



TC 19-210

ACCESS CONTROL HANDBOOK

Headquarters, Department of the Army

OCTOBER 2004

DISTRIBUTION RESTRICTION: Distribution is authorized to US Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made 16 June 2003. Other requests for this document will be referred to Commandant, United States Army Military Police School, ATTN: ATSJ-MP-T, 401 MANSCEN Loop, Bldg 3203, Suite 1069, Fort Leonard Wood, MO 65473-8929.

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

HOMELAND SECURITY ADVISORY SYSTEM

SEVERE

SEVERE RISK OF
TERRORIST ATTACKS

HIGH

HIGH RISK OF
TERRORIST ATTACKS

ELEVATED

SIGNIFICANT RISK OF
TERRORIST ATTACKS

GUARDED

GENERAL RISK OF
TERRORIST ATTACKS

LOW

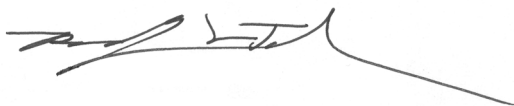
LOW RISK OF
TERRORIST ATTACKS

FOREWORD

The terrorist events of September 11, 2001, identified a critical need across the Army for the implementation of access control operations on installations. Identifying a set standard and method from which to execute access control operations continues to remain a challenge for installation commanders and their staffs. The United States Army Military Police School (USAMPS), Fort Leonard Wood, Missouri, compiled this access control handbook as a ready reference at the unclassified level to encourage the widest possible dissemination to installation staffs and their organizations.

This handbook focuses on access control and the requirements that commanders must consider when implementing an overall installation physical security (PS) plan. Specific areas of focus include access control point (ACP) descriptions and inspections, legal considerations, force protection conditions (FPCONs) and security measures, response force considerations, rules for the use of force (RUF), vehicle characteristics, and barriers/blast mitigation measures.

This handbook, along with the vehicle inspection checklist (VIC) that was developed by a technical support working group (TSWG) for the Directorate for Combating Terrorism (J-34), is intended as a quick reference guide. Commanders and staffs can also complement this handbook with other references, such as the *Installation Commander's Blueprint*, *Installation Preparedness for Weapons of Mass Destruction* (May 2001); the *Installation Commander's Force Protection Handbook* (July 2002); and *Field Manual (FM) 3-19.30*.

A handwritten signature in black ink, appearing to read 'Rodney L. Johnson', with a long horizontal line extending to the right.

Rodney L. Johnson
Colonel, US Army
Commandant, United States
Army Military Police School

**This publication is available at
Army Knowledge Online
<www.us.army.mil>.**

Training Circular
No. 19-210

Headquarters
Department of the Army
Washington, DC, 4 October 2004

Access Control Handbook

Contents

	Page
PREFACE.....	iv
Chapter 1 ACCESS CONTROL POINTS	1-1
Establishment	1-1
Description	1-2
Design Considerations	1-5
Chapter 2 ACCESS CONTROL POINT INSPECTIONS	2-1
Inspection Procedures	2-1
Hand-Carried Items	2-4
Vehicle Inspections	2-5

Distribution Restriction: Distribution is authorized to US Government agencies only to protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection applies to publications required solely for official use and to those containing valuable technical or operational information. This determination was made 16 June 2003. Other requests for this document will be referred to Commandant, United States Army Military Police School, ATTN: ATSJ-MP-T, 401 MANSCEN Loop, Bldg 3203, Suite 1069, Fort Leonard Wood, MO 65473-8929.

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

	Page
Chapter 3	LEGAL CONSIDERATIONS 3-1
	Access to Military Installations 3-1
	Inspections and Searches at Military Installations .. 3-2
	Military Law Enforcement Authority on Installations 3-9
	Use of Force 3-11
Chapter 4	FORCE PROTECTION CONDITIONS AND SECURITY MEASURES 4-1
	Force Protection Conditions 4-1
	Random Antiterrorism Measures Program 4-3
Chapter 5	INSTALLATION SECURITY AND RESPONSE FORCE CAPABILITIES 5-1
	Provost Marshal 5-2
	Tiered Response Capabilities 5-3
	Emergency Responders 5-3
	Special Reaction Team..... 5-6
	Augmentation Guard Force 5-7
	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Installation Support Team 5-8
	Quick-Reaction Force 5-12
Chapter 6	SPECIAL CONSIDERATIONS FOR ENTRY CONTROL POINTS..... 6-1
	Water Ports 6-1
	Airfields 6-4
	Rail Yards 6-5
	Pedestrian Gates 6-6
	Special Events 6-7
Chapter 7	SYSTEMS APPROACH TO SECURITY 7-1
	Support to Force Protection 7-1
	Systems Approach..... 7-2
	One-Team Concept 7-4

Appendix A	METRIC CONVERSION CHART	A-1
Appendix B	VEHICLE INSPECTION HOT SPOTS	B-1
Appendix C	RULES FOR THE USE OF FORCE	C-1
Appendix D	FPCON SECURITY MEASURES UNDER AR 525-13 REQUIREMENTS	D-1
	FPCON NORMAL	D-1
	FPCON ALPHA	D-1
	FPCON BRAVO	D-3
	FPCON CHARLIE	D-6
	FPCON DELTA	D-7
Appendix E	BARRIERS AND BLAST MITIGATION.....	E-1
	Hazard Types	E-1
	Technical Definitions	E-2
	Explosive Detection	E-3
	Blast Mitigation	E-4
	Barriers	E-4
	GLOSSARY	Glossary-1
	BIBLIOGRAPHY	Bibliography-1
	INDEX	Index-1

Preface

This handbook provides installation commanders with the basic information necessary for effective access control to their installations. It does not discuss the technical issues involved with standards and designs. Information regarding standards and designs is evolving and will be resolved by the Headquarters (HQ) Department of the Army (DA) PS Review Board (DAPSRB) and the PS integrated concept teams. This handbook provides commanders with the legal and jurisdictional issues associated with the inspection procedures at an ACP. Additionally, this handbook equips operators (which includes military police [MP], DA police, and sentinels of augmenting units) of an ACP with the various vehicle inspection criteria and measures necessary to conduct an effective ACP.

The openness of the United States (US) society provides an opportunity for our enemies to operate with more freedom than they would have in more restrictive venues. Also exacerbating the threats is the global proliferation of cheap weapons of mass destruction (WMD) and the means to disseminate knowledge about such weapons. Few US cities are fully prepared to deal with incidents involving WMD. Critical infrastructure and the US economy are becoming increasingly more reliant on information and computer-based technologies that are vulnerable to covert attacks. Many military installations and facilities are key force projection platforms and are susceptible to attacks from terrorists using WMD, from unconventional special forces formed from elements infiltrated into the United States, or from indigenous hostile elements.

As a result of recent events, Army installations have increased their force protection (FP) readiness through increased access control operations. Access control is a major implied security mission that supports the installation FP program. The FPCON determines the level of operation at an ACP, and thus, the ACP must be able to quickly and easily enhance security under an increased FPCON. ACPs serve as the access point for all personnel, vehicles, and deliveries to an installation. The ACP becomes the first chance for

forces to inspect incoming personnel, vehicles, and cargo in order to detect, assess, and deter an incident.

Installation commanders must establish installation access control procedures that comply with Department of Defense (DOD) and DA policies. In addition to these policies, installation commanders must consider—

- Manpower availability.
- FPCON.
- ACP layout.
- Other factors, all of which will influence a commander's manning level for an access control operation.

When considering installation access control, commanders must reflect on its purpose, the impact on the surrounding community, and the end state. The purpose of access control is to identify, reduce, or eliminate installation and in-transit vulnerabilities to threats and to enhance the overall FP posture while minimizing the impact on normal operations. The end state is to protect the forces through a myriad of measures that are addressed in the installation access control plan. FPCON levels and access control measures are established in a graduated scale based on the intelligence provided by a threat fusion cell.

Many new concepts that are discussed in this handbook were taken from the following documents:

- *Installation Force Protection Operational and Organizational (O&O) Plan.*
- *Installation Commanders' Blueprint, Installation Preparedness for Weapons of Mass Destruction.*
- *Installation Commander's Force Protection Handbook.*

Army Regulation (AR) 25-30 mandates that all Army programs and functions will use the metric system. To ensure compliance with this requirement, a metric conversion chart is provided in Appendix A.

The proponent for this publication is HQ TRADOC. Send comments and recommendations on *DA Form 2028 (Recommended Changes to Publications and Blank Forms)* directly to Commandant, United States Army Military Police School, ATTN: ATSJ-MP-T, 401 MANSCEN Loop, Bldg 3203, Suite 1069, Fort Leonard Wood, Missouri 65473-8929.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

Access Control Points

The purpose of an ACP is to prevent unauthorized access to the installation while maximizing vehicular-traffic flow. The difference between ACPs and entry control points (ECPs) is that ACPs are those points along an installation boundary that represent an initial security screening point for vehicles and, in some cases, pedestrians entering the installation or cantonment area. Those facilities or locations within the boundary of an installation that require restricted entry are referred to as ECPs. ECPs are generally located at airfields, ammunition supply points (ASPs), high-security areas, HQ complexes, and so forth.

ESTABLISHMENT

1-1. In this discussion, the site selection, site design, and affiliated construction standards of an ACP will not be addressed. The Corps of Engineers will manage these issues once they are determined by the HQDA Access Control Working Group, a subcommittee of the DAPSRB.

1-2. Of importance to an installation commander in the establishment of an ACP is the necessity to conduct a traffic control study of the site being considered. The traffic study must analyze traffic patterns that support or will be affected by the construction of the ACP. The Military Traffic Management Command (MTMC) can assist in this process. The results of the study will ensure the proper placement of an ACP, with

consideration to it being sited at a distance inside the installation to facilitate the queuing of vehicles without creating an off-post traffic problem.

DESCRIPTION

1-3. This section refers to the physical boundaries of the installation and does not address jurisdictional issues off post. An ACP should be subdivided into four zones, each encompassing specific functions and operations. Beginning at the installation boundary, the access zones (*Figure 1-1*) include the—

- Approach zone.
- Access control zone.
- Response zone.
- Safety zone.

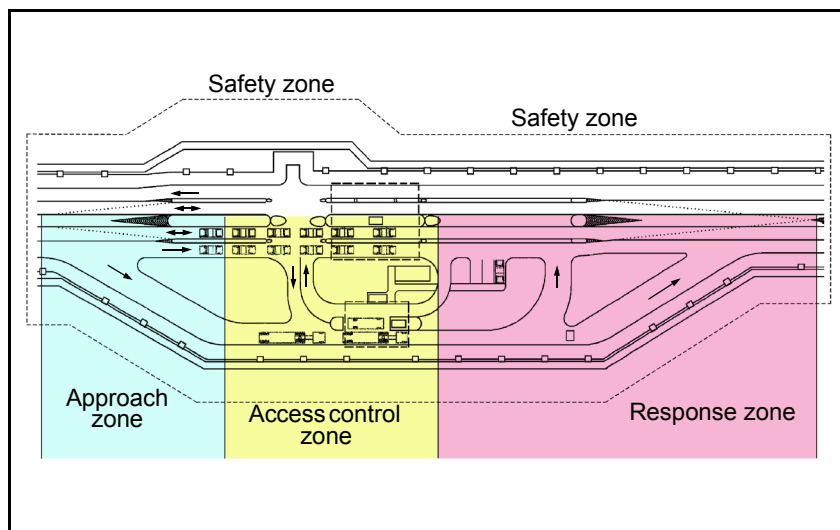


Figure 1-1. Access Control Zones

APPROACH ZONE

1-4. The approach zone lies between the installation boundary and the access control zone. It is the area in

which all vehicles must pass through before reaching the actual checkpoint. Specific functions that occur in the approach zone are—

- Reducing the speed of incoming vehicles.
- Sorting of traffic by vehicle type. For example, sorting employees, visitors, and delivery trucks into the proper lane before reaching the checkpoint.
- Providing adequate queuing distance for vehicles waiting for entry to ensure minimal impact on traffic flow off post. This is particularly important during times of peak traffic.
- Providing an appropriate standoff distance (*Figure 1-2*, page 1-4) to allow the access controller to identify a potential threat vehicle, including any attempting entry through the outbound traffic lanes. This nationally recognized chart is enlarged on the inside of the back cover for easier viewing.

1-5. Roadway layout and traffic control devices (such as signs, message systems, signals, and lane control markings) should be used to perform the functions of the approach zone. Drivers should be notified of the upcoming ACP, the proper speed of travel, and lane usage. The length of the approach zone will depend upon the amount of space available, the distance required to sort traffic, and the required space necessary for creating additional traffic lanes. The approach zone must also consider temporary traffic control measures, such as the placement of traffic barriers to constrain and slow traffic, that are frequently used during higher FPCON levels and those measures relative to the implementation of the Random Antiterrorism Measures Program (RAMP).

ACCESS CONTROL ZONE

1-6. The access control zone is the primary controlling element of the ACP and lies between the approach and

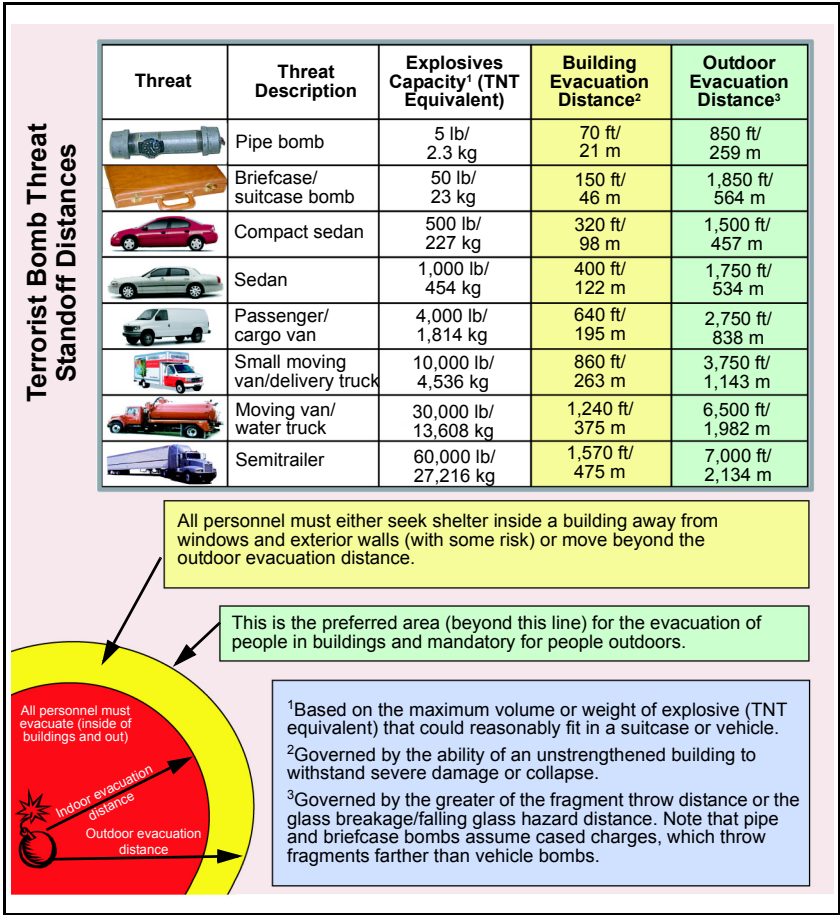


Figure 1-2. Standoff Distances

response zones. This zone includes the gatehouse and the traffic management equipment used in support of the work of the access controllers. The purpose of the access control zone is to determine the authorization of the vehicle to enter the installation and, based on FPCON level requirements, verify the identity of individuals.

