HANDBOOK

No. 07-19 Mar 07

BASE DEFENSE

Tactics, Techniques, and Procedures

Center for Army Lessons Learned (CALL)
http://call.army.mil

Handling Instructions for Center for Army Lessons Learned (CALL) Products

CALL authorizes official use of this CALL product for operational and institutional purposes that contribute to the overall success of U.S. and Allied efforts.

The information contained in this product is provided for informational purposes only and is not necessarily approved U.S. Army policy or doctrine.

This product is designed for official use and cannot be released to the public without the expressed written consent of CALL. This product has been furnished with the expressed understanding that it will be used for official defense-related purposes only and that it will be afforded the same degree of protection that the U.S. affords information marked "UNCLASSIFIED FOR OFFICIAL USE ONLY [FOUO]" in accordance with U.S. Army Regulation 380-5, section 5-2.

Official military and civil service/government personnel may paraphrase; quote; or use sentences, phrases, and paragraphs for integration into official products or research. However, integration of CALL UNCLASSIFIED FOUO information into official products or research renders them FOUO, and they must be maintained and controlled within official channels and cannot be released to the public without the expressed written consent of CALL.

CALL UNCLASSIFIED FOUO information may be placed on protected UNCLASSIFIED intranets within military organizations or units provided that access is restricted through user ID and password or other authentication means to ensure that only properly accredited military and government officials have access to CALL UNCLASSIFIED FOUO materials.

When no loner needed, all CALL UNCLASSIFIED FOUO paper products and compact discs (CDs) will be shredded or destroyed using approved paper shredders or CDROM destroyers.

Foreword

The requirement to conduct counterinsurgency in Iraq and Afghanistan has refocused the Army on using patrol bases (PBs) to allow the troops to remain close to the population and the security forces they support. Operations staged from PBs offer some advantages, such as increased local engagement and security but also have some potential liabilities in the areas of force protection and Soldier quality of life. PBs are known by many names, joint security sites, combat outposts, among others. In this handbook, the term patrol base is used to cover all of these type of small outposts. Along with PBs, forward operations bases (FOBs) have been established to act as logistic sites and headquarters as well as places to allow Soldiers to rest and recuperate between missions. Typically larger than PBs, FOBs have their own unique security challenges. This handbook provides an overview of PB and FOB operations and presents evolving tactics, techniques, and procedures and useful observations, insights, and lessons from Operation Iraqi Freedom and Operation Enduring Freedom. The fundamentals of security, force protection, threat assessment, and command and control addressed in this handbook are applicable to both PBs and FOBs.

Steven Mains
Colonel, Armor
Director
Center for Army Lessons Learned

The Center for Army Lessons Learned key lessons direct readers to the most critical topics outlined in this publication. These key lessons are developed by CALL analysts in coordination with the publication's originator and are intended for the reader who has limited time. Although not intended as a substitute for reading the entire publication, the key lessons provide the reader with a list of specific issues that demand immediate attention.

Key Lessons

- **Establish a base defense operations center.**
- **Implement a base defense communications network.**
- **Establish/rehearse base defense standing operating procedures to include all forward operations base tenant units.**
- **Integrate intrusion detection systems as a base defense multiplier.**
- **Implement perimeter security to include entry control points and personnel and vehicle search procedures.**
- **Employ checklists for force protection operations, quick reaction force organization and employment, and site security assessment.**

Base Defense Handbook

Table of Contents

Center for Army Lessons Learned

Director	**Colonel Steven Mains**
Managing Editor	**George J. Mordica II**
CALL Analysts	**Brice H. Johnson** **Captain Tyrone Martin**
Production Manager	**Valerie Tystad**
Editor **Web Publications Editor**	**Jenny Solon** **Mark Osterholm**
Graphic Artist	**Eric Eck**
Print Support Liaison	**Carrie Harrod**

The Secretary of the Army has determined that the publication of this periodical is necessary in the transaction of the public business as required by law of the Department.

CALL publications cover a variety of military topics. The views expressed in this CALL publication are those of the author(s) and not necessarily those of the Department of the Army or the Department of Defense.

Unless otherwise stated, whenever the masculine or feminine gender is used, both are intended.

Note: Any publications (other than the CALL publications), referenced in this product, such as ARs, FMs, and TMs, must be obtained through your pinpoint distribution system.

This information was deemed of immediate value to forces engaged in the Global War on Terrorism and should not be necessarily construed as approved Army policy or doctrine.

This information is furnished with the understanding that it is to be used for defense purposes only, that it is to be afforded essentially the same degree of security protection as such information is afforded by the United States, that it is not to be revealed to another country or international organization without the written consent of the Center for Army Lessons Learned.

Introduction

The focus of this handbook will be forward operations base (FOB) and patrol base (PB) defense at the tactical level. Much of the information for this handbook was extracted from Center for Army Lessons Learned Handbook, 05-24, *Forward Operating Base* and the Joint Staff J3 Deputy Directorate for Antiterrorism/Homeland Defense Division's *Joint Forward Operations Base (JFOB) Force Protection Handbook*, final draft edition, December 2006. A copy of the latter on compact disk is included with this handbook.

The FOB is not a new concept. Joint Publication (JP) 3-10.1, *Joint Doctrine for Base Defense*, addresses base operations, security, and logistics dating back to the ancient Greeks, the American Civil War, and World War I and cites air base defenses as the beginning of the base defense concept.

In the current theater of operations, PBs established away from the FOBs in hardened facilities and occupied by Soldiers familiar with the area have proven useful in increasing the feeling of security for local populace, which translates into greater human intelligence (HUMINT).

Field manual (FM) 101-5-1, *Operational Terms and Graphics,* provides the following definitions for FOB and PB.

Forward operations base (FOB): In special operations, a base usually located in friendly territory or afloat that is established to extend command and control or communications or to provide support for training and tactical operations. Facilities may be established for temporary or longer duration operations and may include an airfield or an unimproved airstrip, an anchorage, or a pier. A forward operations base may be the location of special operations component headquarters or a smaller unit that is controlled and/or supported by a main operations base.

Patrol bases: The point of origin of a patrol where all equipment not required for the patrol is left. All supplies necessary for resupplying the patrol and additional medical supplies and assistance are staged at this location. See FMs 3-21.8, 3-21.10, and 3-21.9.

FOB Observations

An FOB is a static defensive position that may or may not have primary or secondary missions not related to direct combat. An FOB may be a fighting position (for example, a fire base of an artillery battery or battalion). A maneuver unit may conduct an independent mission from an established FOB. An FOB may be primarily a logistics base, established by plan or sometimes circumstance. A forward area rearming and refueling point may evolve into an FOB.

Current FOBs in Iraq and Afghanistan retain all of these functions. But operations in the contemporary operational environment (COE) document the 360-degree battlefield, non-contiguous operations, and asymmetric threats. Those COE

realities dictate that all FOB operations are to a certain degree tactical operations. As such, they must adhere to basic defensive concepts as offered in JP 3-10.1.

Put in more tactical terms, all FOBs should reflect standard military concerns. An FOB should be built for a defined mission or purpose, hopefully one based on thorough planning and analysis. The location of the FOB should support that mission, rather than hinder it. Moreover, that location should not conflict with other stated mission priorities. The physical terrain on which an FOB is established can dictate its utility, as can the terrain around it. The FOB must benefit from lines of communications that are sustainable both militarily and logistically. Even if the FOB is ideally located, with a clear mission in mind and on terrain well suited to its function, the enemy and local situation must be taken into consideration. FOBs must always provide sufficient defenses to enhance force protection (FP).

FOB operations have always been an operational reality for both Operation Enduring Freedom and Operation Iraqi Freedom. Units are based, sustained, and operate out of FOBs throughout their tours of duty. Responses to the Center for Army Lessons Learned Special Study of the First 100 Days indicated that 79 percent of survey respondents slept and took most meals in an FOB. The purpose of the FOB is to sustain combat power by providing a sanctuary for combat forces to rest and prepare for future operations in the combat zone. It serves as a FP and sustainment asset and a command and control center. The FOB has taken on increased tactical and operational significance as a power-projection platform.

Early in the deployment, all of the operations in the area of operations (AO) were conducted by sending mounted patrols from the FOB. This method became increasingly ineffective as the threat of improvised explosive devices (IEDs) increased. Additionally, locals were not as forthcoming with information because it was impossible to maintain a constant presence in the area. Locals knew that if they appeared to be giving any information to coalition forces (CF), enemy forces would come to threaten or hurt them once the patrol left the area.

Additionally, some observations indicate that FOBs may cause complacency among Soldiers and that the use of a PB, in lieu of the FOB, might increase security, improve FP, increase the quality and quantity of intelligence to include HUMINT, and enable better training of host nation forces.

PB Observations

In some situations, operating from a PB versus an FOB may be a more effective technique. The PB has the following advantages:

- Provides a constant presence in the AOR.
- Increases the feeling of security for the local populace, which translates into greater HUMINT.
- Increases FP because CF do not have to commute to and from the AO.
- Serves as a staging area for daily dismounted patrols, as well as a forward tactical administration center for other offensive operations.

- Increases training time for host nation forces not out on patrol. Additionally, host nation soldiers have constant contact with CF, which increases their ability to understand and learn security processes.

- Promotes teamwork because host nation forces and CF live and work together in a single location and are not separated by FOBs.

The use of PBs by Soldiers familiar with the area can prove useful for many reasons. PBs are established away from the FOBs in hardened facilities. A continuous presence in the area:

- Increases the quality and quantity of intelligence received.

- Yields more insurgent suspects and weapons caches.

- Yields more local information about IEDs.

Conclusion

Units must be prepared to meet FOB and PB security requirements by carefully weighing where assets are positioned and coordinating command and control issues. Additionally, units must continuously assess both external threat and internal security vulnerabilities. Finally, units and leaders must balance the benefits and liabilities of FP, security, and local area engagement when deciding whether to operate from FOBs or PBs.

