
16	☐ Are guard towers placed inside the perimeter with an inner clear zone?	6-64	
17	☐ Are intrusion detection systems (IDS) and surveillance systems (sensors) part of the integrated base defense?	6-68	
	Chapter 7: Internal Security		
18	☐ Is there an established, functional F P W G that is actively working to mitigate risk to the JFOB?	7-3	
19	☐ Is there an established base defense operations center (BDOC) with a functional SOP and unity of command?	7-4	
20	☐ Are the rules of engagement clear and are they	7-10	

	understood by all JFOB occupants?		
21	☐ Does the JFOB have a mass notification system (Giant Voice)?	7-16	
	Chapter 8: Protective Construction		
22	☐ Has the JFOB commander compartmentalized high occupancy facilities to reduce the risk from RAMs, and suicide/homicide bombers?	8-21	
23	☐ Has the JFOB commander optimized the use of cover (specifically full-height, earth-filled side wall protection, overhead cover with pre-detonation screening; and preparation of bunkers to provide troop cover for prolonged or advanced warning attacks).	8-27	
	Chapter 9: Incident Response and Consequence Management		
24	☐ Has the JFOB commander conducted training of the incident response plan to ensure that first responders (fire, law enforcement, medical) are trained to immediately react to the situation in unison to isolate the incident, contain the situation and report to the BDOC?	9-2	
	Chapter 10: Communications		
25	☐ Does the JFOB Communications system provide secure communications between the BDOC, first responders, quick reaction force (QRF), and the guard force?	10-2	
	Chapter 11: Critical Infrastructure Assurance		
26	☐ Has the JFOB commander assessed the impact of critical infrastructure with an emphasis on sewer, water, electricity, academics, and trash (SWEAT) which have proved to be the most important factors in Operation Iraqi Freedom?	11-2	

	Chapter 12: Resourcing Funds and Contracting		
27	☐ Has the JFOB commander identified requirements to make the JFOB more secure (reduce unacceptable risk) that cannot be accomplished within existing resources, justified the requirement, and forwarded the funding requests to the Joint Acquisition Review Board (JARB).	12-4	
28	☐ Is the FP Officer included as part of the contracting team?	12-19	
	Chapter 13: Training and Exercises		
29	☐ Are AT/FP officers adequately trained?	13-4	
30	☐ Is U.S.CENTCOM mandated AOR specific AT training being accomplished within three months prior to assuming assigned duties?	13-5	
31	☐ Are newly assigned troops trained on what to do in the event of attack during in-processing at the JFOB?	13-6	
32	☐ Are exercises used to validate the FP Plan?	13-8	
	Chapter 14: Plans for Force Protection		
33	☐ Does the JFOB have a Base Defense Plan (or Annex) that has been signed as an order by the commander that includes as a minimum: 1. Situation 2. Mission 3. Execution a. Commander's Intent b. Key Tasks and Responsibilities c. Concept of Force Protection 4. Logistics Support for the Defensive Operation 5. Command and Signal	14-3	


JOINT FORWARD OPERATIONS BASE
JFOB
QRT
QUICK REACTION TEST

Inside Back Cover

[redacted] Command and Control and the Base Defense System

[redacted] JFOB Force Protection Planning Process

[redacted] JFOB Threat Analysis

[redacted] Risk Assessment

[redacted] JFOB Site Selection and Layout

[redacted] Perimeter Security

[redacted] Internal Security

[redacted] Protective Construction

[redacted] Incident Response and Consequence Management

[redacted] Communications

[redacted] Principal Critical Infrastructure Assurance Measures

[redacted] Resourcing-Funds and Contracting

[redacted] Training and Exercises

[redacted] Plans for Force Protection

[redacted] Acronyms / Tools

[redacted] JFOB Force Protection Program Assessment Benchmarks