RESPONSE ZONE

1-7. The response zone is the area extending from the end of the access control zone to the location of the final active vehicle barrier. This zone defines the end of the ACP. The purpose of the response zone is to allow the security force to respond to a threat, operate the active vehicle barriers, and close the ACP if necessary. The amount of response time (that amount of time required for complete activation of the active vehicle barriers once a threat is detected) required to respond to a threat is dependent upon the speed that a vehicle is traveling. Therefore, a faster-moving vehicle reduces the response time of the access controller to react to a perceived threat.

SAFETY ZONE

1-8. The safety zone extends from the active and passive vehicle barriers, which define the boundary of the ACP. The potential for a terrorist vehicle exploding in the safety zone exists, and therefore, consideration should be given to the effects that an explosion may have on nearby personnel, buildings, or other assets. See the standoff distances in *Figure 1-2*.

DESIGN CONSIDERATIONS

1-9. Although this handbook does not address the specific standards of design for an ACP, it does reference many considerations that should be taken into consideration when designing an ACP. These considerations are not all-inclusive, but are provided to provoke thought when constructing and operating an ACP. Considerations include layout, traffic and traffic control, pedestrians, and electrical power and lighting.

LAYOUT

1-10. Layout considerations include those guidelines that support the requirements of the four ACP zones. These considerations may vary from installation to

installation due to geographical differences in size, location, and so forth of the ACP and its zones. Layout considerations include—

- **General.**
 - Providing expansion potential due to increased traffic volume.
 - Limiting the proximity of the ACP to nearby facilities with regard to explosions. This may require that an existing ACP be hardened to offset the effect of an explosion.
- **Approach zone.**
 - Using simple or reverse curves, S curves, or traffic circles in the roadway to reduce and control the traffic speed. Curves must be adequate to support the various types of vehicles.
 - Employing temporary barriers, which are required by the installation antiterrorism plan at designated FPCONs. Installations may use Jersey barriers, water-filled plastic barriers, or similar obstructions to reduce the number of lanes and the traffic speed.
 - Maximizing the length of the approach zone to provide optimal sorting distance for the traffic queue.
 - Using reversible lanes to facilitate increased throughput and flexibility where space is unavailable for additional lanes.
 - Sorting traffic when necessary or desirable, such as using the far right lane for truck traffic. This action facilitates the rejection of these vehicles by supporting their larger turning radii.
- **Access control zone.**
 - Providing infrastructure to support manual and automated identification and inspection procedures for inbound and outbound lanes.
 - Providing a location and support for inspection equipment.

- Providing an overhead canopy at the main identification area to protect against inclement weather, facilitate identification and inspection procedures, and provide a platform for lighting and closed-circuit television (CCTV).
- Providing rejection points.
- Providing a channelization island between all inbound and outbound lanes.
- Designating an area to conduct privately owned vehicle (POV) inspections out of the traffic lanes.
- Providing at least one gatehouse, located centrally on a median or positioned to the side of the ACP.
- **Response zone.**
 - Providing a sufficient length of roadway to allow adequate reaction time for security personnel to respond to a threat.
 - Implementing active vehicle barriers at the termination of the ACP to provide the capability to stop threat vehicles from using high-speed attacks to gain entry to the installation.
 - Providing full containment and control of vehicles through the use of active and passive vehicle barriers.

TRAFFIC AND TRAFFIC CONTROL

1-11. Traffic and traffic control considerations deal directly with the traffic encountered at an ACP and the means to move it successfully through the ACP without causing undue congestion or preventing the installation from performing its mission. Such considerations include—

- Analyzing the results of the traffic survey.
- Coordinating with local law enforcement (LE) and the Department of Transportation (DOT) to

determine the effects of increased FPCON levels on off-post traffic.

- Keeping the location of the ACP away from intersections.
- Designing the ACP based on the peak hours traffic volume.
- Affording an adequate number of lanes to process the volume of traffic.
- Using signs, markings, and signals to perform traffic control and to satisfy regulatory requirements. Regulatory signs provide information on traffic laws and regulations, while warning signs, markings, object markings, and delineators indicate hazards to drivers. Sign information, such as shapes and markings, can be found in the latest edition of the Federal Highway Administration booklet called *Standard Highway Signs*. Traffic control devices will comply with the latest edition of the *Manual on Uniformed Traffic Control Devices for Streets and Highways* (which is the national standard according to *Title 23, US Code [USC]*) and applicable state laws.
- Posting appropriate speed limits through the various zones to protect access controllers and to minimize the potential for vehicular accidents.
- Using other traffic control devices (such as rumble strips, speed bumps, guardrails, and posted signs indicating active vehicle barriers).

PEDESTRIANS

1-12. Many installation ACPs handle pedestrian traffic. Special considerations that must be afforded to accommodate this traffic include—

- Providing a sidewalk and safety provisions (such as signs or fences) to direct pedestrians to the appropriate location of the ACP while separating them from vehicular traffic.

- Ensuring that entry controllers have direct visual contact with the pedestrians.
- Providing breaks in the passive barriers to allow pedestrians through to access the ACP.
- Incorporating ACP procedures at turnstiles, when present.

ELECTRICAL POWER AND LIGHTING

1-13. The electrical-power design must consider the current power demands and the power requirements for future ACP technology associated with automated ACPs. This technology may include traffic control devices and identification equipment. Another consideration for power is to have a backup power source available for disrupted power.

1-14. The two facets to consider about lighting are the external and the interior lighting. Some considerations for external lighting include—

- Providing multiple, redundant luminaries to ensure that the loss of a single luminary does not seriously degrade the total available lighting to access controllers.
- Using typical roadway lighting in the approach and response zones. This lighting should provide enough intensity so that pedestrians, access controllers, islands, signage, and hazards can be seen.
- Directing lighting so that it is not in the driver's eyes and does not backlight important signage.
- Integrating the selected light sources with CCTV.

1-15. Some considerations for internal lighting are—

- Using diffused lighting that is adjusted with dimmer controls. This lighting aids with night vision and reduces the ability of those outside the guard booth to see inside.
- Connecting the lighting to the backup power source.

- Limiting the illuminance inside the guard booth to the minimum required for comfortable completion of expected tasks.

OTHER CONSIDERATIONS

1-16. There are a myriad of other considerations to be concerned with when designing an ACP. For example, all ACP facilities must have telephone capabilities. Some installations may require a ring-down telephone, which provides a direct line to the installation emergency dispatch, control center, or MP station. ACPs must provide water for general use and rest rooms for ACP personnel. Likewise, waste system utilities must be provided for the rest rooms.

1-17. Access controllers must be afforded protection and comfort. The guard booths, in which access controllers will be posted, must be elevated above the roadway and protected from accidental impact from traffic in either direction (inbound and outbound) through the use of barrier systems or crash cushions. Consideration for a comfortable work environment should be afforded to the design of the guard booth. It must provide enough work space, based upon the number of access controllers, and provide protection from the elements. Heating and air conditioning in the guard booths should also be provided as comfort measures.

1-18. The provision of an overhead canopy protects access controllers and drivers during inclement weather. It may also improve lighting and can serve as a platform for traffic control devices, signage, and security equipment.

1-19. There are many other factors to consider and adhere to when designing an ACP. They, along with specific standards, can be found in the references cited in the bibliography.

Chapter 2

Access Control Point Inspections

Installation commanders are responsible for protecting the personnel and property under their jurisdiction and for maintaining order on the installation. A key part of that responsibility is the requirement to prescribe procedures for inspecting persons and their property and vehicles at entry and exit points of the installation. The question of whether a vehicle examination is an inspection or a search ultimately rests on the decisions of the Court of Military Appeals. In this handbook, the term “inspection” is used to describe a PS measure. An inspection is different from a search in that an inspection is not based on reasonable suspicion or probable cause. An ACP inspection is the examination of a vehicle or a hand-carried item without the justification for a search.

INSPECTION PROCEDURES

2-1. Installation commanders may direct or establish procedures for ACP inspections of all or randomly selected vehicles entering or leaving an installation under their jurisdiction. This is regardless of whether the owner or operator of the vehicle is military or civilian. Civilians attempting to enter an installation should not be inspected over their objection, but instead, should be denied access to the installation. However, such refusal should be documented, reported, and treated as suspicious activity. Other ACPs should be notified with a description of the vehicle and occupants

to ensure that they do not try to gain access at another ACP. Vehicle inspections at ACPs are not based upon probable cause, but are based on the commander's authority to protect the security of the installation, protect government property, and prevent theft.

2-2. All personnel entering an Army installation should have at least one form of official photo identification. Normally, all visitors are required to sign in and receive a temporary pass to enter the installation. Local policy describes the procedure for issuing temporary passes.

IDENTIFICATION DOCUMENTS

2-3. The installation commander may direct what form of personal identification will be used to gain access to the installation. When conducting 100 percent hands-on identification verification checks, access controllers normally verify the identification of individuals by using one of the following documents or methods:

- **DOD identification card.** These can include the following:
 - *DA Form 1602 (Civilian Identification)* or other US DOD uniformed services civilian identification card, issued to DOD civilians.
 - *Department of Defense (DD) Form 2 (RES) (Armed Forces of the United States Geneva Convention Identification Card)*, issued to reserve or guard members in all branches of service.
 - *DD Form 2 (RET) (United States Uniformed Services Identification Card [Retired])*, issued to retired military in all branches of service.
 - *DD Form 2A (ACT) (Active Duty Military ID Card)*, issued to active duty military in all branches of service.
 - *DD Form 1173 (United States Uniformed Services Identification and Privilege Card)*, issued to military family members and

dependents of foreign country representatives.

- *DD Form 1173-1 (DOD Guard and Reserve Family Member Identification Card)*, issued to Reserve Component and Guard dependents in all branches of service.
- *DD Form 2574 (Armed Forces Exchange Services Identification and Privilege Card)*, issued to Army and Air Force Exchange Service (AAFES) employees.
- *DD Form 2765 (Department of Defense/Uniformed Services Identification and Privilege Card)*, issued to foreign country representatives.
- **Valid state driver's license or state identification card with photo.** If the state driver's license or identification card lacks a photo, then the driver's license must be cross-referenced with another form of photo identification.

If an individual does not have one of the verification documents listed above, local policy may require them to present two forms of identification.

PHOTO IDENTIFICATION CHECKS

2-4. Access controllers physically take the card and compare the picture on the card to the person. Other measures include checking both sides of the card for the following:

- Expiration date.
- Modifications or discrepancies.
- Physical characteristics against the person's physical appearance.
- Holograms, where appropriate.
- That the card is not damaged, coming apart, or showing signs of tampering or alteration.

2-5. If a DOD identification is unserviceable (25 percent of the card is damaged or coming apart) or expired, confiscate the card and complete a *DA Form 4137 (Evidence/Property Custody Document)*. Direct the individual to have a new identification card issued. If there is evidence of tampering or alteration, confiscate the card, deny entry, and notify the MPs. According to state statutes and staff judge advocate (SJA) opinion, the denial of entry to civilians due to altered or tampered identification is an issue for the local commander. When civilians are detained, summon the civilian police immediately.

HAND-CARRIED ITEMS

2-6. At some ACPs/ECPs, access controllers are required to check hand-carried items. These items may include briefcases, purses, packages, boxes, and backpacks. The check of hand-carried items is an examination, not a search. During the examination, have the person open the item and reveal the contents. If during the inspection, an item is discovered that may cause a public safety concern, stop the check and notify the supervisor. If a person refuses an examination of a hand-carried item, deny them entry and notify the supervisor. Look for the specific items as discussed below.

FIREARMS

2-7. It is against Army policy to carry firearms onto an installation. Exceptions, such as those carried by LE personnel or legal hunters, are established by local policy.

KNIVES

2-8. Normally, daggers, swords, and other cutting or stabbing devices are prohibited. Folding knives with a blade of 3 inches or less are excluded from this definition, but local policy will dictate.

EXPLOSIVE MATERIALS

2-9. Watch for such items as dynamite, anything marked “explosive,” blasting caps, composition 4 explosive (C4), or fireworks.

OTHER DANGEROUS ITEMS

2-10. Local guidance will further define current threat-specific dangerous items. In general, a personal protection device, such as commercially purchased mace, is not considered an illegal weapon. An examination should not focus on looking for illegal drugs or contraband; but if illegal materials or substances are recognized during the course of the examination, detain the individual and notify the MPs.

SUSPICIOUS DANGEROUS ITEMS

2-11. If a person is discovered in possession of a firearm or an explosive device, maintain control of the firearm or device, detain the person, and notify the MPs. Follow these procedures if an explosive device is dropped or somehow ends up in your possession:

- Do not handle the item.
- Clear the area according to the standoff distances shown in *Figure 1-2*, page 1-4.
- Report the incident through the appropriate LE channels.
- Secure the area, and detain the person(s) involved.
- Keep everyone clear of the area until the responding emergency agency arrives. If the person leaves before he can be detained, give a complete description and the direction of travel to the appropriate LE agency.

VEHICLE INSPECTIONS

2-12. Normally, Army installations have vehicle and cargo inspection requirements that vary with FPCON

levels. These requirements range from random vehicle content inspections to content inspection of all vehicles. During a random vehicle content inspection, it is important to conduct the inspection without impeding the traffic flow through the ACP or placing the access controller in the traffic flow. This is best accomplished by the use of separate inspection lanes, a pull-off area, or the dedication of a lane as dual-purpose, such as visitor and inspection. Planning considerations for special lanes should include the expansion of operations during higher FPCONs. Access control managers should clearly define the levels of inspection likely to occur for the different types of vehicle traffic (delivery vehicles, authorized vehicles, and visitor vehicles).

2-13. A centralized commercial vehicle inspection station should be available to inspect all delivery and commercial vehicles. If available, require all delivery and commercial vehicles and vehicles pulling trailers to enter a specific gate (as prescribed by local policy). These procedures centralize the commercial vehicle inspection function and potentially reduce manpower and resource requirements.

2-14. POV and commercial vehicle inspection operations are greatly improved when a standard procedure is used. The source document to use for vehicle inspections at all Army installations is the VIC.

2-15. A complete VIC training support package (TSP) is now available for use in preparing security and emergency response personnel to inspect vehicles. The TSP consists of printed instructor guidance, a student manual, and a slide presentation for instructional use. Included are two video home system (VHS) tapes, one containing a train-the-trainer video and the other containing three lessons, unit support summary video clips, and a final exam. Also included are two compact disks read-only memory (CD-ROMs) with train-the-trainer video clips. To receive cost information or order online, send an e-mail request to <*pubs@tswg.gov*>. Include the quantity desired, contact name,

organization, address, and telephone number. Confirmation of the order will be sent via e-mail with an approval number.

2-16. During the inspection of a vehicle, ask the driver to open all compartments, doors, the hood, and if applicable, the trunk. If anything suspicious is found, follow local procedures (the inspection area will likely be evacuated and explosive ordnance disposal [EOD] personnel will probably be notified). Remember that you are not only looking for the “big bomb,” but any type of weapon, improvised explosive device (IED), or cache of explosives.