Given the history of and the ongoing operations in both Afghanistan and Iraq, the FOB has become a fixture in the contemporary operating environment in general and specifically in counterinsurgency operations. The United States Army is the Department of Defense proponent for FP. As Army doctrine is developed and refined, these observations should be useful for units as they plan for, prepare, and conduct operations from either an FOB or a PB. Regardless of location or mission, units conducting operations in the COE will be required to secure themselves and the bases from which they operate. Soldiers and leaders, whether on an FOB or PB, must understand and apply the fundamentals of fixed-site security operations.

Chapter 1

Force Protection Planning: Forward Operations Base

All forward operations base (FOB) defensive plans should:

- Eliminate hiding places.
- Clear fields of fire.
- Provide a 170-foot minimum facility separation from installation boundary.
- Minimize need for signs.
- Minimize access points.
- Eliminate perpendicular lines of approach.
- Illuminate building exteriors where assets are located.
- Secure access to power, water, and gas mains.
- Locate away from vantage points.
- Place mailrooms on the perimeter.
- Provide emergency backup power.

Priorities of Work

- Establish reconnaissance and surveillance operations to include observation points.
- Post local security.
- Position key weapons systems.
- Position other assets (command post, mortars, vehicles).
- Designate final protective lines and final protective fires.
- Clear fields of fire if necessary.
- Prepare range cards and sector sketches.
- Prepare hasty fighting positions.
- Emplace obstacles and mines.
- Emplace early warning devices (whistlers, trip flares, platoon early warning devices).

- Mark/improve markings for target reference points and direct fire control measures.
- Establish rest plans.
- Rehearse engagements/disengagements.
- Adjust positions/control measures as required.
- Stockpile ammunition, food, water, and medical supplies.

Threat Assessment

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

Threats to the FOB 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 chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE).

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 CBRNE 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 FOB's operational area.
- Analyze the FOB's mission and the FOB commander's intent.
- Determine the significant characteristics of the FOB's operational area.
- Establish the limits of the FOB's areas of interest for each geographic battlespace dimension.
- Determine the full, multidimensional, geographic, and nongeographic spectrum of the FOB's battlespace.

- Identify the amount of battlespace detail required and feasible within the time available.
- Evaluate existing databases and identify intelligence gaps and priorities.
- Collect material and intelligence required to support further intelligence of the battlefield 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 or peacekeeping operation, may affect FP.

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 courses of action (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 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 CBRNE weapons.
- Determine how and from where the adversary receives external support.

Determine adversary COAs:

- 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.

Note: For a more detailed look at threat assessment see pp 3-4 through 3-22 of the *Joint Forward Operations Base (JFOB) Force Protection Handbook* compact disk included with this handbook. 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*.

FP Operations

FP changes on a regular basis and will need regular updating and reassessing to ensure the adequate and effective protection of an FOB. The FP plan, the tool used to implement FP, must be developed by a multifunctional working group to ensure all aspects are considered, addressed, and incorporated.

FP planning

While not all FP plans are the same and vary based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations, the following are the basic steps in developing a solid FP plan:

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
- COA development
- Resource documentation

Step 2: Select plan format. The FP plan format follows the standard operations plan and five-paragraph operations order (OPORD) format. However, the format should be tailored to meet the unique requirements of the base or fixed site 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 (PA) representative should supervise the development of the PA 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. Submit the finalized plan 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 base'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 and becomes a "living document." 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.

Perimeter FP

Main considerations for perimeter FP planning:

- Outside the wall:
    - Patrols immediately outside the perimeter must focus on keeping the routes clear and preventing the observation of the entry control points (ECPs) and base activities.
    - S2 of the base defense operations center (BDOC) should debrief units conducting offensive operations in the area of operations (AO) to collect critical intelligence.
    - Use Q36/37 radar to determine the point of origin of an indirect attack so units in the AO can be notified to go to that location. If the point of origin becomes a recurring location for indirect attacks, consider using a sniper team to over watch and kill the enemy or use unmanned aerial vehicles for observation or area denial.
    - Use civil affairs (CA) and psychological operations (PSYOP) teams to continually assess the positive and negative effects of the base upon the local population. In the case of Iraq, use the Iraqi Advisory Task Force when available.
    - The commander or S3 of the BDOC must engage the leaders of the local population and understand the demographics of the AO. The security of the base is an integral part of the security of the local villages and towns. This mutual working relationship will pay dividends.

- º When possible, integrate human intelligence (HUMINT) operations with CA or PSYOP operations within the immediate vicinity of the base.

- º Ensure the guards are trained and comfortable with using air integration.

- º Always walk the land from the enemy's viewpoint. See where the guards must kill the enemy and, if possible, mark and use target reference points for each tower along the perimeter.

- º Randomly vary the amount and location of Class IV material around the ECPs and potential weak points in the perimeter to keep the enemy guessing.

• On the wall:

- º Prevent the casual observation by outsiders of the internal workings of the base.

- º Add an anti-vehicle-borne improvised explosive device (VBIED) ditch along the outside of the perimeter wall or fence. If space is not available on the outside, then put one along the inside of the wall to prevent a successful follow-on attack of a VBIED.

- º Each guard tower should have a tower board with rules of engagement (ROE), general orders, special orders, radio frequencies, and other key standing operating procedures (SOP) laminated and placed in plain view of the guards.

- º Ensure all guard towers or posts have interlocking fields of fire and observation that adequately cover dead space.

- º The sergeant of the guard (SOG) must conduct vignette training covering ROE, training on crew-served weapons and radios, and other SOPs.

• Inside the wall:

- º Post sentries at key facilities and infrastructure to verify security badges of non-coalition forces and prevent the espionage and destruction of vital facilities.

- º BDOC must establish its own roving security patrol to verify security badges of contract vehicle occupants, ensure escorts are following security procedures for day workers, and check the perimeter wall or fence for tampering or breaches that cannot be seen from the towers.

- º FP plan and battle drills for attacks and mass casualties must be exercised on a regular basis.

- Leaders at all levels must be ruthless in enforcing FP measures to protect all their Soldiers and prevent combat complacency.
- An inside perimeter road along the wall or fence will quickly facilitate the movement of quick reaction forces (QRF) during emergencies as well as allow the SOG to conduct guard mount from tower to tower efficiently.
- Congestion increases the amount of potential damage during an enemy attack. The old rule of dispersion still applies. The BDOC must be synchronized with the headquarters of tenant units to ensure traffic is reduced.

- Above the wall: If air units are tenant organizations of the base, ensure the BDOC is linked in with the aviation tactical operations center and that pilots are aware of the common threats against the base in order for them to be another eye in the sky during takeoff and landing.

Incident Response and Consequence Management

Whenever an attack occurs, the BDOC will instruct the base occupants and tenant units to follow the established battle drills and procedures. For the BDOC to successfully respond to an incident and conduct follow-up operations for the consequences, preparations and training of the established battle drills must occur and be updated on a regular basis.

Incident response

There are five phases of incident response which are under the control of the BDOC.

- **Preparation**: The pre-strike phase focuses on identifying mission essential vulnerable areas, developing incident response and consequence management plans, and identifying and providing resource capabilities necessary to respond to attacks on these areas. Training and rehearsals are critical in this phase and should occur on a regular basis.
- **Response**: Occurs immediately after the attack when the incident responders are notified, arrive on scene, and secure and take control of the site.
- **Occupation**: On-scene commander assesses the situation and requests and obtains required support.
- **Support**: Support personnel arrive and conduct emergency operations.
- **Recovery:** Actions that are carried out to recover from the attack and consequence management begins.

Consequence management

Consequence management is focused on recovery operations after the initial attack has occurred and is successful when drills and plans are rehearsed and updated on a regular basis. Command considerations for consequence management include:

- Response route.
- Approach uphill/upwind if possible.
- Avoid choke points.
- Designate rally points.
- Identify safe staging locations for incoming units.
- Ensure the use of personal protective equipment and personnel accountability.
- Continually assess security.
- Evaluate the need for specialized units (explosive ordnance disposal [EOD]).
- Treat every incident as a crime scene. Create a buffer zone around the site, record all movements in and out of the site, and treat everything at the site as evidence.
- Mass casualty and first responder requirements.

QRF Planning

A QRF provides a reserve to the commander. Some typical QRF missions include:

- Assisting the FOB guard force with their mission.
- Adding combat power to units conducting patrols in the FOB or in an assembly area (AA).
- Assisting in crowd control, convoy escort missions, and/or safeguarding officials.

Plan and prepare

- Resource requirements.
- Readiness condition status and FP status (by squad/vehicle).
- Precombat checks/precombat inspections.
- Continency plans.
- Other assets available and coordinate methods of reinforcement.

- QRF near and far recognition signals.
- Running password.
- Availability of QRF interpreter.
- Brief to higher.

Rehearse

- At least one mounted alert and one dismounted alert weekly (time them to establish standard).
- Routes and actions at objective.
- Building clearing techniques.
- Rules of engagement (ROE).
- Link-up point and recall plan.
- Communications plan (higher, unit, cue frequency [freq]).
- Weapons control status.

Sample Order

Task: Employ QRF
Conditions: The task force (TF) (or company) is executing stability operations when an event occurs that requires deployment of a QRF to ensure mission accomplishment and Soldiers' safety. The TF or company has a platoon or section designated as the QRF. The QRF has dedicated transportation: trucks, infantry fighting vehicles, or rotary-wing aircraft.

Standards:

- Follow the ROE.
- Prepare to move in 30 minutes. If rotary-wing aircraft are the means of transportation, be in pickup zone (PZ) posture within 30 minutes.
- Brief the current situation to all personnel before departure.
- Take appropriate action at the scene to protect Soldiers' lives and to ensure mission accomplishment in accordance with ROE.
- Depart the scene with all personnel and equipment accounted for.
- Recover upon return to base. Be ready to be employed again within 3 hours.