2-17. A vehicle can be considered suspicious or to contain a suspicious item if the driver refuses to open any compartment (for example, hood, trunk, passenger door[s], glove box, or even a package). Finish inspecting one compartment before starting on another. It may be necessary to inspect by feeling in areas that cannot easily be seen. If something is found, **DO NOT PULL IT OUT**.

2-18. *Appendix B* shows vehicle inspection “hot spots” that access controllers may encounter on various vehicle types. A hot spot is an area on a vehicle where a device or contraband could be hidden. These areas require special attention during inspections.

2-19. The external portion of the vehicle should be inspected by walking around it in a clockwise direction and then in a counterclockwise direction (*Figure 2-1*, page 2-8). Inspect the external portion of the vehicle as follows:

- Inspect from the bottom of the vehicle and work to the top.
- Look for body repairs or freshly painted sections, anything indicating tampering with the external surface of the vehicle.
- Use a flashlight and a mirror with a creeper (if possible) to carefully inspect under the vehicle.

- Check the suspension, the drive train, the wheel wells, the bumpers, under the engine, and above the gas tank.
- Look for any unusual devices that are taped, tied, screwed, or otherwise attached to the undercarriage.
- Look for an unusually clean portion of the undercarriage, the presence of new weld marks, or new bolts or screws.
- Check that all connections are properly made (for example, the gas tank filler tube runs from the fill port to the tank or the exhaust pipe runs from the manifold along the entire length of the vehicle to the muffler). Inspect the exhaust pipe for inserted objects.

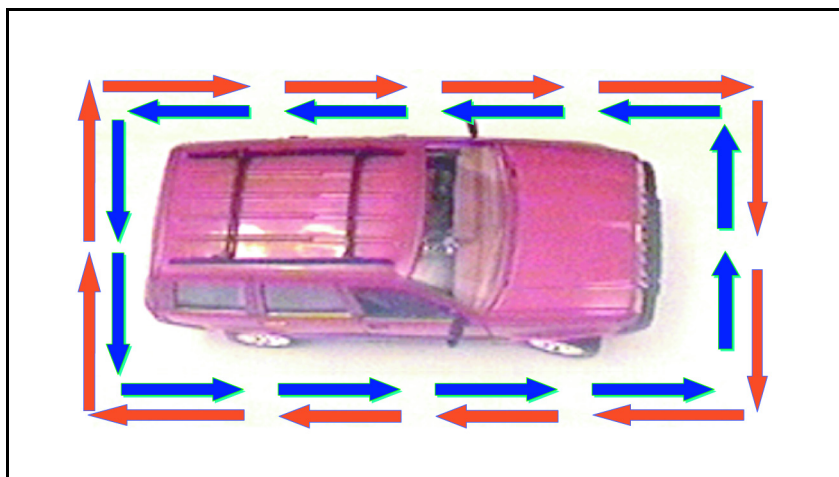


Figure 2-1. Exterior Inspection

2-20. The engine compartment of a vehicle (*Figure 2-2*) should be inspected as follows:

- Take a minute to observe everything within view, and then start at the outer most edge (the front or side the battery is on) of the compartment and work towards the center of the vehicle.

- Look for additional wires running from the vehicle battery.
- Look for out-of-place or unusually clean components, devices, and/or wiring and electrical tape.
- Check under larger components (for example, the air cleaner and fan blade shrouds) for packages or devices.
- Look for containers that may contain fuel, indicating that the gas tank may contain an explosive charge.
- Inspect the insulation on the firewall, hood, and so on for rips, tears, bulges, and repairs.
- Look for additional wires running from the hood light or the absence of a bulb in the hood light socket.



Figure 2-2. Engine Compartment Inspection

2-21. The inside of the trunk of a vehicle should be inspected as follows (*Figure 2-3*, page 2-10):

- Take a minute to observe everything within view, and then begin at the edge and inspect inward.
- Pay attention to packages/devices that look out of place (for example, alarm clocks or iron or polyvinyl chloride [PVC] pipe). Even things normally found in a trunk should be inspected (for example, tool boxes and supplies such as blankets and water containers).
- Look for bits of electrical tape, wire, stripped wire insulation, string, fine wire, fishing line, and/or a time fuse on the floor.
- Check for hidden compartments (for example, spare tire well or jack/tool storage).
- Check for any additional or improvised wires attached to the brake lights or rear turn signals.
- Look in the area behind the rear seat.



Figure 2-3. Inside Trunk Inspection

2-22. The passenger compartment of a vehicle should be inspected as follows (*Figure 2-4*):

- Observe everything within view, and then start at the floor and work up. Pay close attention to packages and devices that look out of place (for example, alarm clocks or iron or PVC pipe).
- Look for bits of electrical tape, wire, stripped wire insulation, string, fine wire, fishing line, and/or a 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.

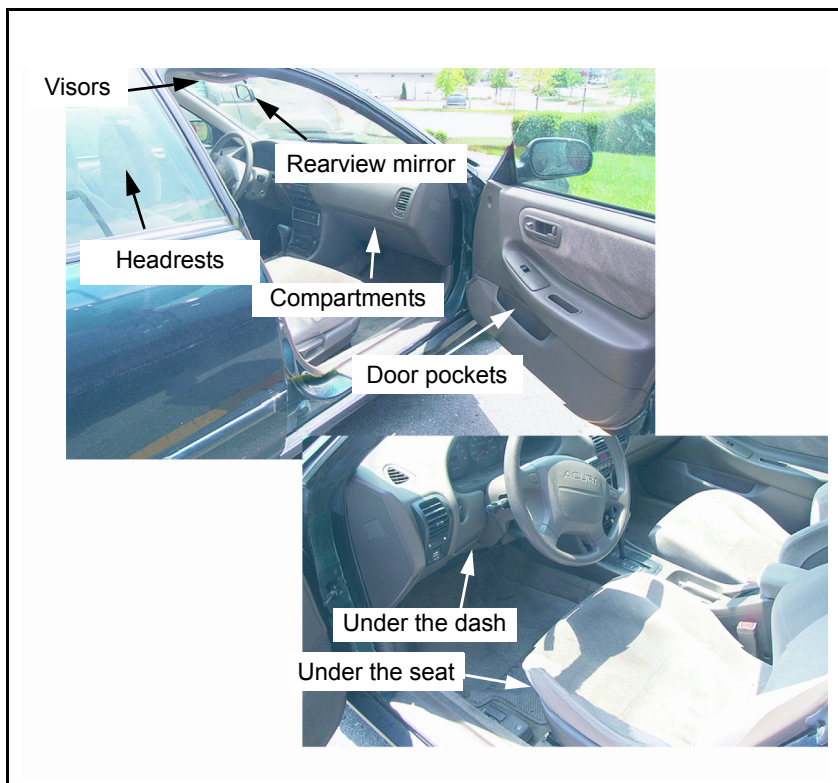


Figure 2-4. Passenger Compartment Inspection

Chapter 3

Legal Considerations

DOD Directive (DODD) 1325.6 provides that the commander of a military installation or other military-controlled facility under the jurisdiction of the United States shall prohibit any demonstration or activity on the installation or facility that could result in interference with, or prevention of, orderly accomplishment of the mission of the installation or facility; or present a clear danger to loyalty, discipline, or morale of the troops. It is a crime for any person to enter a military reservation for any purpose prohibited by law or lawful regulations or for any person to enter or reenter an installation after having been barred by order of the commander under *Section 1382, Chapter 67, Part I, Title 18, USC*.

ACCESS TO MILITARY INSTALLATIONS

3-1. The installation commander must develop a restricted-access plan providing for increased vigilance and more restrictive installation access as required by circumstances (*AR 190-16*). This restricted-access plan will be activated in the event of a—

- National emergency.
- Disaster.
- Terrorist or hostile threat (FPCON).
- Significant criminal action.
- Civil disturbance.
- Contingency that would seriously affect the ability of the installation to perform its mission.

3-2. The commander's authority to exclude civilians from an installation is an inherent right and does not depend on statute or legislative jurisdiction. The *Internal Security Act of 1950* and *Section 797, Subchapter I, Chapter 23, Title 50, USC*, as implemented by *DODD 5200.8* and *AR 190-13*, give commanders the authority to control access to the installation by issuing regulations with penal force when the security or protection of the facility or property is the major interest.

3-3. *Section 1382, Chapter 67, Part I, Title 18, USC*, provides statutory authority to exclude individuals from an installation, makes post regulations criminally enforceable against trespassers, and makes it a criminal offense to reenter the installation for any purpose after having been removed or after being ordered not to reenter. The installation commander should personally issue a bar letter to individuals that he has restricted from the installation. A bar letter is a written order directing the individual not to reenter the installation. A copy of this letter should be retained as evidence to prove that actual notice not to enter was given. The reasons for issuing a bar letter must be reasonable and the installation commander cannot act arbitrarily or capriciously when issuing a bar letter.

INSPECTIONS AND SEARCHES AT MILITARY INSTALLATIONS

3-4. Installation commanders are required to establish appropriate rules governing the entry and exit on an installation (*AR 190-16*). This includes the inherent responsibility and power to conduct inspections of personnel and property within his control. The purpose of an inspection is to determine and ensure the security, military fitness, and good order and discipline of the installation. Again, an inspection is different from a search in that an inspection is not based upon reasonable suspicion or probable cause. The principal type of inspection is the gate inspection.

INSPECTIONS

3-5. Entry onto a military installation is a privilege, not a right. All personnel entering the installation are subject to inspections. Civilians who object to an inspection upon entry will be denied access to the installation. Individuals, who upon presenting themselves at the gate for inspection and who present probable cause to believe that they are in violation of the law (for example, driving under the influence [DUI]), will be taken into custody and processed for the offense. All personnel are subject to inspections upon leaving an installation, regardless of their objections.

Army Regulation 190-16 and Military Rule of Evidence 313

3-6. Scheduling inspections is an incident of command. The primary purpose of an inspection is to ensure the security, military fitness, and good order and discipline of the installation. Inspections should be conducted in a reasonable manner, all personnel should be treated the same, and technical aids (for example, military working dogs [MWDs]) are authorized for use during inspections. The scope of the inspection and the manner in which it is carried out are directed by the commander. The installation commander must issue specific written instructions that state the times, locations, scope, and method of the inspections. The inspectors simply carry out the directives of the commander.

3-7. Any contraband found as a result of inspections will be confiscated, and the individual(s) will be taken into custody. All personnel are subject to both administrative and criminal sanctions for the possession of contraband. While on the installation, personnel are also subject to inspections directed by the installation commander pursuant to *Military Rule of Evidence (MRE) 313*. Vehicle inspections at other locations on the installation are also authorized to be conducted for the purposes of road safety or installation security. All personnel are required to comply with these inspections.

Implied Consent

3-8. The installation commander can place conditions on the acceptance of a vehicle pass for driving on the installation. Drivers, occupants, and vehicles may be granted installation access (pass) with the provision that they consent to being searched while on the installation. The acceptance of a pass with the applicable notice provisions (consent to search) is an authorized use of the commander's inherent power on the installation. The occupants of the vehicle must be placed on notice that they are providing consent to being searched (to include the vehicle) upon acceptance of the vehicle pass. An application for a vehicle pass and the pass itself should provide notice in bold letters (in large type) that acceptance of the pass grants consent to search the passenger(s) and vehicle at any time while on the installation.

SEARCHES

3-9. Military judges, magistrates, and commanders who are responsible for the property to be searched have authority to grant search authorizations when presented with facts and circumstances that support probable cause that the evidence and/or person to be sought is in a specific location where there is a reasonable expectation of privacy. When granting search authorizations, commanders must be neutral and detached—they cannot be involved in the actual investigative process.

3-10. Probable cause is defined as: Would a reasonable person looking at the facts and circumstances presented believe that the specific evidence to be sought is in a location where there is a reasonable expectation of privacy right now? In other words, are there facts and circumstances presented that would lead a reasonable person to believe that it is more likely than not that the evidence to be found is in a certain location where there is an expectation of privacy? If the commander finds there is probable cause, a search authorization can be issued.

3-11. A search authorization is a directive to the person applying for the authorization to search the specified location for the specific evidence to be seized. Probable cause determines the scope of the search. For example, if you are looking for an elephant, you cannot look for that elephant in a matchbox because it would not fit inside it. Search authorizations can be granted orally or in writing. If granted orally, a record of the facts and/or circumstances supporting probable cause and the explicit authorization provided should be kept. Exceptions to the requirement for a search authorization include—

- **Inspections.** Inspections at entry points to the installation.
- **Government property.** Government property that is issued for other than personal use (such as computers, military vehicles, and working space). Items such as wall lockers, footlockers, family quarters, bachelor officers' quarters (BOQ), and bachelor enlisted quarters (BEQ) are issued for personal use and have an expectation of privacy.
- **Consent to search.** Individuals can voluntarily consent to a search of areas where there is an expectation of privacy. A person who has apparent authority over the property may consent to a search of that property. Consent must be voluntary and not mere submission to authority. Consent given can be withdrawn or tailored to a time or location. Once withdrawn, the consent previously given is no longer valid. When two people have apparent authority over property, either person can provide consent that will override the other person's lack of consent. For example, a civilian wife who is at the MP station can consent to a search of the on-post quarters that she lives in with her military husband, even if the husband is at the house at the time the consent search is conducted and does not want the search. The wife's consent to

search is valid, and the search will be conducted over the protests of the military husband.

- **Incident to lawful apprehension (military) or lawful detention (civilian).** Pursuant to a lawful apprehension or detention based on probable cause to believe a crime has been committed, the person apprehended or detained will be searched for weapons, methods of escape, and contraband that can be destroyed. The person, to include the lunging area where such items can be immediately obtained, will be searched. When an apprehension or detention is made of a person in a vehicle, the lunging area includes the passenger compartment and all unlocked containers located in the passenger compartment. An apprehension or detention does not authorize a search of the trunk unless the trunk is open and is within the lunging area.
- **Plain view.** Any time the police are in an area where they have a right to be and they observe evidence of a crime, they are authorized to seize the evidence and apprehend the offender. For example, an individual makes a complaint that requires the MPs to interview him and he invites the MPs into his house to conduct the interview. While in the house, the MPs observe a marijuana plant growing in the living room. The MPs have full authority to seize the marijuana and apprehend the individual.
- **Inventories.** Periodically, commanders are required to conduct inventories of material, gear, clothing, equipment, and so on. If they uncover evidence of a crime while conducting an inventory, they have full authority to seize the evidence and charge the offender. Inventories are required for the personal property of personnel who go absent without leave (AWOL). If a vehicle is towed to the MP impound lot as a result of breaking down and the owner has failed to remove the vehicle from the roadway in the requisite amount of time, the MP will inventory

the vehicle and its contents to safeguard the owner's property and to preclude false claims against the government. If contraband is found during the inventory, it will be seized and the owner will be charged. Inventories for towed vehicles should be done pursuant to a standing operating procedure (SOP) that standardizes how and when they are to be conducted.

- **Abandoned property.** Property, that based on objective facts is found unattended, is presumed to be abandoned. There is no expectation of privacy in abandoned property. This property can be freely searched, and any contraband found can be seized.
- **Exigent circumstances.** There are times when circumstances dictate that action has to be immediately taken to recover contraband, seize a person who has committed a crime, or respond to emergencies. These circumstances are called exigencies, which allow MPs to act if they have probable cause. Failure to act in these situations can result in serious consequences to the military community. Exigent circumstances include the following:
 - **Hot pursuit.** There is no concept known as sanctuary when the police are in pursuit of a suspect. When MPs have probable cause to apprehend a suspect and the suspect runs into a house or a structure, regardless of who owns or occupies the structure, the police can go into the house after the suspect. This penetration of a reasonable expectation of privacy by the MPs to take the person into custody who is attempting to elude the MPs is a reasonable exercise of government authority.
 - **Destruction of evidence.** If MPs have probable cause to believe that evidence is being destroyed, they may penetrate an expectation of privacy to confiscate the

evidence. Failure to act will allow the evidence to be destroyed.

- **Emergencies.** When an emergency arises, MPs have full authority to penetrate an expectation of privacy to handle that emergency. Examples include fires, crimes being committed, and responding to domestic disturbances in households. Protecting life, rendering medical aid, and stopping ongoing crime involving a threat to life are all valid situations that allow MPs to act because they have probable cause to believe an exigency exists.
- **Vehicle searches.** MPs who have probable cause to believe that contraband is located in a mobile vehicle have full authority to search the vehicle for the contraband. The scope of the search is based on the probable cause (you cannot look for an elephant in a matchbox). Failure to act can result in the vehicle with the contraband being driven away.

3-12. Due to the nuances of probable cause and to ensure that search authorizations meet all the requirements of the law, it is highly recommended that military magistrates be used to grant search authorizations. Military magistrates are attorneys specifically selected to act under the guidance of a military judge when granting search authorizations. Every installation has 24-hour on-call military magistrates.

STOPS AND FRISKS

3-13. MPs have authority to stop personnel on the installation anytime they have a reasonable suspicion, based on articulated facts, to believe that criminal activity is afoot. The person being detained is not free to leave until the MPs have either negated or verified their suspicion. This is not an apprehension or detention—it is an investigative tool allowing the MPs to ascertain if

the facts they are aware of involve a crime; they are trying to ascertain if a crime is being committed, nothing more.

3-14. If no crime has been committed, based upon the investigation at the scene, the person is free to leave. If the MPs have a separate reasonable suspicion to believe that the person stopped poses a danger to them (based on articulated facts) they may cuff and frisk the person (and their immediate possessions) for weapons. A frisk is not a search—it is a pat down of outer clothing for weapons only. For example, a woman who meets these criteria will be frisked and her purse will be gently squeezed for weapons. If the stop involves an automobile, the MP can frisk the car (look inside for weapons—this does not mean a search). If the MPs negate their suspicion of criminal activity, the person is free to leave. The frisk of the person/purse/vehicle is reasonable action based on the suspicion (supported by articulated facts) by the MPs that the person poses a threat. If during the frisk contraband is found, the person will be apprehended or detained and then searched pursuant to the apprehension or detention.

NOTE: Exercise caution when conducting searches and seizures because if a search warrant or search authorization was required and not obtained, any evidence found, as well as evidence derived there from, could be inadmissible in trial (*MRE 311, Exclusionary Rule, “Fruit of the Poisonous Tree Doctrine”*).

MILITARY LAW ENFORCEMENT AUTHORITY ON INSTALLATIONS

3-15. Installation commanders are inherently responsible for the maintenance of law, order, and discipline on their installation. This includes the authority to conduct investigations of offenses and other incidents. This responsibility also extends to civilians on the installation who threaten or impede the normal functioning of the command by conduct that is criminal or is prohibited by regulation. Violations of regulations

or statutes can result in a civilian's removal from the installation (bar letter), citation to a US magistrate court, or temporary restraint by military LE pending transfer to appropriate civilian authority (*DODD 5200.8*).

ARMY LAW ENFORCEMENT AUTHORITY OVER MILITARY PERSONNEL

3-16. Jurisdiction over personnel generally follows the limitations of the jurisdiction of the installation. The installation commander's authority extends to military LE personnel to maintain law and order on the installation. Army LE personnel are authorized and directed to apprehend military members who commit offenses punishable under the *Uniform Code of Military Justice (UCMJ) (Chapter 47, Part II, Subtitle A, Title 10, USC)* pursuant to *AR 600-20*. They may apprehend military personnel for all offenses under the *UCMJ*, military regulations, federal laws and regulations, and state laws, where applicable. Sources that provide apprehension authority are—

- *Rules for Courts-Martial (RCM) 302.*
- *AR 190-30.*
- *AR 195-2.*
- *UCMJ, Article 7.*

3-17. *Article 7, UCMJ*, apprehension authority applies worldwide. Additional sources that describe LE personnel jurisdiction and authority over military personnel are *AR 190-14*, *AR 195-1*, and *Criminal Investigation Division (CID) Regulation 195-1*.

OTHER LAW ENFORCEMENT PERSONNEL'S AUTHORITY

3-18. Authority for federal civilian employees assigned to security, police, and guard duties is derived from *AR 190-56*. Federally employed civilian police, security guards, and contract guards can perform LE and security duties authorized by the installation commanding officer and are subject to any limitations imposed thereon. These personnel can have no more authority than the commander possesses. The

commander is the source of jurisdiction and authority for all other personnel assigned to security force duties.

3-19. These personnel may apprehend persons on the installation for felonies, breaches of peace, or threatening property or welfare (*AR 190-56*). This apprehension authority is limited to issuing citations and turning the subject over to the appropriate civilian or military authorities. The provost marshal (PM), in cooperation with SJA, will issue written instructions for Army civilian police and security guards that describe procedures and the limits of their authority. These instructions will include the limitations for detention, apprehension, and the use of force. Additionally, instructions for the reaction force and hostage situations will be included (*AR 190-56*).

USE OF FORCE

3-20. *DODD 5210.56* and *AR 190-14* establish the use of force and the minimum qualification requirements for Army LE personnel. *AR 190-14* also—

- Prohibits the carrying of non-government-owned or -issued weapons and ammunition.
- Controls the carrying of these weapons.
- Prohibits carrying a firearm when taking medication that would impair one's judgment.
- Prohibits consuming alcohol within 8 hours of carrying a firearm.
- Sets the standards for the use of force.

3-21. Any person who is to carry a weapon must have written authorization before having the weapon issued. In order for military LE or security personnel to obtain this authorization, and any subsequent renewals, they must receive instruction for the use of force for the particular duties in which they will be employed. Additionally, the regulation requires that military LE personnel must demonstrate knowledge and skill in the use of unarmed defense techniques, the MP club, chemical-aerosol irritant projectors when issued and carried on duty, and their assigned firearms.

Furthermore, they must be qualified and trained on the use of all firearms authorized for carrying. This mandatory training and proficiency training must include a thorough briefing on individual responsibilities; use of deadly force training; and instruction on safety functions, capabilities, limitations, and maintenance procedures for the respective firearm. Military LE personnel must qualify annually on the MP firearms qualification course (*AR 190-14*).

3-22. Military LE will avoid the use of force when they can carry out their duties without resorting to its use. In circumstances where force is warranted, only the minimum amount of force necessary to reach the objective will be used. *DODD 5210.56*, *AR 190-14*, and *MRE 302(d)(3)* provide that when making an apprehension, military LE personnel can use such force and means reasonably necessary under the circumstances to affect the apprehension.

NOTE: When evaluating the degree of force required, regulation requires the following options be considered in the order listed:

- 1. Verbal persuasion.**
- 2. Unarmed defense techniques.**
- 3. Chemical-aerosol irritant projectors.**
- 4. MP club.**
- 5. MWD.**
- 6. Presentation of deadly force capability.**

3-23. Deadly force is only justified under conditions of extreme necessity and as a last resort when all lesser means have either failed or cannot reasonably be used. Circumstances when deadly force is justified include the following:

- **(1) Self-defense and defense of others.**
Deadly force may be used upon reasonable belief that it appears necessary to protect military LE

or other personnel in imminent danger of death or serious bodily harm.

- **(2) Asset involving national security.** Deadly force may be used when it reasonably appears necessary to protect assets vital to national security, such as nuclear weapons or sensitive codes.
- **(3) Assets not involving national security, but inherently dangerous to others.** Deadly force may be used when it reasonably appears necessary to prevent the theft or sabotage of resources (for example, weapons, ammunition, or chemical agents) that are inherently dangerous to others and would present a substantial potential of death or serious bodily harm.
- **(4) Serious offense against persons.** Deadly force may be used upon reasonable belief that it appears necessary to prevent the commission of a serious offense involving violence and threatening death or serious bodily harm such as murder, armed robbery, or aggravated assault.
- **(5) Apprehension or detention.** Deadly force may be used upon reasonable belief that it appears necessary to arrest, apprehend, and prevent the escape of a person who there is probable cause to believe committed an offense in bullet numbers 2, 3, and 4 above.
- **(6) Escape.** Deadly force may be used upon reasonable belief that it appears necessary to prevent the escape of a prisoner if there is probable cause to believe that the escaping prisoner poses a threat of serious bodily harm to military LE personnel or others. An unarmed fleeing felon who does not pose this threat cannot be subjected to the use of deadly force.

3-24. Additional requirements for the use of firearms in deadly force situations include the following:

- Give an order to halt before firing; warning shots are prohibited.
- Shoot with the intent to render the person incapable of continuing the activity.
- Fire shots with due regard to the safety of innocent bystanders.

NOTE: Do not unholster a weapon unless there is a reasonable expectation that its use will be necessary.

Appendix C further discusses RUF for US-based military personnel performing security duties.

Chapter 4

Force Protection Conditions and Security Measures

Military doctrine has established five FPCONs that correlate with identified threat levels. *AR 525-13* has established security measures that are implemented with each of the FPCON levels. FPCON levels are implemented at the direction of higher HQ or at the discretion of the command based on the threat assessment for that area. At the lower levels, the commander can implement measures from any of the higher levels. This is especially true when implementing the RAMP.

FORCE PROTECTION CONDITIONS

4-1. The five FPCON levels that military installations respond to are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. The conditions characteristic to each level are described below, along with what numerical security measures, as outlined in *AR 525-13*, must be conducted at that designated level. In order for access controllers to know the threat level of the nation in contrast to the threat level of the installation at any given time, a depiction of the Homeland Security Advisory System is provided on the inside cover of this handbook.

4-2. Installation commanders determine the implementing guidance that will accompany each security measure outlined in *AR 525-13*. A description of the measures prescribed by *AR 525-13* for FPCON NORMAL through DELTA are provided in *Appendix D*.

NORMAL

4-3. FPCON NORMAL applies when there is no credible threat of terrorist activity and units are conducting routine security operations in concert with the installation PS plan.

ALPHA

4-4. FPCON ALPHA applies when there is a general threat of possible terrorist activity against installations, facilities, or personnel and the nature and extent of which are unpredictable. FPCON ALPHA assumes security measures 1–10. ALPHA measures must be capable of being sustained indefinitely, with limited impact on normal operations.

BRAVO

4-5. FPCON BRAVO applies when an increased and more predictable threat exists. FPCON BRAVO encompasses security measures 11–29, in addition to the measures of FPCON ALPHA. FPCON BRAVO measures must be capable of being maintained for weeks, without causing undue hardship, substantially affecting operational capabilities, or aggravating relations with local authorities and members of the local civilian community.

CHARLIE

4-6. FPCON CHARLIE applies when an incident occurs or intelligence is received indicating that some form of terrorist action against facilities or personnel is likely. In addition to measures from FPCON NORMAL, ALPHA, and BRAVO, measures 30–40 will be implemented. Implementation of CHARLIE measures for more than a short period probably will create hardship and affect the peacetime activities of the unit and its personnel.

DELTA

4-7. FPCON DELTA applies in the immediate area where a terrorist attack has occurred or intelligence has been received that terrorist action against a specific location or person is imminent. FPCON DELTA is normally issued as a localized warning and requires implementation of mandatory security measures 41–51. All measures from FPCON NORMAL, ALPHA, BRAVO, and CHARLIE are continued or introduced if not previously implemented. Implementation of FPCON DELTA cannot be sustained for extended periods without causing significant hardships for personnel and affect the peacetime activities of units and personnel.

RANDOM ANTITERRORISM MEASURES PROGRAM

4-8. RAMP is a security program that involves implementing multiple security measures in a random fashion to change the appearance of an installation or activity security program. Units employ RAMP techniques as part of their FP program year-round. They are required to use the techniques of RAMP at least annually as part of their antiterrorism program. RAMP initiatives at the installation level are normally controlled by the installation antiterrorism officer (ATO) and are documented and maintained on file for review.

Chapter 5

Installation Security and Response Force Capabilities

The installation commander has the capability to respond to major threats to the installation with various security and response forces. If an installation ACP is compromised and a major incident would threaten the safety and security of the installation, a response must be swift and decisive. The nature and types of security threats to military installations vary widely from one installation to another. These variables include the geographic location of the installation, the criticality of the assets, the vulnerability of the installation and its assets, and the level of hostile intent. The key is to plan around reasonable threat scenarios and deploy security and response forces to eliminate the threat. Identifying critical vulnerabilities to a major threat provides focus for applying installation resources and response forces to reduce those vulnerabilities. The installation commander determines the critical functions or mission essential vulnerable areas (MEVAs) that support his ability to accomplish the assigned installation mission and then plans to protect them. MEVAs to consider include—

- Power generation nodes.
- Command and control (C2) facilities.
- Water points.
- Troop billets.
- Aerial ports of embarkation (APOEs) and seaports of embarkation (SPOEs) and/or debarkation.

PROVOST MARSHAL

5-1. Many of the forces available for security and response operations work directly for the installation PM. The PM plans and manages LE and access control (which includes a visible deterrent to threats), the initial response to security-related incidents, and the investigation of critical incidents. Through active police intelligence operations (PIO), the PM provides the installation commander with situational awareness and addresses information gaps to ensure that installation threat assessments are both valid and reliable. Refer to *FM 3-19.1* for information on PIO.

5-2. The *Installation Commanders' Blueprint, Installation Preparedness for Weapons of Mass Destruction* suggests that the installation commander may assign specific intelligence responsibilities to the PM or designate the PM as the focal point for installation intelligence collection and dissemination. In this role, some of the key duties may include—

- Leading the installation intelligence fusion cell.
- Serving as liaison with local, state, federal, or host nation (HN) LE agencies (*AR 381-10*).
- Preparing the installation threat assessment.
- Assisting with preparing the intelligence portion of the installation FP or other response plans.
- Providing the installation commander with the operational impacts of changing intelligence situations.

5-3. A key function of the PM is the formal liaison between installation LE and the many federal, state, and local police and security agencies operating within the installation commander's area of operations (AO), influence, and interest. Frequent information sharing within the intelligence fusion cell solidifies these critical partnerships that, in turn, greatly enhance intelligence capabilities.

TIERED RESPONSE CAPABILITIES

5-4. Response operations to major threats on military installations are tiered. Response operations consist of—

- Emergency responders.
- Special reaction teams (SRTs).
- Augmentation guard forces.
- Chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) installation support teams (ISTs).
- A Quick-reaction force (QRF).

5-5. Many of these forces provide basic capabilities for the day-to-day security of the installation, regardless of FPCON levels. However, as described earlier in this handbook, the majority of these forces are MP from modification table of organization and equipment (MTOE) units and are susceptible to deployments.

5-6. Installation commanders should establish memorandums of understanding (MOUs) and memorandums of agreement (MOAs) with local and state civilian agencies to ensure that those emergency responders will respond to major threats. It is important to integrate these arrangements into the overall security plan for an installation and during fort-to-port operations. Additionally, it is imperative that the local commander has a realistic assessment of the training and reliability of the off-post support.