Sub-tasks:

- Analyze and plan the mission:
  - Commander analyzes operations being conducted by the higher headquarters.
  - Commander prepares continency plans to assist any element in his unit who requires a QRF.
  - Task organization is situational, but the basic organization includes the headquarters (HQ), assault element, support element, and a security element. The HQ includes a medical team (or, at a minimum, combat lifesaver with equipment.)
- Ensure that the QRF is ready to execute continency plans:
  - Rehearse mission.
  - Ensure Soldiers retain their personal weapons and ammunition.
  - Load crew-served weapons and all equipment on the vehicles or place them on the PZ. Ensure equipment is guarded.
  - Set up sleeping areas in the vicinity of the vehicles or the PZ.
- Establish and rehearse a signal to alert the QRF.

- Take appropriate actions when alerted:
  - Soldiers immediately move to the vehicles or the PZ.
  - Leaders conduct personnel and equipment accountability.
  - Sub-unit leaders assemble at the QRF commander's vehicle to receive the verbal warning order (WARNO).
  - As soon as the QRF commander has his mission and has selected a course of action, he briefs his sub-unit leaders on the mission, overall plan, and commander's intent.
  - Sub-unit leaders brief their own subordinates on the mission and plan.
  - QRF departs for the mission site no more than 10 minutes after the WARNO is issued.

- Soldiers immediately perform radio checks on internal and command freqs and establish communication with the unit requiring assistance.

- Approach final AA:
  - Ensure final AA is covered and concealed from the mission site.
  - Ensure weapons status "red" prior to departing final AA.
  - Establish overwatch of scene, if possible.

- Actions at the scene:
  - Establish security.
  - Link up with local commander to evaluate local situation.
  - Ensure the unit is synchronized with the local unit.
  - Employ force within the provisions of the ROE to help the local unit accomplish its mission or evacuate the unit in contact.
  - Conduct ammunition, casualties, and equipment reports prior to departure.
  - Radio ahead for additional medical assistance if necessary.
  - Return to FOB.

- Recover:
  - Repair or identify damaged equipment; resupply ammunition, rations, and medical supplies; inspect and re-pack personal equipment; refuel and position vehicles.
  - Evacuate or treat injured personnel.
  - Repair or identify damaged equipment.
  - Resupply ammunition, rations, and medical supplies.
  - Repack personal equipment (squad leaders inspect).
  - Refuel and position vehicles.
  - Conduct radio checks.
  - Conduct detailed weapons and vehicle maintenance.
  - Conduct after action review.
  - Refine SOP as required.

FP Operations Checklist

Reassess threat:

- Types used and characteristics
- Patterns of employment
- Effects of threat weapons

Reassess vulnerabilities/key assets.

Establish perimeter security:

- Barriers
- Access control
- ECPs
- Guard towers

Establish internal security:

- FP conditions
- Random antiterrorism measures
- ROE
- Roving patrols

- Incident response
    - QRF
    - Fire
    - Medical
    - EOD
    - Military working dogs

Implement structural hardening:

- Dispersion
- Full-height sidewall protection
- Compartmentalization
- Large gathering areas
- Perimeter security
- Individual living areas
- Tents
- Temporary buildings

- Windows
- Walls
- Roofs

Establish incident response capability.

Install intrusion detection and surveillance systems: active and passive.

Install mass notification and warning systems: Inspect warning systems – Giant Voice.

Develop consequence management capability.

Conclusion

FP conditions and procedures change on a regular basis and need consistent and repetitive updating and reassessing to ensure adequate and effective protection of FOBs. The FP plan is an ever evolving document and must be developed, reviewed, and updated by a multifunctional working group to ensure all aspects are considered, addressed, and incorporated.

Chapter 1, Annex

Force Protection Program Assessment Benchmarks

Introduction

The benchmarks provided are examples to assist the commander in developing a force protection (FP) assessment checklist for a forward operations base (FOB). The benchmarks 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 FP program review.

FOB Program Management Benchmarks

BM#	Benchmark	Go/No	Notes
	Command and Control and the Base Defense System		
1	□ Are tenant units located on the FOB assigned defensive responsibilities commensurate with their capabilities?		
	Force Protection Planning		
2	□ Does the commander have a clear and concise mission statement in the FOB defensive order that supports and complies with higher headquarters operations order (OPORD)?		
3	□ Is there an established master plan for the FOB that includes long-term efforts for mitigation of vulnerabilities that require continuity, such as future construction, entry control point (ECP) improvement, perimeter security improvements, FP specific construction projects?		
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, and other factors)?		

	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 [VBIEDs]); the enemy's tactics, techniques, and procedures; the probability of attack, and the enemy capability to launch an attack?		
	Risk Assessment		
6	□ Has the commander analyzed the risks of attack to personnel assigned to the FOB and prioritized the risks?		
7	□ Does the operations section lead the force protection working group (FPWG) to focus their efforts in developing courses of action to mitigate risks?		
	FOB Site Selection and Layout		
8	□ Is the FOB located on key terrain that provides the line of site advantage to the FOB; i.e., does the FOB overlook surrounding terrain versus giving the advantage to the enemy? □ In urban areas, are FOBs located to prevent observation from nearby high-rise buildings?		
	Perimeter Security		
9	□ Does the FOB have a perimeter that permits security forces to detect, warn, assess, deny, and defeat attackers?		
10	□ Do physical barriers optimize the use of security forces?		

11	□ Does the perimeter allow adequate standoff? Is there a clear zone with no occupancy inside the perimeter (standoff area to protect from blast/fragments)?		
12	□ Does the FOB use explosive detection military working dogs to screen for explosives at ECPs?		
13	□ Are ECPs adequate to mitigate potential for access with VBIEDs, as well as suicide/homicide bombers?		
14	□ Are search areas at ECPs concealed from view and are persons being searched concealed from view?		
15	□ Does the FOB use Mobile Vehicle and Cargo Inspection System to screen delivery trucks?		
16	□ Are guard towers placed inside the perimeter with an inner clear zone?		
17	□ Are intrusion detection systems and surveillance systems (sensors) part of the integrated base defense?		
	Internal Security		
18	□ Is there an established, functional FPWG actively working to mitigate risk to the FOB?		
19	□ Is there an established base defense operations center (BDOC) with a functional standing operating procedure (SOP) and unity of command?		

20	□ Are the rules of engagement clear and are they understood by all FOB occupants?		

21	□ Does the FOB have a mass notification system (Giant Voice)?		
	Protective Construction		
22	□ Has the FOB commander compartmentalized high-occupancy facilities to reduce the risk from rockets, artillery, and mortars and suicide/homicide bombers?		
23	□ Has the FOB commander optimized the use of cover (specifically full-height, earth-filled side wall protection, overhead cover with pre-detonation screening, and bunkers to provide troop cover for prolonged or advanced warning attacks)?		
	Incident Response and Consequence Management		
24	□ Has the FOB 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?		
	Communications		
25	□ Does the FOB communications system provide secure communications between the BDOC, first responders, quick reaction force, and guard force?		
	Critical Infrastructure Assurance		
26	□ Has the FOB commander assessed the impact of critical infrastructure with an emphasis on sewer, water, electricity, academics, and trash, which have proved to be the most important factors in Operation Iraqi Freedom?		

	Resourcing Funds and Contracting		
27	□ Has the FOB commander identified requirements to make the FOB more secure (reduce unacceptable risk)?		
28	□ Is the FP officer included as part of the contracting team?		
	Training and Exercises		
29	□ Are antiterrorism (AT)/FP officers adequately trained?		
30	□ Is U.S. Central Command mandated area of responsibility-specific AT training being accomplished within three months prior to assuming assigned duties?		
31	□ Are newly assigned troops trained on what to do in the event of attack during in-processing at the FOB?		
32	□ Are exercises used to validate the FP plan?		
33	**Plans for FP** Does the FOB 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 FP 4. Logistics support for the defensive operation 5. Command and signal		

Chapter 2

Force Protection Measures: Forward Operations Base

Section I: Base Defense Operations Cell (BDOC)

The BDOC is the command and control center of defense operations and therefore critical for maintaining situational awareness. Using the best information available, the BDOC commander or S3 make critical timely decisions that ultimately affect the lives of base inhabitants or the local populace.

When establishing and organizing the BDOC, remember that the FOB is essentially a strong point defense in depth surrounded by an engagement area that the commander and S3 develop. Base defense begins at the maximum range of the indirect system employed by the enemy and continues all the way down to how Soldiers respond to threats within the perimeter of the base or fixed site. The BDOC has to consider all base defense possibilities in order to develop and train solid standing operating procedures (SOPs); force protection conditions (FPCONs); uniform measures; and battle drills for key leaders, personnel, and every inhabitant of the base.

For larger bases, dedicated security forces will be assigned to the BDOC and provide baseline security with augmentation by all tenant units. Tenant units will be tasked to provide security support to include guard towers, entry control point (ECP) support, sector security support, key asset protection, and contractor escort. This situation will often involve and require coordination between tenant unit commanders in regards to troop-to-tasks strength and priority of missions.

Communications Considerations

A solid communications network with backups is essential for the BDOC to maintain situational awareness and take the appropriate actions. Everyone must be able to talk to the BDOC in such a way as not to cause chaos. A standard reporting procedure and infrastructure allows timely and accurate reporting. A solid communication network supports the following FP activities:

- Maintaining vigilance against insurgent attack
- Reporting status of teams and organizations
- Sounding alarms
- Requesting assistance for emergency support (medical/fire)
- Calling for quick reaction force (QRF)/air support/counterfire
- Directing counterstrikes
- Coordinating incident response and consequence management

Communications systems should allow continuous access by the BDOC to the base operations center, rear area operations center, rear tactical operations center, and coalition and host nation (HN) forces. In addition, communications systems should

be capable of accessing supporting intelligence/counterintelligence, fire support, and air defense units.