EMERGENCY RESPONDERS

5-7. Emergency responders provide basic support to installations on a day-to-day basis, regardless of FPCON levels. Many of these forces are available 24/7. Some installations have most of the required emergency responders on their installation under the commander's control. More often, however, the installation commander must look elsewhere for assistance. There are various options for filling the need for a given capability. The commander can work with the local

community or other nearby military installations for assistance and, within certain legal parameters, implement an MOU or MOA.

5-8. Connectivity with the local community also facilitates interoperability with state and regional federal incident response agencies and organizations. In a similar manner, working through foreign-liaison elements, outside continental US (OCONUS) commanders can coordinate for HN providers. As a part of the commander's long-range strategy, he may only need to fill a gap in response capability until the installation receives the requisite resources to fill the need without outside help. The key is that once a required need has been identified, it must be accounted for in some manner.

5-9. Emergency responders on most Army installations include—

- MPs.
- DA civilian police or guards.
- Fire department and/or hazardous material (HAZMAT) personnel.
- MWD teams.
- Emergency medical services (EMS) personnel.
- EOD personnel.
- CBRNE-IST.

5-10. Normally, these forces are integrated through the installation 911-operator system and are, in fact, the first layer of security for the installation. Increases in MP patrols provide the most seamless increase in security posture on an installation, because the additional capabilities are integrated directly into its day-to-day operations.

5-11. In recent years, there has been an increase in the numbers of civilian personnel performing LE and security duties on Army installations. This trend is expected to continue. The PM is responsible for training these forces and integrating their efforts into the

installation LE and security plan. *Training Circular (TC) 19-138* is the official guide for training DA civilian police and guard personnel. The installation commander is the source of jurisdiction and authority for all LE personnel assigned to the installation.

SELF-PROTECTION MEASURES

5-12. Terrorists have a history of using secondary devices to target emergency responders. Response plans should include contingencies designed to counter these measures and protect responders.

5-13. MPs should use the time/distance/shielding concept to protect themselves from hazards that WMD and other threats may pose. All forms of protection can be defined in terms of time, distance, and shielding. Responders should use all three forms of protection to maximize their safety.

- **Time.** Limit exposure time in the hazard area. Use rapid entries to conduct reconnaissance of the crime scene or rescue victims. The less time responders spend in the affected area, the less likely they are to get injured. Minimizing the amount of time spent in the affected area will also reduce the chances of disturbing the crime scene.
- **Distance.** Stay upwind of the hazard, and maximize the distance between you and the affected area. Emergency responders should be familiar with and follow the guidance described in the *2000 Emergency Response Guidebook (ERG2000)*, developed jointly by the US DOT, Transport Canada, and the Secretariat of Communications and Transportation of Mexico. Refer to <http://hazmat.dot.gov/guidebook.htm> for additional information.
- **Shielding.** Shielding requirements vary depending on the hazard. Use what is available, to include vehicles, buildings, and protective clothing.

COMMUNICATIONS INTEROPERABILITY

5-14. The possibility of damage to a central communications node requires redundant communications systems for both installations and local community responders. Communications systems interoperability between the installation responders and local, state, federal, and HN response assets is critical.

EXPLOSIVE DETECTOR DOG SEARCHES

5-15. One of the most accurate methods used to locate and identify explosive devices at ACPs is an explosive detector dog (EDD) team. Specific EDD search procedures vary according to local policy, individual MWD handler preference, and the unique abilities of individual canines. However, the typical approach follows these five general steps:

Step 1. The driver exits the vehicle and opens all doors, the hood, the trunk, any other compartments, and any packages. The driver is placed in a holding area where he is not allowed to witness the vehicle search.

Step 2. The EDD team (the handler and the dog) proceeds directly to the downwind side of the vehicle.

Step 3. The EDD team starts the search at a specific point and searches in a counterclockwise direction, with the handler visually guiding the EDD to search for scents along the fenders, wheel wells, hubcaps, spare tire, and bumpers.

Step 4. The dog is directed to search all opened compartments, vehicle seats, and floorboards.

Step 5. The dog is directed to search any onboard packages and parcels.

SPECIAL REACTION TEAM

5-16. The installation commander's most lethal full-time response force is the SRT. An SRT is an integral part of FP and is the principal response force in case of a major disruption or a special threat situation.

Installation commanders are required to maintain an SRT capability. Commanders may resource the SRT through a full-time team or an MOA with a nearby base or civilian police agency.

5-17. *AR 190-58* and *FM 3-19.11* (restricted manual) provide guidance for SRTs. *Figure 5-1* illustrates the recommended composition of an SRT. SRTs are highly trained, readily available (regardless of FPCON level), and used for precision operations.

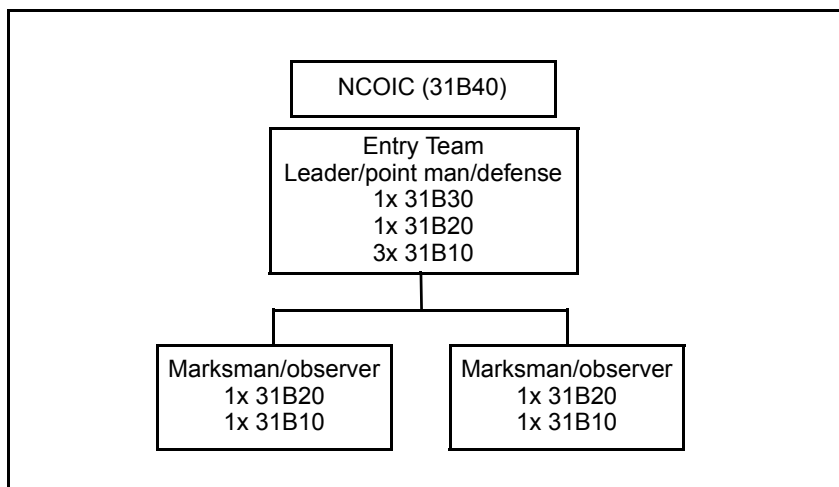


Figure 5-1. Special Reaction Team Organization

5-18. An SRT is manned, trained, and equipped to perform missions that include—

- Precision, high-risk entry for barricaded persons.
- Apprehension of dangerous suspects.
- Countersniper operations.
- Precision marksmanship.

AUGMENTATION GUARD FORCE

5-19. Augmentation guard forces may be necessary to support increased FPCON security requirements.

Manpower sourcing of augmentation guard forces normally comes from existing manpower on the installation. When adequate forces are not available, an alternative is active Army forces from other installations. A final source is a mobilized reserve component force. These forces will normally conduct local/point security type missions to secure MEVAs and high-risk targets (HRTs) and to augment ACP manpower requirements. The PM plans for the certification of these forces to ensure smooth integration into the overall security effort. These forces must train to standard, to include, but not limited to, the following:

- Weapons qualification and clearing procedures.
- Access control procedures.
- Interpersonal communication (IPC) skills.
- Customs and courtesies.
- Vehicle inspections.
- Emergency and security equipment operations.
- Self-protection techniques.
- Use of force.
- Sentry duties.
- Communications procedures.
- Legal and jurisdictional issues.

CHEMICAL, BIOLOGICAL, RADIOLOGICAL, NUCLEAR, AND HIGH-YIELD EXPLOSIVE INSTALLATION SUPPORT TEAM

5-20. The CBRNE-IST is a matrixed organization that is composed of assigned, tenant, and local agency assets. The CBRNE-IST provides an installation commander with organic CBRNE capabilities as discussed below.

MANNING

5-21. *Figure 5-2* depicts the recommended composition of a CBRNE-IST. Installation commanders may need to tailor this organization based on available resources.

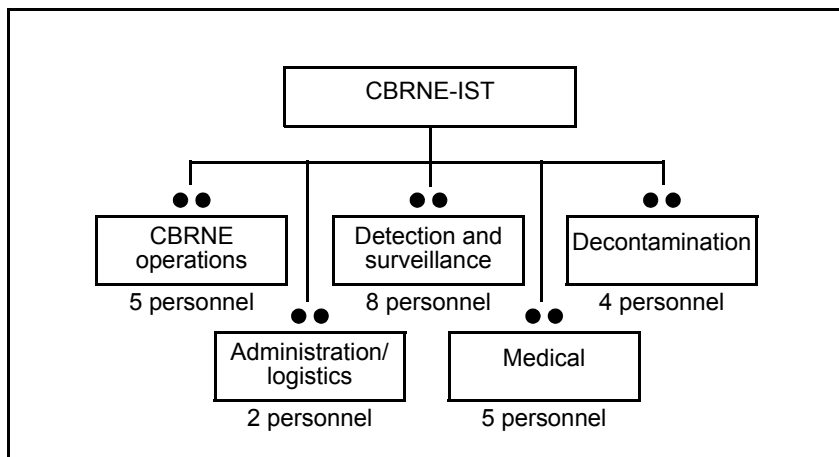


Figure 5-2. Organization of a Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Installation Support Team

MISSIONS

5-22. The CBRNE-IST is manned, trained, and equipped to perform the following missions:

- Conduct early warning of hazards by using standoff and/or network point sensors.
- Detect CBRNE hazards.
- Perform identification of CBRNE hazards.
- Locate and mark CBRNE hazards.
- Communicate directly with the installation commander, the incident commander, and the information operations center (IOC) via secure voice communications.
- Calculate hazard predictions.
- Perform triage and emergency medical procedures.
- Coordinate the evacuation of casualties.
- Coordinate administrative and logistical support.
- Coordinate security support.
- Conduct limited decontamination.

CONCEPTS

5-23. The following specifications guide the employment of the CBRNE-IST:

- Is activated by the installation commander once indications are received that a CBRNE attack may occur or once emergency responders suspect or determine that a CBRNE incident has occurred.
- Is organized as an element of the installation response capability.
- Is tailored from on-call assets.
- Integrates CBRNE-IST, CBRNE-rapid response team (RRT), special medical-augmentation response team (SMART), the Chemical Corps, and other government assets.
- Reports directly to the installation commander if activated prior to an incident. Once an incident occurs, reports directly to the incident commander.
- Trains and exercises continuously to ensure success.
- Requires support from the installation medical-treatment facility (MTF), directorate of logistics, directorate of public works, and community support agencies.
- Sustains operations for no more than 24 hours after an incident without augmentation.
- Provides support to civil authorities, provided the CBRNE-IST remains within supporting distance of the parent installation.
- Is reinforced by CBRNE-RRT.
- Activates the reconnaissance and surveillance section before an incident at named areas of interest as part of a collection plan.

- Performs the following tasks once a hazard is detected:
 - Alert and recall (assuming CBRNE-IST is not already assembled).
 - Brief IOC mission.
 - Deploy to the incident site.
 - Detect and identify the CBRNE hazard, if not already identified.
 - Assess, decontaminate, treat, and facilitate casualty evacuations.
 - Provide a hazard predication warning to the IOC.
 - Determine the physical boundaries of the hazard, and mark the area.
 - Establish the initial decontamination operation—
 - Establish initial hot line procedures.
 - Decontaminate.
 - Coordinate additional decontamination capability.
 - Provide first aid.
 - Continue the surveillance of the hazard.
 - Conduct a hand-off, as required.
 - Advise the installation commander.

TRAINING

- 5-24. CBRNE-IST training is based on the following:
- Appropriate individual certification for current duty position.
 - Hands-on equipment training.
 - Training via US Army Chemical School (USACMLS) mobile training teams and the Fort Leonard Wood CBRNE resident and distance learning (DL) courses (the DL course is under development).

5-25. Medical section members attend the following courses:

- Basic life support.
- Advanced trauma life support.
- Advanced cardiac life support.
- Medical management of chemical and biological casualties.

QUICK-REACTION FORCE

5-26. A QRF is an uncommitted, battle-rostered organization. The QRF provides an installation the ability to employ a sizeable force, capitalizing on shock and speed as a show of force under the principles of war, to neutralize the threat and restore installation security.

5-27. The QRF is characterized by—

- Modularity for expansion to support small, medium, and large installation requirements.
- Familiarization with C2.
- Individual and collective task training.

5-28. The QRF is the commander's force in reserve. The size of the QRF is based on mission, enemy, terrain, troops, time available, and civilian considerations (METT-TC) and is, ideally, a platoon-size element. *Figure 5-3* illustrates the minimum composition of the QRF. The QRF must be located at a central location on the installation that provides security to the force and enables quick response to an incident.

5-29. The QRF supports the installation security plan, and missions are assigned according to the installation commander's intent and guidance. Once the QRF is activated, it is under the operational control (OPCON) of the installation commander. This responsibility may be delegated to the PM, since the PM is normally the incident commander of most life-threatening incidents.

5-30. The installation security plan should have trigger mechanisms to activate the QRF. These trigger

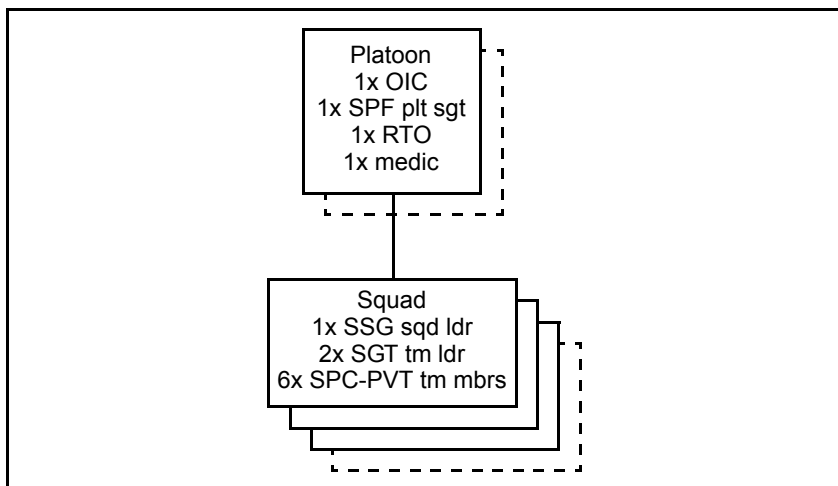


Figure 5-3. Organization of a Quick-Reaction Force

mechanisms should parallel the threat and QRF readiness level. Special consideration is given to the QRF to ensure that it remains a force that is in reserve, responding only to incidents that cannot be contained or eliminated by the security forces currently in place. Once deployed, it is extremely difficult to disengage the QRF from a threat in order to respond to another threat of a greater magnitude.

5-31. The QRF provides the ability to generate an otherwise uncommitted security force that reacts and responds to unforeseen threat circumstances, exceeding the capability of guards and augmentation forces. It must be focused on the quick generation of combat power. Its primary tasks include—

- Reacting to ACP breaches.
- Reinforcing MEVA augmentation forces.
- Establishing an outer perimeter at an incident site.
- Patrolling.

5-32. A primary trigger for employment of the QRF would include an incident that falls within the mission

set of the QRF and the need to reinforce other security responders or the incident has exceeded their capability. QRF recall status is FPCON based.

5-33. Every installation is different; therefore, equipment requirements may vary from one installation to the next. Contingent upon the type of threat, the QRF should possess both lethal and nonlethal capabilities.

TRAINING

5-34. The QRF must be trained and certified on individual and collective tasks. All leaders, from squad leader and above, must be tacticians. They must understand and use initiative in accomplishing the mission. This means that they must know how to analyze the situation quickly and make decisions rapidly in light of the commander's intent. They must be prepared to take independent action if necessary. The art of making sound decisions quickly lies in the knowledge of tactics, the estimate process, techniques, and procedures. The skills required of leaders include physical toughness, technical knowledge, mental agility, and a firm grasp of how to motivate soldiers to fight in the face of adversity.

5-35. The QRF must be trained to accomplish, at a minimum, the following collective tasks and battle drills. These tasks are not all-inclusive and must be tailored to meet the commander's intent and the installation mission requirements. They include—

- Conduct movement to contact.
- Conduct civil disturbance control operations.
- Conduct cordon and search.
- Clear built-up areas and buildings.
- Treat and/or evacuate casualties.

5-36. Training priorities and tasks are based on the types of threats outlined in the installation security plan. The QRF is trained according to *TSP 191-95B-004* (available from the USAMPS).

WEAPONS

5-37. The QRF weapons mix is based on the installation commander's intent, the mission, and the type of weapons available. The QRF should have a minimum of at least three squad automatic weapons and three shotguns. Each soldier should possess an M16A2 or M4 rifle. The QRF should have both lethal and nonlethal capability. Possible weapons include the following:

- M16A2 or M4 rifle (M203).
- M9 pistol.
- M12 or shotgun.
- M249 squad automatic weapon.
- Other weapons as determined by the installation SOP.

EQUIPMENT

5-38. Communications for the QRF should be accomplished using the following three nets:

- Emergency operations center (EOC).
- QRF.
- Internal element.

5-39. There should be at least one secure net. Communications equipment should include:

- Frequency-modulated (FM) radio, single-channel ground-to-air radio system (SINCGARS), or other means of secure communication.
- PRC-127 squad radio.
- Handheld radios.
- Batteries and chargers for all systems.
- OE-254 antenna(s).
- Cellular telephones and pagers.

VEHICLES

5-40. The QRF should have a tactical means of mobility 24/7. Armor vehicles provide the best protection for the QRF; other vehicles include—

- High-mobility multipurpose wheeled vehicle (HMMWV) (M998/M1025/M1026/M1114).
- Lightweight medium tactical vehicle (LMTV).
- M101A1 trailer.
- Other vehicles as determined by the installation SOP.

SPECIAL EQUIPMENT

5-41. Soldiers assigned to the QRF must be issued a Kevlar® helmet, body armor, and a protective mask. Other equipment includes the following:

- Night vision devices.
- Combat lifesaver bags.
- Bullhorn.
- Flexicuffs.
- Litters.
- Light sets.
- Generator.
- Tents.
- Civil disturbance and crowd control gear.
 - Body shields.
 - Riot batons.
 - Shin guards.
 - Face shields.
 - M36 riot dispensers.
 - O-chlorobenzylidene malononitrile (CS) and/or oleoresin capsicum (OC).
 - Barrier materials.
 - Nonlethal ammunitions.
 - Other items as determined by the installation SOP.

Chapter 6

Special Considerations for Entry Control Points

US military installations share many similarities, and each reflects its own unique character. Depending on the location of the installation and the utility of its mission, each will present diverse security and access control considerations akin to its infrastructure and the amount and type of activity that each support. On some installations, only military entities require access to or traverse the post, while others coshare water, railroad, and airfield commerce with nearby civilian communities. Some installations offer commanders unique challenges in that they coexist with water ports, airfields, and rail yards. These challenges require special access control or full security measures, and the establishment of ACPs would not be sufficient. While many installations do not operate pedestrian gates, some installations could not function without them. These gates often serve as ACPs and require special considerations. Another unique access control consideration is associated with the conduct of special events on an installation. These events pose special challenges and vulnerabilities.

WATER PORTS

6-1. The events of September 11, 2001, caused port officials to reevaluate the criminal concerns present at

ports. In fact, the Maritime Transportation Security Act of 2002, for the first time ever, mandated that all ports, facilities, and vessels have comprehensive security plans and incident response plans. Before that date, curtailing illegal immigration, drug trafficking, and thefts were the priority. Today, the prevention of international terrorist movement is at the forefront of port security operations. Installation commanders with ports inherent to their installation or military facility must develop innovative security measures to protect them from both criminal and terrorist threats.

6-2. Ports and harbors are prime targets for criminal, terrorist, and enemy activities. Perimeter areas of these facilities are more vulnerable because of the extensive distance and exposed beach or pier areas. Terminal areas may include fully developed piers and warehouses or may be unimproved beaches where logistics-over-the-shore (LOTS) or roll-on/roll-off (RO/RO) operations are conducted.

6-3. It is virtually impossible to establish ACPs at ports and harbors. It is more realistic to conduct full security operations at these locations, with the main effort focused on security from the perimeter of the port outward. Security measures focus on aggressive patrolling to detect, report, and, if need be, combat enemy threats. Measures may include—

- Conducting route and area reconnaissance patrols.
- Developing police intelligence in the AO.
- Controlling traffic in the area surrounding the port.
- Conducting mounted or dismounted patrols (with MWDs, if available) around the port perimeter.
- Establishing an access control/identification section.
- Watching for diversions of supplies out of the port.

- Providing a response force to react to incidents inside the port perimeter.
- Providing observation and early warning of threat ground and air attacks.

6-4. If a pier or other maritime environment is designated as a restricted area, access from the water and the land must be controlled. Entry on the landward side of a pier can be limited with fencing, pass control, and aggressive patrolling; but the part of the pier that protrudes over the water is accessible from the sides and from below. Methods for securing the pier along its water boundaries include—

- Patrols (both walking on the pier and in small boats).
- Protective lighting.
- Log booms.
- Nets.
- Buoys or floats.
- Anchored or pile-mounted navigational aids and signaling devices.
- Barges.

6-5. While most of the barriers described above will stop or impede access to facilities from boats or swimmers, nets are among the most effective. Well-marked, partially submerged objects are also effective; however, there may be legal prohibitions against placing barriers that may constitute a hazard to navigation. These barriers should be placed only after coordination with and approval by the appropriate legal authorities. Sometimes it is best to close off the waterside of a pier. A floating boom will keep small boats out. Suspending a cable or a chain-link net from the bottom of the boom will deny access underwater.

6-6. At least two security zones must be established on the waterside of a facility—the reaction zone and the keep-out (exclusion) zone. Security forces in these zones notify vessels, craft, and swimmers that they are

entering restricted waters and should alter their course. Security forces may stop and search intruders if necessary. Security zones should extend at least 1,000 meters from the nearest protected asset; however, in some port areas, this large of a security zone is not possible. In such cases, other measures (such as boat patrols) must be increased to mitigate the possibility of attack.

- The reaction zone extends from the high-water mark to a distance beyond the maximum range of anticipated waterborne threats. Security forces stop and challenge intruders inside the reaction zone.
- The keep-out zone is the zone closest to the protected assets. It extends from the asset to the maximum range of anticipated threat weapons. Security forces should prevent the entry of all unauthorized craft or vessels into this zone. The tactical response force (in this case, a boat) may be used. In addition to organic security, forces may be provided by contracted personnel.

6-7. In addition to these measures, installation commanders must ensure that personnel identification and internal security measures are implemented. Perimeter gates should be locked when not in use and guarded when open. Security tools (such as lighting, CCTV, communications, and X-ray equipment) must be integrated into security operations.

AIRFIELDS

6-8. Installation commanders rely on the perimeter ACPs for validating the authenticity of a person's identification on an installation. This validation process must overlap to an installation airfield. Protection of airfields by a dedicated ECP may not be possible or appropriate, but protection of aircraft and helicopters on the ground at airfields is vital. Dedicated security should be afforded to these craft. Landing strips and sites at installations must be checked and secured well in

advance of arrivals. Security must be maintained until departures have been completed.

6-9. Inspections of outgoing and incoming cargo, passengers, and passenger baggage will be made. If cargo is sealed, the seal will be checked and verified. The seal represents that the cargo has been inventoried and inspected. If a seal has been broken or tampered with, it must be immediately reported to the security commander.

RAIL YARDS

6-10. Installation commanders are responsible for securing railways within the installation boundary and securing off-post railway sections when they are used for military purposes. The latter is inherent in the commander's in-transit cargo responsibilities. Railways may be used to move military personnel and equipment during deployments and redeployments. In stability operations and support operations, it is conceivable that an adversary will make use of any railway service. Thus, it is critical to secure railcars at all times. During loading, stops, and off-loading, 360° security must be provided.

NOTE: Never divulge the embarkation or debarkation times or the load of a train except to those who have a need to know. Movement by rail is difficult to conceal and is manpower-intensive.

6-11. Installation commanders must consider the following vulnerabilities and capabilities when addressing rail security:

- Portal locations and accessibility by those with criminal intent.
- General accessibility to the rail by road.
- Electrical power availability to rails.
- Radio frequency (RF) communications accessibility.

6-12. Railcars that are incoming to an installation must be inspected. If a car is sealed and is not intended for that installation, the seal must be checked and verified. If the seal has been tampered with or broken, it must be reported to the train commander. Again, because the feasibility to dedicate an ECP at a rail yard is not likely, the installation commander will rely on the validation of identification at an ACP to support the authenticity of personnel on the ground at rail yards. Personnel, equipment, and baggage will be verified and inspected upon deployments and redeployments.

PEDESTRIAN GATES

6-13. Safety considerations at pedestrian gates must be afforded to both the controller and the pedestrian. The safety of the access controller and the safety and identification of the pedestrian must be priorities.

6-14. Many installation ACPs handle pedestrian traffic. Special considerations must be afforded to accommodate this traffic. They include—

- Providing a sidewalk and safety provisions to direct pedestrians to the appropriate location of the ACP, while separating them from vehicular traffic.
- Providing breaks in the passive barriers to allow pedestrians to access the ACP.
- Ensuring that entry controllers have direct visual access to the pedestrians.
- Incorporating ACP procedures at turnstiles, when present. Access controllers must validate identification and inspect packages, handbags, briefcases, and other items.

6-15. Pedestrian gates must be located so that access controllers have a complete view of them. A pedestrian should never have the opportunity to appear at an ACP without the controller being able to observe him from the onset. Access controllers for pedestrian gates should

have no other duties but that of the gate. The same security and comfort considerations provided to access controllers at vehicular ACPs (discussed in *Chapter 1*) must be provided to access controllers at pedestrian gates.

SPECIAL EVENTS

6-16. Special events on military installations often raise the overall installation threat level. Events demonstrating national pride, such as Independence Day and Armed Forces Day, all pose unique challenges. LE planners can expect large concentrations of people attending the events and a substantial increase in traffic flow and parking requirements. Additional LE, FP, and antiterrorism measures are necessary to counter additional vulnerabilities associated with large crowds on an installation. Local ACP plans should address these issues and the effects on the surrounding community.

Chapter 7

Systems Approach to Security

The Army Installation Security Program is designed to deter enemy and criminal elements from conducting hostile operations against Army resources and to reduce the theft of Army property. This program supports the goal of protecting soldiers and their family members, DA civilians and their family members, facilities, information, and materiel resources from terrorism under the DOD FP program. Further, the Army Installation Security Program is threat-based. Deliberate and crisis planning actions developed through the installation PS plan correspond with the level of protection required to provide adequately secured Army assets. These actions are based on the potential for damage, destruction, or compromise to these assets.

SUPPORT TO FORCE PROTECTION

7-1. An FP program synchronizes five elements—antiterrorism, PS, high-risk personnel (HRP) security, intelligence operations (IO), and LE. Of these five elements, PS in the operation of installation access control is of particular interest to installation commanders. While security, in itself, is the total spectrum of procedures, facilities, equipment, and personnel employed to provide a secure environment, PS is the physical and procedural measures designed to deter, detect, and defend personnel, property, equipment, facilities, information, and material against espionage, terrorism, sabotage, damage, misuse, theft,

and other criminal acts. It is the synergy of these measures that provides successful access control operations and reinforces FP objectives.

SYSTEMS APPROACH

7-2. The security of an installation consists of multiple layers and graduates incrementally, following a systems approach. The optimum consideration for securing Army assets is a systematic process—one that provides an integrated system. Mutually supporting elements that provide for an effective protective system integrate—

- Physical protective measures, including barriers, lighting, and electronic security systems. *Appendix E* includes advice on the use of barrier types and their respective mitigation.
- Procedural security measures, including those procedures in place before an incident and those employed in response to an incident. They also include procedures employed by the person responsible for the asset and the manager of the guard force.
- Measures to protect assets against terrorism.

7-3. This handbook directly addresses installation ACPs and how the above listed elements support effective access control procedures. Directly, these elements provide for the integration of access controllers, the assimilation of the security force, and the incorporation of technology. Indirectly, they are a force multiplier to the installation commander's FP program.

ACCESS CONTROLLERS

7-4. Access controllers provide the first physical line of defense to an installation. They determine the validity of a person's access to an installation and either allow or reject that person's access. They are assisted in this process through the special guard orders posted at the

ACP. The special guard orders should include execution instructions for such items as—

- Sign-in procedures.
- Access rosters.
- Emergency vehicles.
- The processing of authorized identification card holders.
- A contact roster for key personnel.
- Installation maps.
- Phone numbers for the key organizations of the installation being guarded.
- Random antiterrorism measures for FPCON.
- The use of force.
- Lists of personnel barred from the installation.

SECURITY FORCE

7-5. The security force provides security for an installation by forming concentric rings or sectors of security. The more protected or vulnerable an asset and the closer to it one gets, the smaller the ring or sector and the greater the security. Conversely, the less important the asset and the farther away from it one gets, the larger the ring or sector and the lesser the security force.

TECHNOLOGY

7-6. Technology is a means to vertically enhance security by different means. It collectively supports the safety and security of access controllers, all members of the installation, and military assets; communications through personnel and mass notification systems and various C2 systems; and protective measures through barriers, fixed and portable lighting systems, interior security systems (such as CCTV and electronic alarms), robotics, sniffers, detectors, X-ray capabilities, mirrors, and ballistic-protection devices.

7-7. The ability to harness technology and employ it in a meaningful fashion requires competent and savvy users. It is critical that access controllers receive training on the individual pieces of technology used in support of access control; they must understand the full scope of their duties as it relates to other activities or areas adjacent to interests influenced by their actions. This training must provide an understanding of how the integration of these pieces work cohesively to provide the best possible access control to an installation.

7-8. Technology is constantly evolving, and as such, requires continuous evaluation. Currently, the Access Control Working Group has decided on a PS package for installation access control. The package is specified as small, intermediate, or large and may have a minus or plus, depending upon the installation needs.

ONE-TEAM CONCEPT

7-9. The success of installation access control is predicated on the premise that the intelligence fusion cell, an FP committee, and other installation special staff are working as one team towards one goal. The intelligence fusion cell includes the following:

- The PM.
- CID.
- Counterintelligence.
- Military intelligence (MI).
- Representatives from local, state, and federal LE and intelligence agencies.

The FP committee can include the following:

- The senior FP specialist.
- The FP officer.
- The plans and training officer.
- A PS specialist.
- A CBRNE specialist.

Other installation special staff can include the following:

- Engineers.
- The ATO.
- The MI officer.

7-10. Each element has a designated area of responsibility to support the FP element of PS, which in turn strives to provide meticulous and flawless access control operations. While representing individual entities, these personnel meet often and disseminate information aggressively.

7-11. There may be a variation from installation to installation in the representation of those making decisions regarding the systems approach to security. Nevertheless, there must be a system or a process in place to discuss and arrive at answers concerning access control procedures, because ACPs affect more than just the procedures at the gate.