The communications system architecture must also be secure (a must), robust (resistant to interference), redundant (alternate systems), and reliable (routinely maintained).

There are three basic forms of communications used by FOBs:

- Radios are used for both point-to-point and mass communications to large numbers of individuals or tenant units at the same time and are the best medium for emergency traffic.
    - Radios used within the FOB or fixed site must be secure (Single-Channel Ground and Airborne Radio System [SINCGARs] and Icom).
    - Small walkie-talkie types of radios are convenient for informal communications, but they are almost always unsecure. Soldiers and leaders must never allow the enemy to gain even the smallest advantage in regards to operations security.
    - The four most important considerations for radio communications are:
        - Operator training
        - System maintenance and power supply
        - Atmospheric interference
        - Counter-improvised explosive device (C-IED) technology interference
- Telephones (landline) are point-to-point and provide an extremely durable and secure means of voice communications, but they require robust support to install, operate, and maintain. Telephones are best for informal coordination with no interruptions.
- Computer networks are best used for the mass dissemination of nonemergency threat updates and general base defense operations orders and fragmentary orders including Nonclassified Internet Protocol Router and Secret Internet Protocol Router systems, emails, or Websites. It is important that the information management officer for the BDOC ensures all tenant organizations are in compliance with information assurance requirements.

Other communications considerations:

- Training at the lowest level on all communication systems is critical. There might be a time when a Soldier in a guard tower is directing an aviation asset to a target on the ground that only he can see.

- Two nets are the best to prevent interruptions of emergency traffic with administrative traffic and radio checks on large FOBs. Even if there are two nets, more robust reporting procedures may be required for larger bases, which may have over 50 guard towers, sentry points, and gates.
- The BDOC must be the only frequency hop master on the base defense net.
- If at all possible, all administrative traffic must be via telephone or computer networks.
- Pro-words and known reference points inside the base must be established to quickly clear a net for the BDOC to orient the correct assets to any emergency situation.
- Soldiers are sensors, whether in a guard tower or walking from unit to unit, and they must be able to report quickly and accurately. Use the established size, activity, location, uniform, time, and equipment (SALUTE) format.

Soldiers not in guard towers should report to the nearest unit tactical operations center (TOC) and submit a SALUTE format to be sent to the BDOC.

Soldiers in towers must be able to quickly orient a radio telephone operator or battle captain at the BDOC to what they are observing. If possible the BDOC should keep a battle book that has a color digital picture from each of the cardinal directions from the tower, with the direction in mils. When a Soldier in a tower reports seeing suspicious activity at 0800 mils from tower A12 at a greater distance than the blue building, the BDOC knows exactly where the Soldier is referencing and can quickly direct the appropriate assets to investigate.

Elements who should be on the communications network (as applicable):

- BDOC
- Guard towers/sentry posts
- External and internal patrols
- Airspace control/flight line
- Technology systems (counter rocket, artillery, and mortar and blimp)
- QRF
- Dining facilities
- Morale, welfare, recreation facilities (gyms, post exchange, internet café, etc.)
- Entry control points (ECPs)
- Detainee facility

- Power generation platforms and their maintenance support activities
- Military police/criminal investigation command
- Chaplain
- Fire department
- Morgue
- Fuel points
- Munitions supply/storage points
- Emergency engineer support
- Headquarters of tenant units
- Mayor's cell
- Mass casualty responders
- Dedicated emergency recovery assets (motor pool)
- Counter fire net or radars

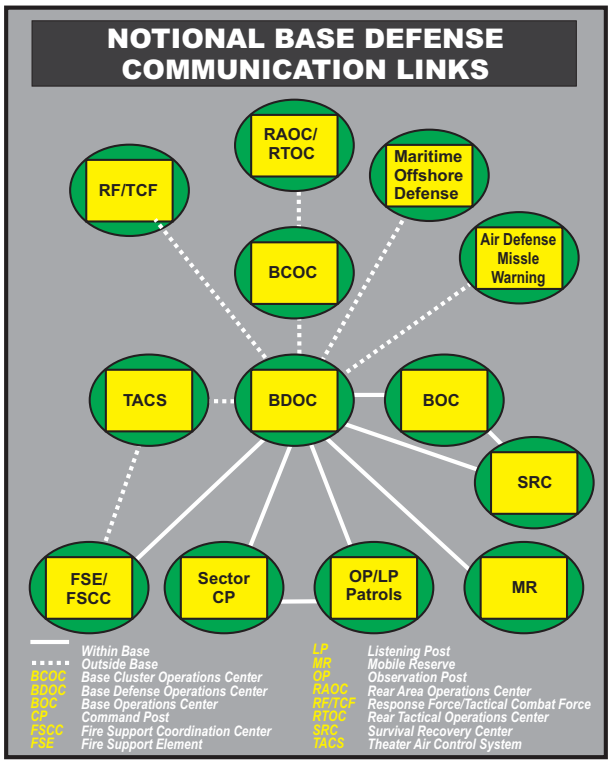


Figure 2-1. Notional base defense communications links

Communications checklist

- When was the last communications rehearsal conducted for mass casualty, QRF, and other battle drills?
- Are the uninterruptible power supply systems maintained and exercised regularly?
- Does the power generation equipment undergo a periodic load test?
- Are the communications systems capable of being used to transmit instructions to all key posts simultaneously in a rapid and timely manner?
- Are proper radio procedures practiced?
- Is all communications equipment properly maintained?
- Are there at least two dedicated radio frequencies for security forces?
- Are all radios and portable radios secure?

Intelligence/Threat Analysis

Soldiers are sensors; however, some leaders and planners make the mistake of relying solely on the Soldier in the guard tower for what is occurring at the base or fixed site. Base defense measures also apply inside the perimeter and to the units that patrol immediately outside the base perimeter. The BDOC must use its S2 cell as an active player to seek out sources of information to add to the situational awareness for the BDOC commander or S3.

Intelligence sources for the S2:

- Sentries in the towers, at guard points, and at gates (sergeant of the guard debriefs).
- Soldiers moving around the base.
- ECPs (badging process for day workers and contractors, searches of personnel, and locals hanging out in front of the gates).
- Human intelligence and intelligence reports from other sources that have more assets (higher headquarters, Iraqi advisor task force, or other government agencies).
- Unit debriefs of patrols immediately outside the wire. If the BDOC does not own this unit as an organic asset, consider having the S2 brief the patrol before it leaves and debrief the patrol when it returns. It would also be wise for the S2 to go on an occasional patrol to develop a feel for the terrain around the base.
- Aviation units that routinely use the airspace around the base or fixed site.

- Pattern analysis of attacks.
- Available technology (unmanned aerial vehicles).

The current threat can be organized and thus considered by these types:

- Indirect fire (rockets, artillery, mortars)
- Direct fire (small arms fire [drive-by attacks], sniper, shoulder-fired rockets [RPG rockets])
- Vehicle-borne improvised explosive devices (VBIEDs) and improvised explosive devices (IEDs) on the routes around the perimeter (egress/ingress)
- Infiltration by day workers/contractors, espionage
- Interception of nonsecure system communications; computer network attacks
- Sabotage of critical infrastructure both inside and outside the base; suicide bombers approaching the gate
- Indirect observation, such as casual observation of coalition or interpreter movement around the gates by vendors or locals at the nearby bus stop

Section II: Random Antiterrorism Measures (RAMs) and Perimeter Defense

RAMs

The basic approach to implementing RAMs is to identify FPCON measures or other site-specific measures that can be randomly employed to supplement the measures already in place. RAMs change the security atmosphere surrounding a base. When implemented in a truly random fashion, RAMs alter the external appearance or security "signature" of an FOB, so insurgents conducting surveillance cannot identify FP patterns. RAMs present the insurgents with an ambiguous security profile for the base. The impact of RAMs is difficult to measure, but such programs introduce uncertainty for planners and organizers of insurgent attacks.

RAMs provide the FOB with the following advantages:

- Varies security processes, making it more difficult for insurgents to identify important assets, build detailed descriptions of significant routines, or predict movement within a targeted facility or installation.
- Increases awareness for base personnel and FP/security personnel.
- Reduces adverse operational impacts and unplanned economic costs when enhanced FP measures must be maintained for extended periods.

RAM considerations:

- Implementation of RAMs will consume security forces 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, and 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 base RAM program. RAMs should not be limited to security force personnel.
- 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 timeframe or location for a given measure.
- Prior to implementation, local threat capabilities should be assessed and then effective RAM identified.
- RAMs should help to mitigate base vulnerabilities.
- RAMs should be conducted both internally to the base and externally in coordination with local HN authorities.
- RAMs should be compatible and coordinated with current base surveillance detection and security measures.

RAM examples:

- Outside the wall:
    - Move Jersey barriers or other Class IV objects around to change the flow of traffic immediately in front of any gate or high speed avenue of approach.
    - Use tracked-vehicle tracks as speed bumps to slow traffic. These can be easily acquired and moved at random.
- On the wall:
    - Install random flood lights that come on and off at various times.
    - Do not switch out sentries at regular times; do it randomly.
- Gates:

- Change access times for entry points.
- Change access procedures at random.
- Change the way personnel are searched (for example, take photos of tattoos and search shoes one day, turn coats inside out the next day).

- Inside the wall:
  - Conduct random traffic control points to verify contractor or day worker access privileges and search for contraband.
  - Conduct random sentry changes at various facilities.

Perimeter Defense

The perimeter forms the first line of defense for the FOB. The goal of the perimeter is to safeguard the base by protecting personnel and property. The perimeter is a defense in-depth engagement area extending to the furthest reach of the enemy's indirect threat to the center of the base or fixed site and internal operations. In some cases, the BDOC may have organic assets that patrol in the immediate area of operation (AO) around the base (three to five kilometers). If not, the BDOC must be interfaced into the TOC of the tenant organization responsible for the security of the AO and routes in this AO. This is the only way for the BDOC to respond in a timely and efficient manner as the threat is identified outside or at the perimeter.