7-12. When security missions in support of FP are planned and executed, they afford cohesive access control operations. The intelligence fusion cell, the FP committee, and the installation special staff supports the following major security missions in support of FP:

- Intelligence assessment.
- C2.
- Access control.
- MEVA, HRT, and HRP security.
- The security of off-post personnel and materiel in coordination with LE agencies.
- Tiered response capabilities.
- In-transit security operations.
- SPOE and APOE security operations.
- Command information and community interfaces.

7-13. It is the culmination of the efforts by the installation commander, every command, every installation activity, and every soldier that generates a safe and secure environment for installation members and Army assets through access control operations.

Appendix A

Metric Conversion Chart

This appendix complies with current Army directives which state that the metric system will be incorporated into all new publications. *Table A-1* is a metric conversion chart.

Table A-1. Metric Conversion Chart

US Units	Multiplied By	Metric Units
Feet	0.30480	Meters
Inches	2.54000	Centimeters
Inches	0.02540	Meters
Inches	25.40010	Millimeters
Pounds	0.45360	Kilograms
Metric Units	Multiplied By	US Units
Centimeters	0.39370	Inches
Kilograms	2.20460	Pounds
Meters	3.28100	Feet
Meters	39.37000	Inches
Meters	1.09360	Yards
Millimeters	0.03937	Inches

Appendix B

Vehicle Inspection Hot Spots

This appendix shows vehicle inspection “hot spots” that access controllers may encounter on various vehicle types. A hot spot is an area on a vehicle where a device or contraband could be hidden. These areas require special attention during inspections (*Figures B-1 through B-19*, pages B-2 through B-10).

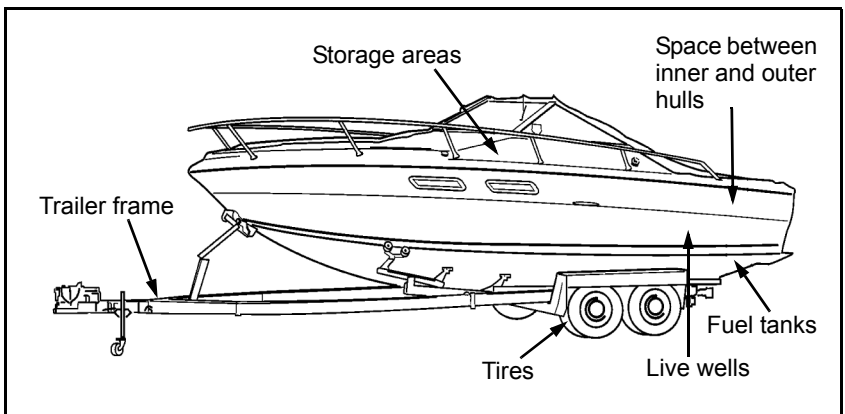


Figure B-1. Boat/Boat Trailer

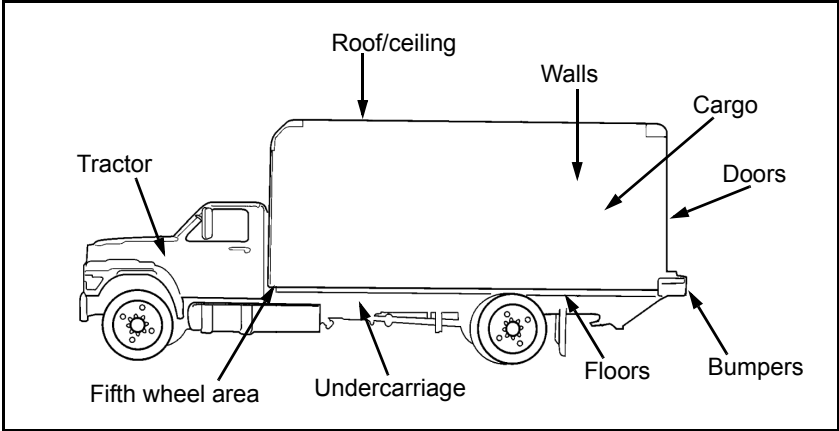


Figure B-2. Box Truck

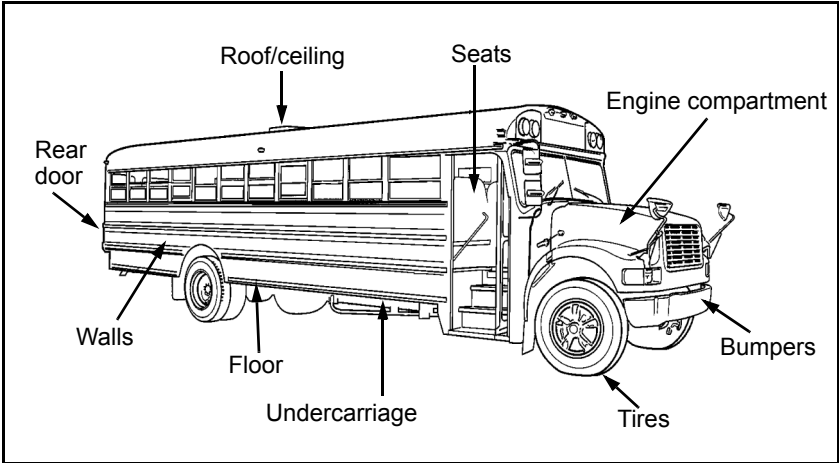


Figure B-3. Bus

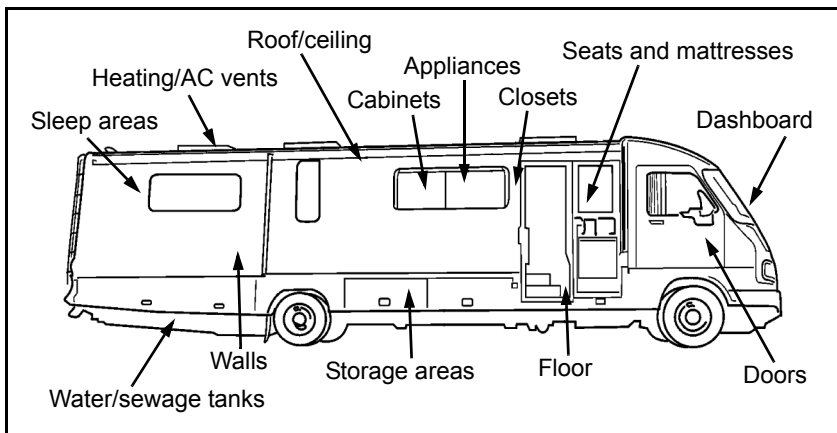


Figure B-4. Camper/Motor Home

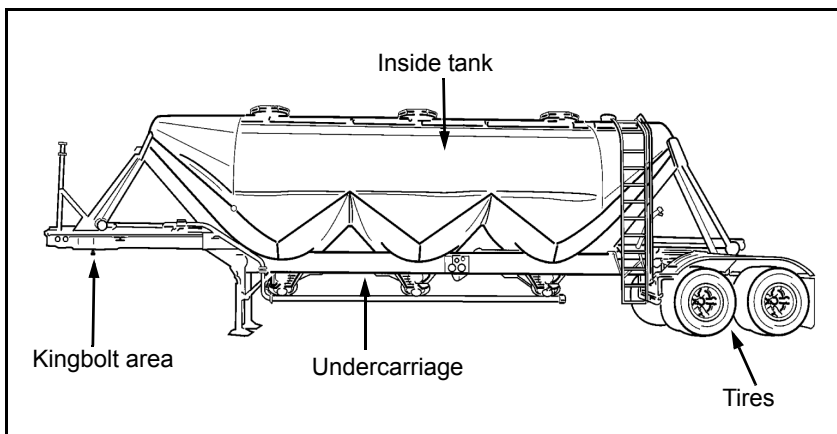


Figure B-5. Closed Hopper Vessel

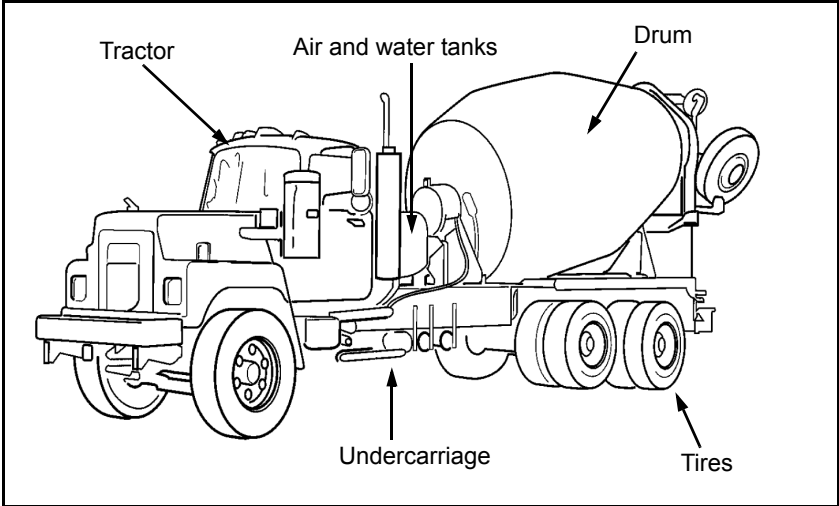


Figure B-6. Concrete Mixer

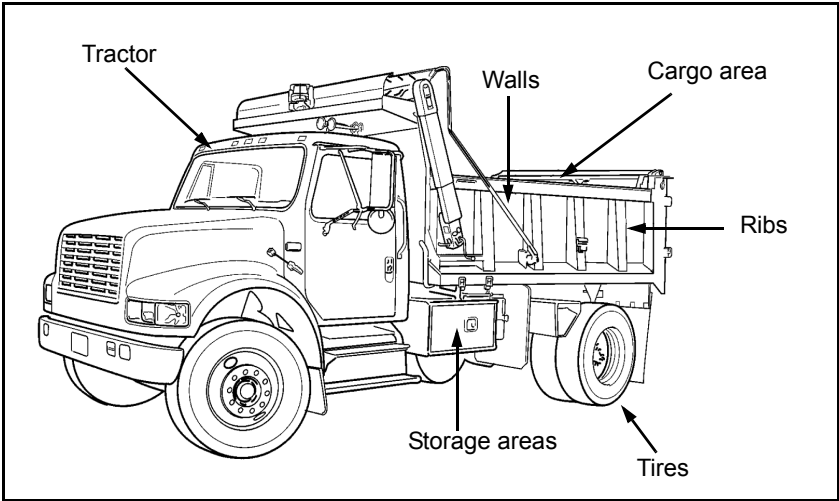


Figure B-7. Dump Truck

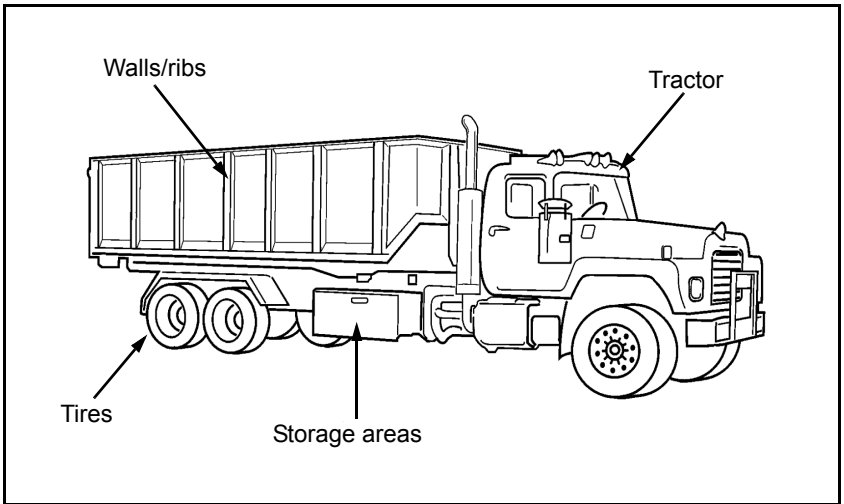


Figure B-8. Garbage Truck (Dumpster)

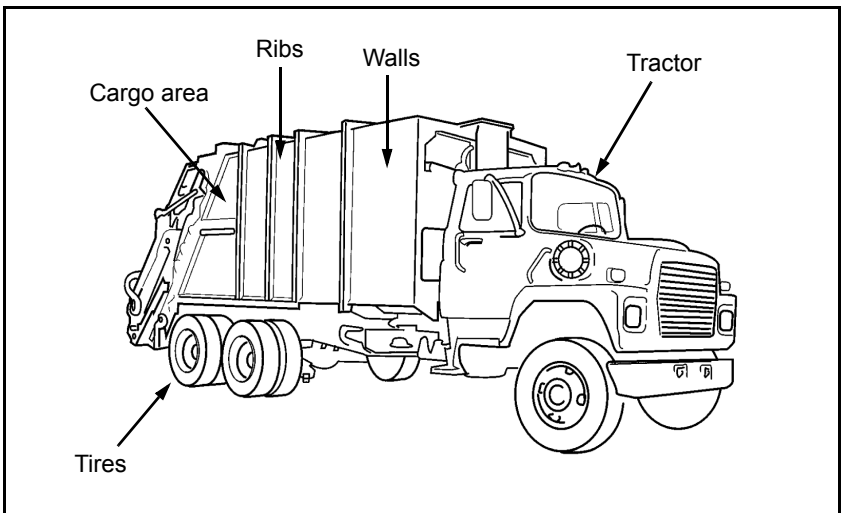


Figure B-9. Garbage Truck (Permanent Bed)