The security elements that comprise the perimeter security system include:

- Standoff
- Physical barriers
- Access control
- ECPs
- 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 and indirect fire) is to keep the attack as far away from the base and inhabited structures as possible. Ideally, maximum standoff should be a primary consideration when personnel are deciding where to locate a base. If distance is not possible, the next best solution is to maximize standoff for

individual, inhabited structures. Standoff must be coupled with appropriate operational security procedures in order to be effective.

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 base perimeter to perform several functions:

- Define the perimeter of the base or fixed site.
- Establish a physical and psychological deterrent to attackers and to individuals attempting unlawful or unauthorized entry.
- Optimize use of security forces.
- Enhance detection and apprehension opportunities by security forces.
- Channel the flow of personnel and vehicles through designated ECPs in a manner that 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)
- Man-made (fences, walls, gates, vehicle barriers)

Physical barriers best practices include the following:

- 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 base.
- Combinations or layers of barriers should be separated by a minimum of 30 feet 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 the base or as a temporary serpentine in ECPs
- 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 FOB 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 (cutting a hole through a fence) or by nature (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 FOB 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 anti-vehicular.

Antipersonnel barriers: Are designed to deter personnel on foot from entering a base. 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 base. 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 climbing over them or using wire cutters. Consequently, antipersonnel barriers must remain under constant observation.

Anti-vehicular barriers: Are designed to stop vehicles at the perimeter of a base. They also assist in establishing standoff distance from protected assets. When placing anti-vehicular barriers, focus attention along high-speed avenues of approach outside the perimeter. When selecting the type of barriers, consider secondary debris and fragmentation created by explosives in close proximity to concrete barriers or concrete walls. Typical anti-vehicular barriers for bases include:

- Concrete barriers (Jersey, Texas, Alaska, Bitberg)

- Concrete blocks

- Cabled chainlink 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.

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?
    - Has the number of access points requiring vehicle barrier installation been minimized?
    - What is the most cost-effective barrier available that will absorb the kinetic energy developed by the threat vehicle?
    - How many barriers are required at each entry point to meet throughput requirements?
    - Will the barriers be subject to severe environmental conditions?
    - Will barriers interfere with established clear zone requirements?
    - Will active barriers fail to open or close in the event of power failure?
    - Is this a temporary or permanent FOB?

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

Expedient barrier systems: Common construction items, such as large diameter concrete culverts, steel pipes, and large construction vehicles (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 meter [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 feet (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 pound (lb) (1,523 kilogram [kg]) vehicle, traveling at 51 miles per hour (mpg) (82 kilometers per hour [kph]). The vehicle penetrated the barrier 1 ft (0.3 m). The tires were 36-ply with an 8-ft (2.4 m) diameter. They weighed 2,000 lb (909 kg) each.

Access control

Personnel access control system: The objective of a personnel access control system is to establish control pertinent to the FOB 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.

The policy must 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 FOB and associated critical assets, security personnel can implement the following access control measures:

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

- **Pass and badge system**: If the number of personnel requiring access to the FOB exceeds a number that can be recognized personally by security personnel for the FOB, 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 Department of Defense (DoD) or U.S. Government employee.

- **Exchange-pass system**: An exchange-pass identification system may be employed to ensure stringent access control for an FOB. 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 FOB.

- **Escort system**: Escorting is an effective method to control visiting personnel or contracted workers within an FOB. The escort must remain with the visitor at all times while he/she is within the FOB. 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 FOB. A major objective in escorting visitors around an FOB is to ensure that all material brought into the FOB by the visitor is searched for contraband or explosives and that no packages or other materials are left behind when the visitor departs.

Note: For expanded information regarding personnel access control, see pp 6-22 to 6-31 of the *Joint Forward Operations Base (JFOB) Force Protection Handbook* CD included with this handbook.

Vehicle access control: Specific procedures for vehicle search are based on the FOB mission and operational constraints and manpower, equipment, and explosive-detection assets available to conduct searches. The following procedures are provided as a general discussion of techniques for vehicle searches.

- **Visual searches**: Visual searches are used to find hastily placed IEDs and to identify indicators of deliberately placed IEDs, 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 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 that 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 is submerged in the transported liquid.

- **Military working dog (MWD) searches**: MWD searches rely on the dog's ability to detect the scent of certain explosives. In order to ascertain 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.

- **Explosive detector dog (EDD) searches**: Although specific EDD search policies will vary according to local FOB policy, individual MWD handler preference, and the unique abilities of individual canines, the typical approach follows five general steps:

    - The driver exits the vehicle and opens all doors, the hood and trunk lids, any other compartments, and any packages. The driver 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.
- 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.

- **Package searches**: Package searches involve examining baggage for weapons and explosives. Searchers should make the owner open all baggage, and MWDs should also check baggage.
- **Individual searches**: Individual searches are used to check personnel for weapons, explosives, and triggering devices. All drivers and passengers should be searched prior to entering the FOB. Handheld metal detectors and physical searches (frisking) are effective means of conducting individual searches.

General guidance for conducting vehicle searches: Specific guidelines for conducting vehicle searches should be established for each FOB. The following procedures can be used as general guidance for conducting detailed vehicle searches:

- Driver brings vehicle into search area.
- Driver dismounts vehicle and opens trunk and all 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 (gas in washer fluid reservoir), air filter replaced with wires or explosives, new components in engine, and extraneous components (an alternator not connected to a belt).
- In the case of cargo vehicles, an MWD thoroughly sweeps the truck. The search team randomly chooses cargo items and directs the driver to open them. Storage tank and side gas tanks are probed. The Mobile Search

Advanced X-Ray Portable Inspection System and the Mobile Vehicle and Cargo Inspection System (VACIS) gamma ray imaging system can also be used to search commercial vehicles.

- Search team directs driver to bring vehicle on top of ramp and 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.

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 or package. Searchers should complete one search technique before starting another one.

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, and 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, wheel wells, bumpers, under the engine, and above the gas tank.
- Look for any unusual devices taped, tied, and/or screwed to the undercarriage.
- Look for an unusually clean portion of the undercarriage and/or the presence of new weld marks or new bolts/screws.
- Be sure all connections are properly made (the gas tank filler tube runs from the fill port to the tank and 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 moment 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 toward 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 (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 and hood for rips, tears, and/or bulges 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 (alarm clocks and/or iron or polyvinyl chloride [PVC] pipe) that look out of place. Inspect items normally found in a trunk (tool box, supplies, blankets and water containers).
- Look for bits of electrical tape, wire, stripped wire insulation, string, fine wire, fishing line, and/or time fuse on the floor.
- Check for hidden compartments (spare tire well and jack/tool storage).
- Check for any additional or improvised wires attached to the brake lights or rear turn signals.
- Do not 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 (alarm clocks or 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.
- Check under the dash for any loose or unusual wiring. Pay attention to any modifications to the dash (extra switches with no function label and/or indicator lights that remain on although the vehicle is not running).
- Check the roof liner for bulges, rips, and/or repairs indicating possible concealment of an explosive device.
- If the vehicle is a tractor-trailer type, treat the tractor like a large 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 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 previously mentioned physical inspection methods. The current approaches used to address these special case vehicles are as follows:

- 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 FOB.
- Physically inspecting the entire vehicle again at the FOB with search personnel and MWDs.

Entry control points (ECPs)

During Operation Iraqi Freedom, ECPs have been attacked with VBIEDs. VBIED attacks have also been coupled with dedicated assaults to gain access into the FOB. In the future, attacks may include suicide bombers wearing IED vests. Properly designed ECPs can help defend against these types of attacks while remaining functional.

This section provides general design concepts and considerations for ECPs and must be adapted to the specific needs of each FOB. The objective of the ECP is to prevent unauthorized personnel and vehicle access and maximize vehicular traffic flow.

Figure 2-2

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 enemy 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**: Tactic 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**: Individual 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 an FOB should be subdivided into the following four functional zones, each encompassing specific functions and operations:

- **Approach zone**: The approach zone is the initial interface between the off-site road network (public highways) and the FOB. 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 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 access control zone should include design elements that support the following functions and operations:
    - º Verification of personnel identification
    - º Random or 100 percent inspection of personnel and vehicles
    - º Visitor control (issue of visitor/vehicle passes)
    - º Overwatch for approach zone
    - º Maintenance of vehicle speed management/reduction techniques
- **Response zone**: The response zone is the area extending from the end of the access control zone to the final denial barrier or gate to the FOB or fixed site. This zone defines the end of the ECP. The response zone should be designed so security personnel can carry out the following functions:
    - º Have time to react to a threat, operate the final denial barriers, and close the gate, if necessary.
    - º Monitor overwatch for the entire ECP.
    - º Define the FOB perimeter.
- **Safety zone**: The safety zone extends from the passive and active barriers in all directions to protect site personnel from an explosion at the ECP. Acceptable standoff distance or safety zone must be determined by an assessment of the threat (expected weight of the explosive charge) and the FOB or asset to be protected. If an adequate safety zone or standoff distance cannot be achieved to produce acceptable damage and injury levels, other alternatives must be evaluated or a decision made to accept additional risk.

The diagram in Figure 2-3 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 multipurpose ECP, since several types of entry control operations are combined in one location.

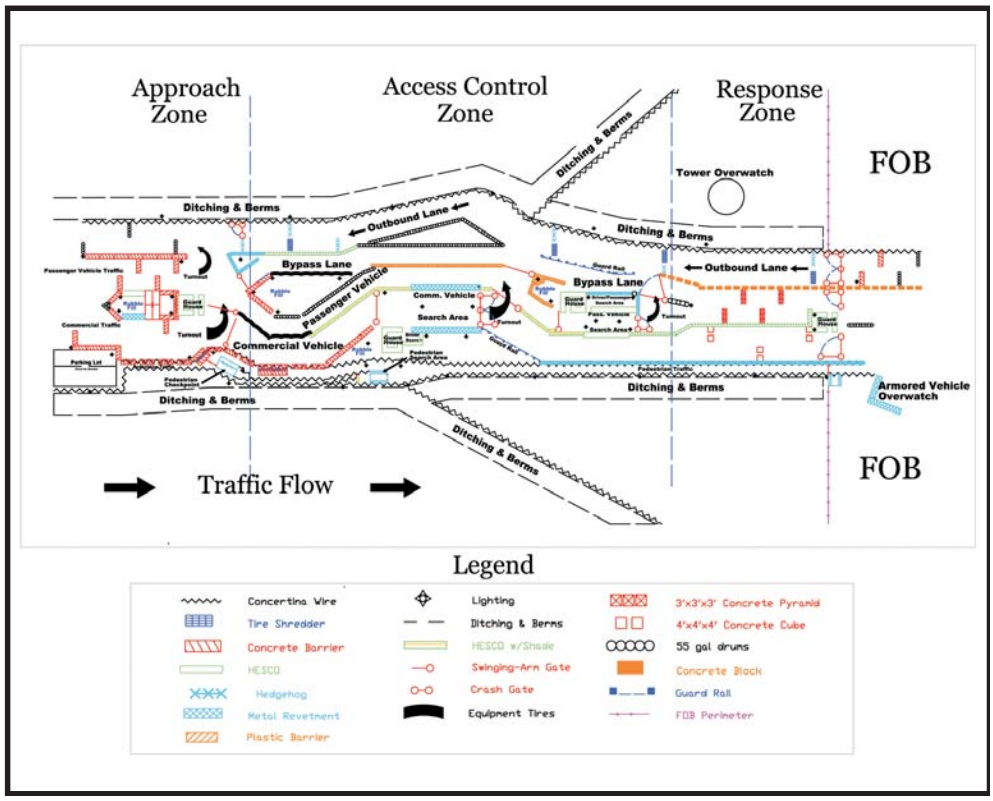


Figure 2-3. Example of functional zones, design concepts, and types of construction materials

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

- **Security**: 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 to:
    - Facilitate access control.
    - Enhance the defense-in-depth concept.
    - Provide effective risk mitigation.
    - Accommodate RAMs for sustained operations.
    - Operate during all FPCONs, including 100 percent vehicle inspections.
- **Safety**: ECPs must have a working environment that is both safe and comfortable for FOB security personnel. Security personnel safety includes provisions for personal protection against attack and errant

drivers. Special consideration must be given to climate, location, and orientation.

- **Capacity**: ECPs must maximize vehicular traffic flow to eliminate undue delays that would affect FOB operations while maintaining vigilance against attacks.

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

Design guidelines common to all ECPs: The ECP design should anticipate increased traffic volume and should support the employment of required FPCON measures and RAMs, as outlined in the FOB force protection plan.

- **Site selection**: 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

- **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 or delivery gate]).

    - Pedestrian access (hours vary)

- **Type of access**: Should be a principal factor in the design of the ECP. The preferred type of access for an ECP in a high threat environment

limits all pedestrian and vehicle access to mission-essential personnel. Numerous factors should be considered when commanders are determining the type of access at an FOB, including:

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

- **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. 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. **Note**: See p 6-39 of the *Joint Forward Operations Base (JFOB) Handbook* CD included with this handbook.
  - Where possible, a tertiary gate should be planned for contingencies and for emergency vehicular and pedestrian egress.

- **Required turning radius**: The roadway should be designed with the required turning radius to allow a single movement for the vehicle to be rejected or redirected. **Note**: See p 6-39 of the *Joint Forward Operations Base (JFOB) Force Protection Handbook*, CD included with this handbook.

- **Limit number of functions**: The number of ECPs should be kept to a minimum. However, a large FOB should consider limiting the number of functions to be conducted at each ECP. Limiting the amount of usage reduces the infrastructure and manpower requirements. For the following reasons, whenever possible, truck/commercial and passenger vehicle traffic should be segregated:
  - Effectiveness of 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 percent inspections.

- **Separate search areas**: If space is available, inspection/search areas should be exclusive, separate, and offset from traffic lanes to facilitate by-passing 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. **Note**: See pp 6-42 through 6-43 of the *Joint Forward Operations Base (JFOB) Force Protection Handbook*, CD included with this handbook.

- **Dedicated right-of-way**: 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.

- **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.

    - 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.

    - Vehicle containment can be achieved through a combination of passive (require no action once in place and are normally used to direct and channel the flow of traffic) and active (require some action, either by personnel, equipment, or both) vehicle barrier systems. The selection of passive and active anti-vehicle barriers should be based on their capacity to stop threat vehicles. Barriers should:

        - Have a limited profile in order to minimize cover and concealment positions for aggressors.

        - Encompass a contiguous perimeter around the ECP, with the final denial barriers completing the containment.

        - Be arranged to ensure that a vehicle does not circumvent the ECP once the vehicle has entered the approach zone.

        - Complement the employment of other physical and procedural security requirements.

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

        - Natural barriers may consist of a dense tree stand, berms, or drainage ditches on either side of the roadway; berms and ditches should have slopes that prevent vehicles from passing over the obstruction.

        - Constructed barriers may include cable-reinforced fencing and concrete walls. 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.

- **Pedestrian access control**: 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).
    - Walkways should be designed with limited obstructions to ensure that security personnel can maintain visual contact with the pedestrians as they approach the ECP.
    - Breaks should 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 should be considered and incorporated, if possible. If included, they should ensure control and prevention of possible tailgating.
- **Electrical design**: See "Security Lighting" section of this chapter.

Additional key design concepts:

- Entry roads to the FOB should not provide direct or straight-line vehicular access to high-risk assets.
- Parking areas should be located away from high-risk FOB and critical assets to minimize blast effects from potential VBIEDs.
- Signs identifying high-risk FOB and critical assets should be kept to a minimum.
- Layered defense.
- Nonlinear design.
- Maximized protection for ECP personnel (multiple guardhouses).
- Maximized standoff.
- Traffic and pedestrian segregation and channeling.
- Multiple vehicle turnaround/rejection areas.
- Vehicle speed management/reduction through the use of serpentines and vehicle barriers.

- Segregated search areas with line-of-sight denial from possible external surveillance.
- Overwatch positions (hardened fighting positions).
- Hardened perimeter gate access (final denial barrier).

Exit-point design concepts: Approaches to all vehicle exit points should be designed so that high-speed approach from outside the perimeter is not possible.

- An active barrier should be used to maintain positive control over an exit lane and to prevent someone from entering the FOB or fixed site through the exit.
- 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.

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.

Search area design concepts:

- Parking area: Should be established outside the ECP and search area at a distance that provides adequate standoff for inhabited areas, should remain under constant observation by security personnel, should be regularly searched with MWDs.
- Staging area: Should provide enough space to stack and stage vehicles awaiting search; if possible, personnel awaiting search should not be able to observe the search procedures.
- Search area:
    - In order to maximize the effectiveness of security personnel and MWDs, the search area should have overhead protection from the sun.
    - Berms, tall concrete barriers, or earth-filled barriers placed around the search area 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.
    - Berms, camouflage netting, or other types of screening should be used to obstruct observation of the search area from personnel outside the FOB.
    - Obscure the search area from drivers and passengers being searched; keep drivers and passengers under constant observation by an armed guard not involved in the search.

- MWD rest area: MWDs 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: Most effective means to visually inspect the undercarriages 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.

- Other search area considerations:

    - 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.

    - 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.

    - Search pits should be well illuminated to allow searchers to see all portions of the vehicle. Security personnel should have flashlights or extension lamps available for use.

    - Closed circuit television (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.

    - Many commercially available bomb detection devices are available including the VACIS – gamma ray imaging system.

Security lighting

Higher levels of brightness improve the ability of security forces to see for long distances at differing low-level contrasts, identify indistinct outlines of silhouettes, and spot intruders. 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 than desert landscapes to achieve a constant level of brightness .

- 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:

- Provide adequate illumination or compensating measures to discourage or detect attempts to enter the base 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 (CCTV) and recognition factors can be installed. Where color recognition will be a factor, full-spectrum (high-pressure sodium vapor) lighting versus single color should be used.

- Use lights that illuminate the ground or water but not the air above and penetrate fog and rain.

Types of perimeter lighting:

- **Continuous lighting**: Most common protective lighting system 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 bases where light discipline is a must, as continuous lighting could help attackers pinpoint the location of the FOB.

- **Glare lighting**: Installed slightly inside a security perimeter and directed outward and 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**: Similar to continuous lighting; however, this lighting 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 base.

- **Emergency lighting**. May duplicate any or all of the above systems and 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**: Very effective in deterring intruders as it is activated 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:

- **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.

    - Additional task lighting may be necessary for adequate identification of vehicle occupants and contents.

    - 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.

Hardened fighting positions/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. At 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 (night vision scopes).
- Heating, ventilation, air conditioning, 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 verbal means.
- Installation of a searchlight on the center of the tower roof that can be rotated manually by the tower occupant.
- Location and height of the guard tower/overwatch best suits a particular FOB, based on the nature of the facility, the terrain under observation, the physical environment, and the function of the tower.
- Guard tower/overwatch positions must be located so that the entire inner and outer clear zones and fence line can be observed.

Intrusion detection and surveillance (IDS) systems

Several technological devices and systems are currently available to assist in base defense security operations. The systems' primary purpose is to detect both exterior and interior threats, report detection, and enable personnel to assess what and where the threat is and initiate an appropriate response to safeguard the FOB. Relying on perimeter IDS involves inherent risks, and in high-threat environments, security personnel cannot rely solely on IDS; however, IDS should be an essential part of an integrated and layered approach to FOB FP.

IDS systems 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:

- **Threat detection**: A wide variety of systems can be used to detect the presence of activity at a distance from the FOB. However, several factors can influence system performance:
    - Seasonal and/or ambient weather conditions
    - 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
    - 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 that dispatches security forces. The annunciation capability should have redundancy.
- **Threat assessment and classification**: Detected data must be assessed and classified to determine whether the alarm is real or false and whether the intrusion is hostile or benign. 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 in order to facilitate definitive threat classification and assessment and 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.
    - Facilitate the evacuation of the protected asset to a safe area.

- Secure the protected area and contain the threat.
- Prevent additional hostile resources from arriving.

Note: For additional information on IDS selection considerations and types of IDS systems, see pp 6-71 through 6-79 of the *Joint Forward Operations Base (JFOB) Force Protection Handbook* CD included with this handbook.

Security force

In conjunction with the physical security measures employed on the perimeter, the first line of defense against hostile acts on an FOB is the security force. Security forces consist of personnel specifically organized, trained, and equipped to provide security functions for the entire FOB. Security forces also consist of personnel assigned as interior guards for specific areas or assets, who also require organization, training, and equipment specific to their assigned duties. Properly used, these personnel can be one of the most effective tools in a comprehensive, integrated FOB FP 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, and espionage.
- 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 an FOB, the commander must address the threat, size and location, geographic characteristics, and mission of the FOB and ask the following questions:

- 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 for the security force?
- What critical assets or unique systems are located at the FOB?
- Where is the security force located?
- What specialized equipment is needed for the security force?
- What forces are required to reinforce the primary security force?
- Who interfaces with these auxiliary security elements?

- What is the alert notification procedure for these elements?
- What are the rules of engagement for the security force?
- Who authorizes direct action by security force personnel?
- Was the security force included in force protection plan development?
- What specialized training does the security force require?
- Are no-notice exercises and rehearsals conducted?
- Is specialized training for securing critical assets or unique systems provided?
- Has coordination been accomplished for patrolling areas outside the FOB?
- Have security force orders/SOPs 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 or material they may need to access?
- Does the FOB maintain an organized and equipped 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?

Chapter 3

Force Protection Planning: Patrol Base

Lessons learned in Operation Iraqi Freedom (OIF), Operation Enduring Freedom (OEF), and historical analysis indicate that success is more likely when operating from small combat outposts or patrol bases (PBs) that enable forces to maintain contact with the people and the Iraqi forces. This technique requires a minimum general security condition where insurgents are less numerous or lack freedom of movement, so it often must be implemented progressively throughout the battlespace.[1]

OIF and OEF experiences indicate that more numerous PBs not only increased security for the locals that, in turn, resulted in increased human intelligence (HUMINT) production, but it also increased the rate at which the capabilities of the Iraqi Army improved and increased their legitimacy.[2] The Iraqi and Afghani soldiers were more likely to accept instruction when the coalition Soldiers shared their hardships and dangers. In addition, the almost constant contact with coalition forces allowed the Iraqi forces to benefit from their example and increased their access to multipliers such as intelligence feeds. Recent experience indicates that PBs enable combined patrols to no longer be restricted to movement on the main supply route alone and, as a result, take a key weapon, improvised explosive devices, away from the enemy.[3] Smaller bases also allow more innovative and reactive actions because the forces are close to where the HUMINT is collected.[4]

PBs require dedicated intelligence and communications assets, not only to receive intelligence passed from higher, but also to develop an intelligence picture from combined patrols. PBs can be squad, platoon, or company-sized based on the requirements, but each requires the ability to collate and analyze patrol reports. Augmentation of the maneuver element with trained, dedicated, intelligence assets will prevent diversion of limited maneuver resources to perform this vital function.

PBs require limited self-sufficiency in power generation, sanitation, food, and ammunition to enable continuous operations if supply lines are cut for a period of time. The greater the distance from support forces, the greater the need for self-sufficiency; however, PBs should never become mini-FOBs. The purpose of PBs is to allow projection of forces into the local community, not to insulate the forces from the local community.

PB Operations

When conducting PB operations, small unit leaders must consider and address the following five areas:

- Command post (CP)/command and control (C2)
- Communications
- Force protection (FP)
- Detainee holding
- Life support

CP/C2

The CP does not have a set organization. It consists of the commander and other personnel and equipment required to support the C2 process for a specific mission. The CP locates where the commander determines it can best support his C2 process. The CP/C2:

- Provides communications with higher, lower, adjacent, and supporting units.
- Assists the commander in planning, coordinating, and issuing orders.
- Provides for its own security.

The CP consists of the commander and his radio-telephone operators, the fire support team headquarters, the communications sergeant, and the CBRNE (chemical, biological, radiological, nuclear, and high explosive) noncommissioned officer. The executive officer, first sergeant, armorer, reserve element leader, and the leaders of attached or supporting units may also locate with the CP.

Communications

The PB must establish communications with:

- Higher
- Lower
- Adjacent
- Supporting units

Detainee holding

The PB must have the capability to hold detainees. The detainee holding area (DHA) is normally located in a safe and secure area capable of receiving and evacuating detainees. The DHA is a temporary location to field-process and house detainees and provide resources for intelligence exploitation. It is generally comprised of a semi-permanent structure designed and resourced to house detainees. Basic elements include:

- Protection against enemy direct and indirect fire
- Shelter or cover from weather
- Latrines
- Basic hygiene facilities
- Medical treatment facilities

Life support

Life support considerations for a PB include:

- Power
- Plan/provisions for medical evacuation
- Minimum medical provisions and designated casualty collection point
- Latrines
- Hygiene
- Water
- Messing and rest area

PB Priorities of Work

The priorities of work are generally the same as for a forward operations base. However, because most PBs will be established in urban areas, give special attention to the unique qualities of the urban environment.

- Select key weapons and crew-served weapons positions to cover likely mounted and dismounted avenues of approach:
    - To cover armored avenues of approach, position antiarmor weapons inside buildings with adequate space and ventilation for backblast (on upper floors, if possible, for long-range shots).
    - Position machine guns (MGs)/squad automatic weapons (SAWs) to cover dismounted avenues of approach. Place them near ground level to increase grazing fires. If ground rubble obstructs grazing fires, place MGs/SAWs in the upper stories of the building. Ensure weapons are mutually supporting.
- Clear fields of fire: Prepare loopholes, aiming stakes, sector stakes, and target reference points. Construct positions with overhead cover and camouflage (inside and outside).
- Identify and secure super- and subsurface avenues of approach (rooftops, stairwells, sewers, and basements).
- Stockpile ammunition, food, drinking water, medical supplies, and fire-fighting equipment.
- Construct barriers and emplace obstacles to deny the enemy access to streets, underground passages, and buildings and to slow his movement:
    - Integrate barriers and obstacles with key weapons.

- Cover all barriers and obstacles by observation and fire (both direct and indirect).
- Conceal the obstacle from enemy observation as much as possible.
- Erect the obstacle in an irregular pattern to hinder enemy movement.
- Employ the obstacle in depth (if possible). Tie the obstacle in with existing obstacles.

- Improve and mark movement routes between positions, as well as routes to alternate and supplementary positions.
- Improve routes by digging trenches, using sewers and tunnels, creating entry holes, and emplacing ropes for climbing and rappelling and ladders for ascending and descending.

PB/Defensive Site Planning Considerations

Leaders should consider the following when establishing or conducting operations from a PB/defensive site:

- **Security**: The first priority is establishing all-around security, including patrols and OPs with periods of limited visibility.
- **Protection**: Select positions that provide protection from direct and indirect fires.
- **Dispersion**: A position should not be established in a single building when it is possible to occupy two or more buildings that permit mutually supporting fires. A position without mutual support in one building is vulnerable to bypass, isolation, and subsequent destruction from any direction.
- **Concealment**: Do not select obvious defensive positions (easily targeted by the enemy).
- **Fields of fire**: To prevent isolation, individual and crew-served weapons positions should be mutually supporting and have fields of fire in all directions.
- **Covered routes**: Defensive positions should have at least one covered and concealed route that allows resupply, medical evacuation, reinforcement, or withdrawal without being detected or at least provides protection from direct fire weapons.
- **Observation**: Positions should permit observation of enemy avenues of approach and adjacent defensive sectors. Upper stories of buildings offer the best observation but also attract enemy fire.

- **Fire hazard**: If possible, avoid selecting positions that are obvious fire hazards.

- **Time**: Time is the one element the unit and its leaders have little control over. The most important factor to consider when planning the use of time is to provide subordinate leaders with two-thirds of all available time.

Plan for contingencies, select an alternate site.

Endnotes

1 FM 3-24, *Counterinsurgency*, Dec 2006, p 5-24.

2 3d ACR AAR, 29 Jun 06, p 15-3.

3 Center for Army Lessons Learned (CALL) Initial Impressions Report No. 06-25, 3d ACR pp 45-46.

4 CALL Handbook, No. 05-11, *Tactical Forward Operating Base*, Chapter 6.

Chapter 4

Force Protection Measures: Patrol Base

Patrol bases are a deliberate combat action and are not planned or emplaced lightly. They require sufficient combat power to secure themselves against a determined, surprise attack. This combat power can be in the form of forces on the patrol base, as well as a robust quick reaction force (QRF) and indirect or aerial fire support assets. Leaders must have plans to reinforce patrol bases in case of attack, as well as redundant communications means to request assistance from ground and aerial fire support assets.

Passive and active security must be planned and developed before, integrated during, and improved after building the patrol base. The base should be defendable, but not isolated from the secured area. Defensive barriers, such as Hescos or concrete walls that minimize exposure of the inhabitants of the patrol base, should be integrated. Fighting positions have to be planned and built. Active measures such as aggressive patrolling, counter-sniping, adjusting the daily routine, and counter-indirect fire means will prevent an enemy from successfully attacking the patrol base.

Force Protection (FP)

Minimum FP considerations include:

- Perimeter security (berms, walls, obstacles).
- Fighting positions (primary, alternate).
- Entry control points.
- QRF/reserve (organic and supporting).
- Active security measures including patrols and observation posts (OPs)/listening posts.
- Passive security measures including enforcement of noise and light discipline and use of night-vision devices and thermal sights.

Random Antiterrorism Measures (RAMs)

A key weakness for any base is predictability. RAMs consistently change the look of a PB FP program. In any attack, surveillance is one of the first steps of planning. The threat observes a PB looking for security posture vulnerabilities. RAMs introduce uncertainty to a site's overall FP program in order to defeat surveillance attempts and make it difficult for the enemy to accurately predict friendly actions. RAMs can and will effectively reduce the predictability factor and eliminate an adversary's advantage.

RAM actions:

- Maintain situational awareness of area and ongoing threats.

- Ensure all levels of personnel are notified of any changes in threat conditions and protective measures.
- Ensure personnel are alert and immediately report any threat or suspicious activity.
- Avoid routines and vary times and routes.
- Increase the number of visible security personnel wherever possible.
- Rearrange exterior vehicle barriers, traffic cones, and roadblocks to alter traffic patterns near facilities and cover by alert security forces.
- Institute/increase vehicle, foot, and roving security patrols, varying them in size, timing, and routes.
- Implement random security guard shift changes.
- Designate a QRF/reserve for contingencies.
- Limit the number of access points and strictly enforce access control procedures.
- Implement stringent identification procedures to include conducting 100 percent “hands-on” checks.
- Increase perimeter lighting.
- Deploy visible security cameras and motion sensors.
- Institute a robust vehicle inspection program.

Appendix

Chapter Index: *Joint Forward Operations Base (JFOB) Force Protection Handbook*, final draft edition, December 2006

CALL PUBLICATIONS INFORMATION PAGE

In an effort to make access to our information easier and faster, CALL has put all of its publications, along with numerous other useful products, on a Web site. The CALL Web site is restricted to Department of Defense personnel. The URL is http://call2.army.mil.

If you have any comments, suggestions, or requests for information, you may contact CALL by using the Web site "Request for Information or a CALL Product" or "Give Us Your Feedback" links at <http://call.army.mil>. We also encourage Soldiers and leaders to send in any tactics, techniques, and procedures (TTP) that have been effective for you or your unit. The TTP may be sent to us in draft form or fully formatted and ready to print. Our publications receive wide distribution throughout the Army, and CALL would like to include your ideas. Your name will appear in the byline.

If your unit has identified lessons learned or tactics, techniques, and procedures, please contact CALL using the following information:

Telephone: DSN 552-9569/9533; Commercial 913-684-9569/9533

Fax: DSN 552-4387; Commercial 913-684-4387

NIPR Email address: call.rfimanager@leavenworth.army.mil

SIPR Email address: call.rfiagent@leavenworth.army.smil.mil

Mailing Address: Center for Army Lessons Learned, ATTN: OCC, 10 Meade Ave., Bldg 50, Fort Leavenworth, KS 66027-1350.

If you would like copies of this manual or have a request for information (RFI), please submit your request at NIPR: http://call.army.mil **or SIPR:** http://call.army.smil.mil. Use the "Request Information or a CALL Product" link. Please fill in all the information to include unit name and official military address. Please include building number and street for military posts.

Additionally, we have developed a repository, the CALL Archives, that contains a collection of operational records (OPORDS and FRAGOS) from recent and past military operations. Much of the information in the CALL Archives is password-protected. You may obtain your own password by accessing our Web site and visiting the CALL Archives page. Click on "Restricted Access" and "CALL Archives Access Request." After you have filled in the information and submitted the request form, we will mail you a password. You may also request a password via STU III telephone or a SIPRNET e-mail account.

CENTER FOR ARMY LESSONS LEARNED

CALL's products are produced at Fort Leavenworth, KS, and are not distributed through publication channels. Due to limited resources, CALL selectively provides its products for distribution to units, organizations, agencies, and individuals and relies on them to disseminate initial distribution of each publication to their subordinates. Contact your appropriate higher element if your unit or office is not receiving initial distribution of CALL publications.

Installation distribution centers
Corps, divisions, and brigades
Special forces groups and battalions
Ranger battalions
Staff adjutant generals
TRADOC schools
ROTC headquarters
Combat training centers
Regional support commands

CALL PRODUCTS "ONLINE"

Access information from CALL's Web site. CALL also offers Web-based access to the CALL Archives. The CALL home page address is

http://call.army.mil

CALL produces the following publications:

CTC Bulletins, Newsletters, and Trends Products: These products are periodic publications that provide current lessons learned/TTP and information from the training centers.

Special Editions: Special Editions are newsletters related to a specific operation or exercise. Special Editions are normally available prior to a deployment and targeted for only those units deploying to a particular theater or preparing to deploy to the theater.

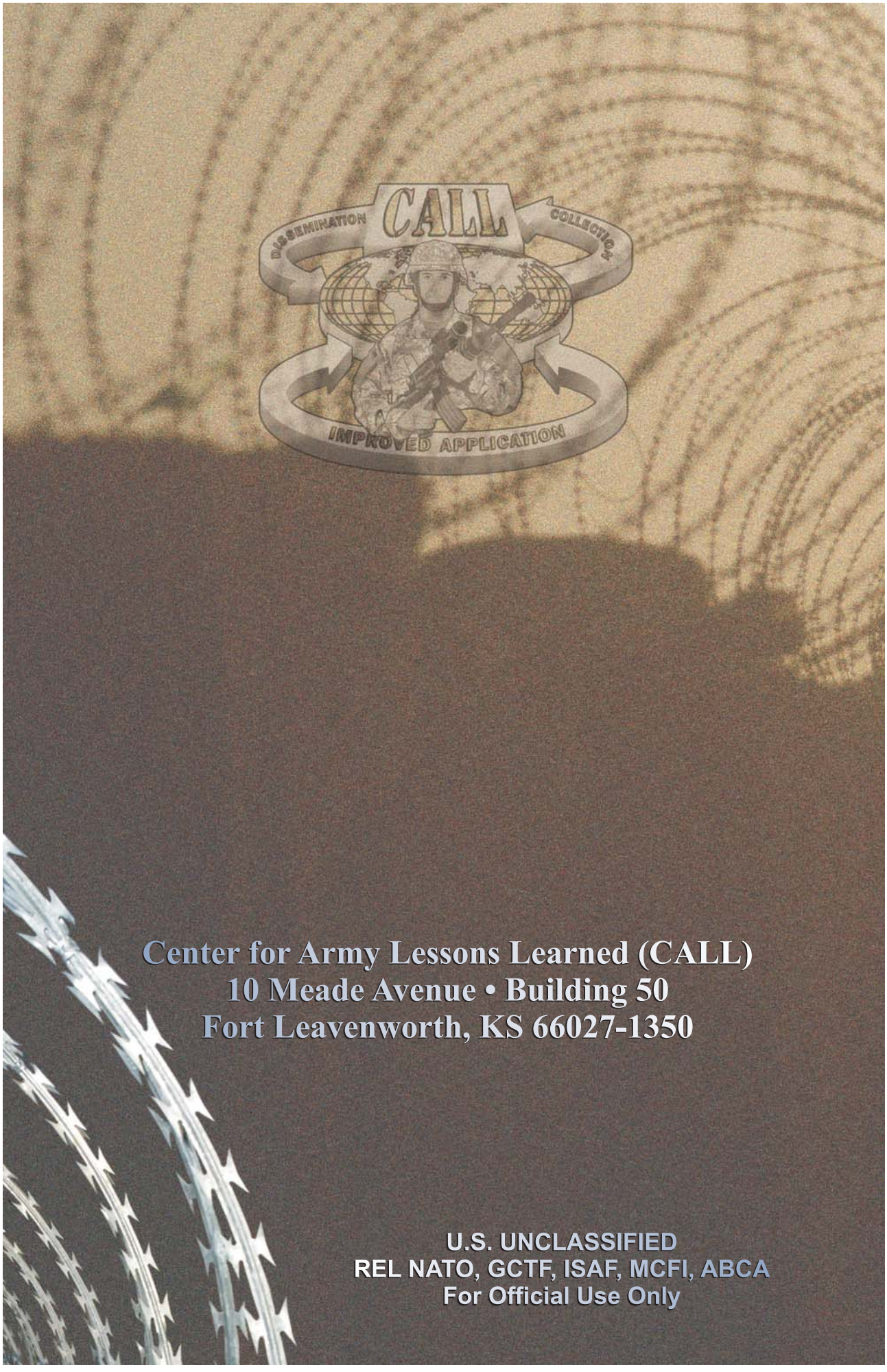
News From the Front*:* This product contains information and lessons on exercises, real-world events, and subjects that inform and educate Soldiers and leaders. It provides an opportunity for units and Soldiers to learn from each other by sharing information and lessons. *News From the Front* can be accessed from the CALL Web site.

Training Techniques: Accessed from the CALL products page, this online publication focuses on articles that primarily provide TTP at the brigade and below level of warfare.

Handbooks: Handbooks are "how to" manuals on specific subjects such as rehearsals, inactivation, and convoy operations.

Initial Impressions Reports: Initial Impressions Reports are developed during and immediately after a real-world operation and disseminated in the shortest time possible for the follow-on units to use in educating personnel and supporting training prior to deployment to a theater. Products that focus on training activities may also be provided to support the follow-on unit.

Support CALL in the exchange of information by telling us about your successes so they may be shared and become Army successes.



Center for Army Lessons Learned (CALL)
10 Meade Avenue • Building 50
Fort Leavenworth, KS 66027-1350