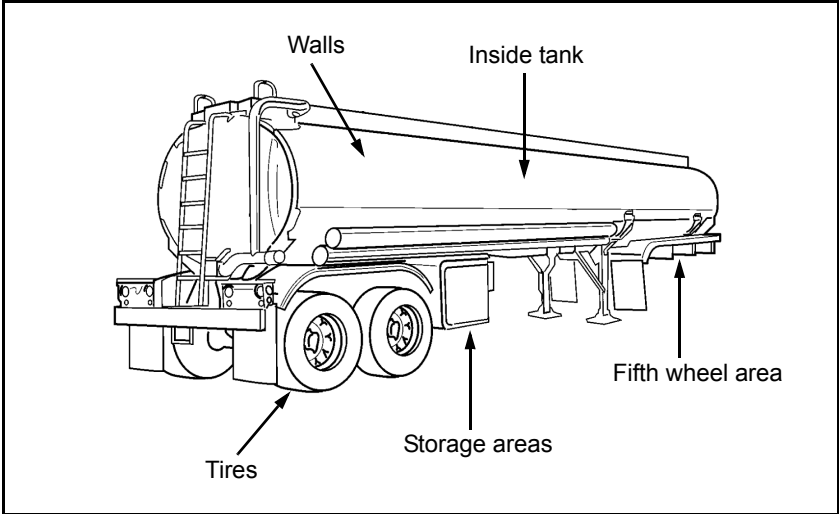


Figure B-10. Gasoline Trailer

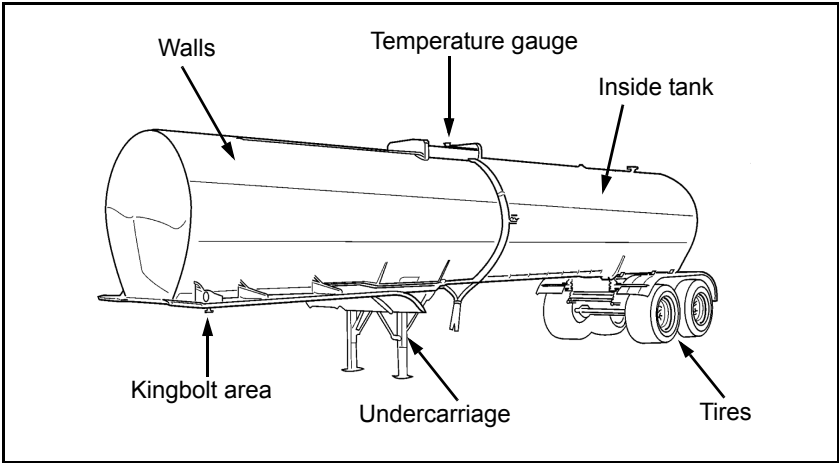


Figure B-11. Hot-Liquid Asphalt Tanker

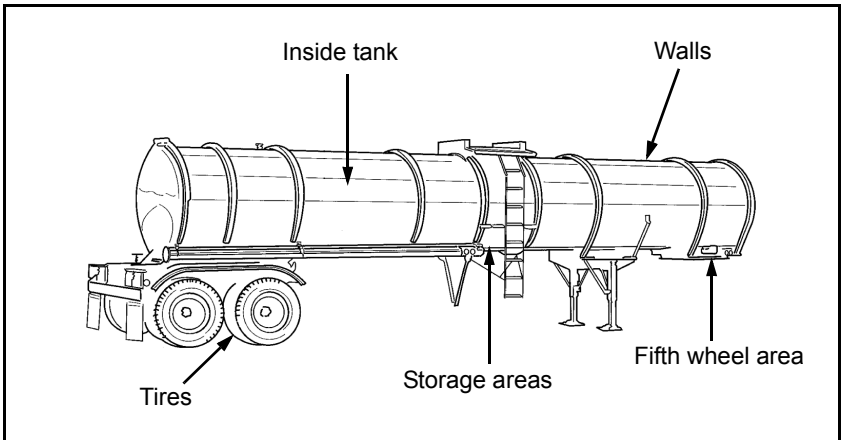


Figure B-12. Liquid Tanker

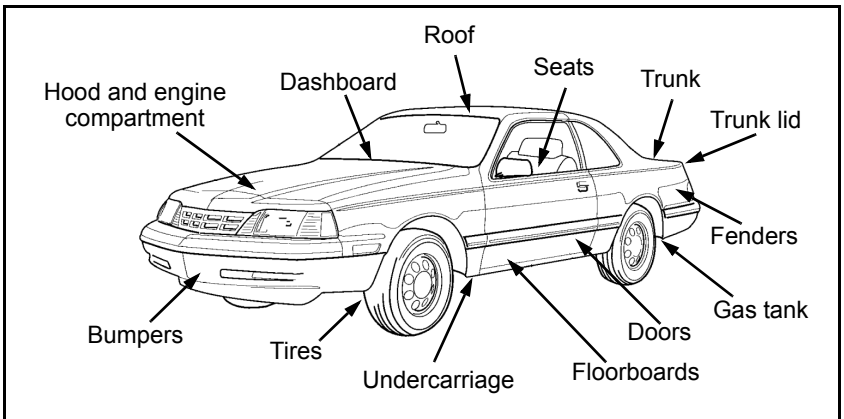


Figure B-13. Passenger Vehicle

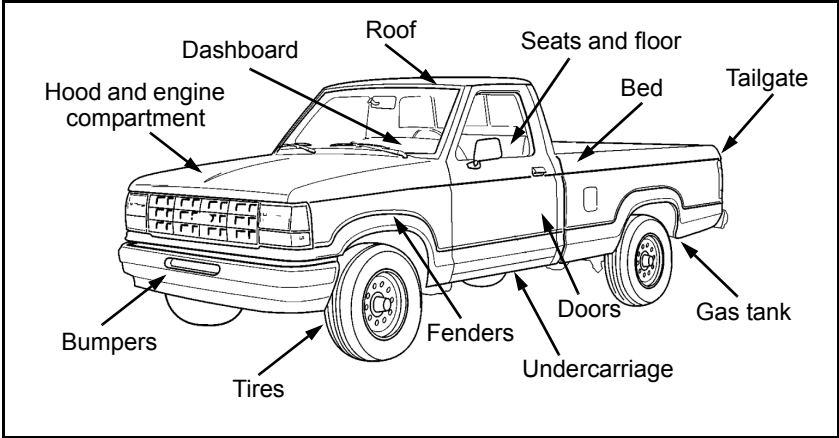


Figure B-14. Pickup

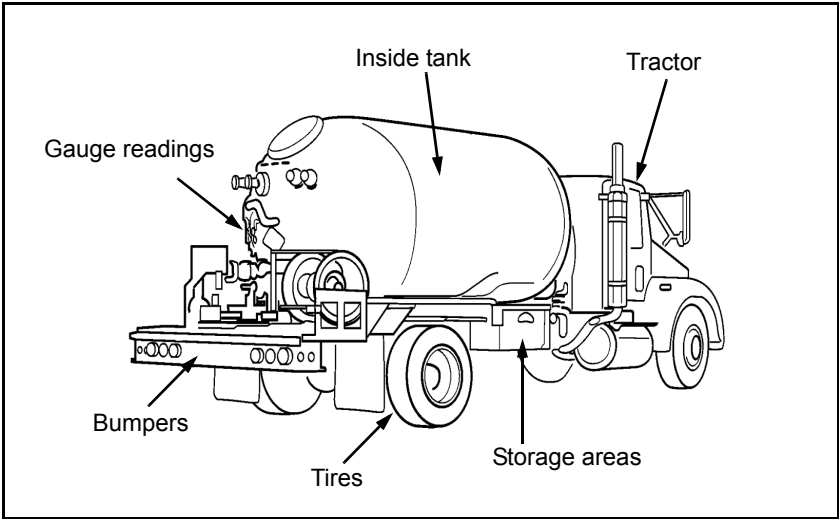


Figure B-15. Propane Tanker

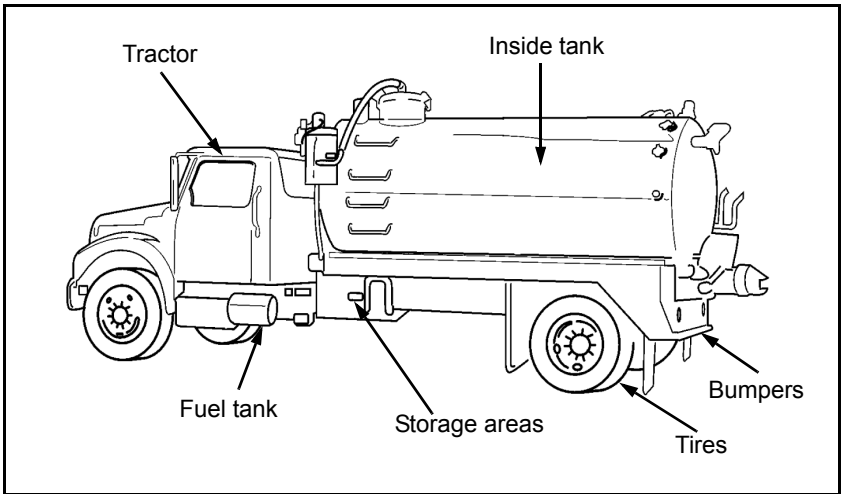


Figure B-16. Septic Service Tanker

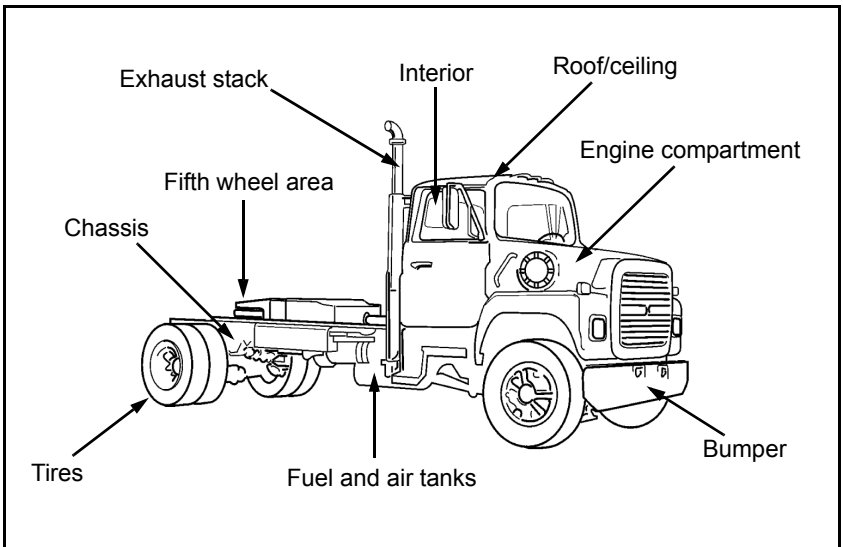


Figure B-17. Tractor

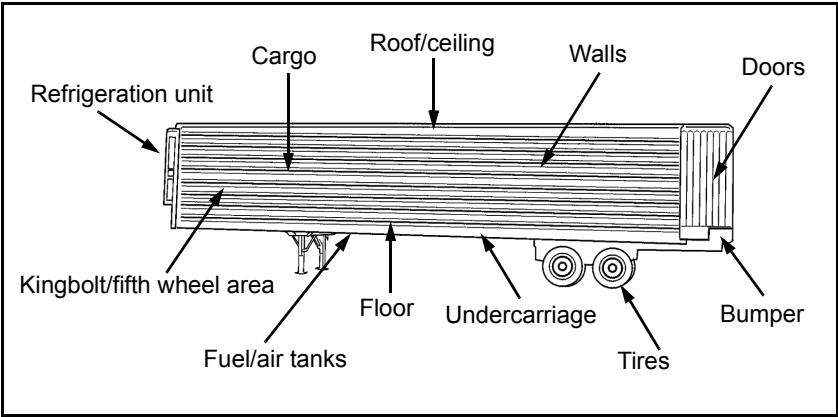


Figure B-18. Trailer

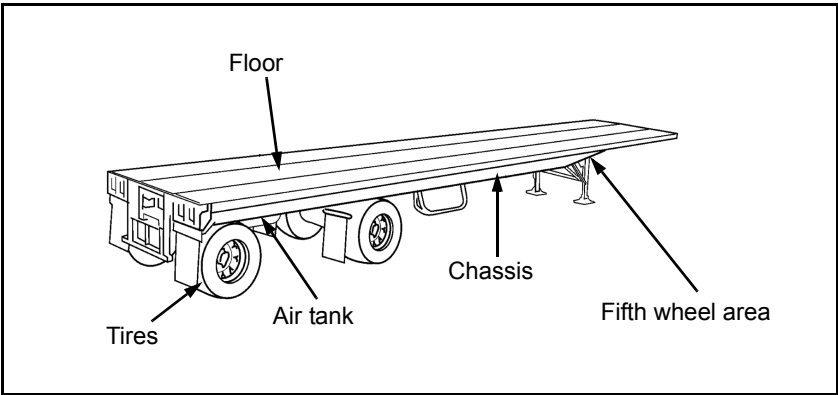


Figure B-19. Trailer Undercarriage

Appendix C

Rules for the Use of Force

RUF are different from the more familiar rules of engagement (ROE). RUF are escalating rules for US-based military personnel performing security duties when dealing with US citizens. ROE are directives delineating the circumstances and limitations for military forces to initiate or continue combat engagement with other forces. *AR 190-14* prescribes the RUF. SJA reviews the RUF prior to publishing.

C-1. An example of an RUF follows:

- A soldier has the inherent right of self-defense and the defense of others.
- Minimum force necessary and proportional to the threat is used.
- Deadly force is used only as a last resort—
 - For immediate threat of death or serious bodily injury to self or others.
 - For defense of persons under protection.
 - To prevent theft, damage, or destruction of firearms, ammunition, explosives, or property that is designated as vital to national security.

C-2. When the situation permits, security personnel will utilize escalating degrees of force. These degrees are defined as—

- SHOUT—verbal warnings to halt.
- SHOVE—nonlethal physical force.
- SHOW—intent to use weapons.
- SHOOT—deliberately aimed shots until the threat no longer exists. Warning shots are not permitted.

Appendix D

FPCON Security Measures Under AR 525-13 Requirements

The five FPCON levels that military installations respond to are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. A description of the FPCON NORMAL through DELTA measures, as prescribed by *AR 525-13*, are listed below.

FPCON NORMAL

D-1. When in FPCON NORMAL, implement a routine security posture designed to defeat the routine criminal threat.

FPCON ALPHA

D-2. When in FPCON ALPHA, implement the following measures:

- **Measure 1.** At regular intervals, remind all personnel, including family members, to report the following to appropriate LE or security agencies:
 - Suspicious personnel, particularly those carrying suitcases or other containers or those observing, photographing, or asking questions about military operations or security measures.
 - Unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of US installations, units, or facilities.
 - Abandoned parcels or suitcases.
 - Any other activity considered suspicious.

- **Measure 2.** The duty officer or personnel with access to building plans and area evacuation plans must be available at all times. Key personnel should be able to seal off an area immediately. Key personnel required to implement security plans should be on call and readily available. Ensure that LE and security agencies have immediate access to building floor plans and emergency evacuation plans for HRTs.
- **Measure 3.** Secure buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities and areas at installation, directorate, or activity level.
- **Measure 4.** Increase unannounced security spot checks (inspection of personal identification; vehicle registration; and contents of vehicles, suitcases, briefcases, and other containers) at ACPs on US installations and facilities.
- **Measure 5.** Reduce the number of access points for vehicles and personnel to minimum levels, consistent with the requirement to maintain a reasonable flow of traffic.
- **Measure 6.** As a deterrent, randomly apply Measures 14, 15, 17, or 18 from FPCON BRAVO, either individually or in combination with each other.
- **Measure 7.** Review all operations plans and orders and SOPs that pertain to the implementation of FPCONs BRAVO through DELTA.
- **Measure 8.** Review security measures for HRP, and implement additional measures warranted by the threat and existing vulnerabilities (for example, HRP should alter established patterns of behavior and wear inconspicuous body armor when traveling in public areas).
- **Measure 9.** Increase liaison with local police, intelligence, and security agencies to monitor the threat to Army personnel, installations, and facilities. Notify local police agencies concerning FPCON BRAVO measures that, if implemented,

could impact on their operations in the local community.

- **Measure 10.** Spare for major Army command (MACOM) or installation use.

FPCON BRAVO

D-3. When in FPCON BRAVO, in addition to the measures required by FPCON ALPHA, implement the following measures:

- **Measure 11.** Increase the frequency of warnings required by Measure 1, and inform personnel of additional threat information, as appropriate.
- **Measure 12.** Keep all personnel on call who are involved in implementing antiterrorism contingency plans.
- **Measure 13.** Review the provisions of all operations plans and orders and SOPs associated with the implementation of FPCON CHARLIE.
- **Measure 14.** Move automobiles and objects, such as trash containers and crates, away from HRTs and MEVAs to a distance based upon countering the assessed threat. If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures according to local plans (for example, frequent inspection by EDD teams, centralized parking, or controlled access to parking areas).
- **Measure 15.** Secure and regularly inspect all buildings, rooms, and storage areas not in regular use.
- **Measure 16.** At the beginning and end of each workday and at frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or packages, signs of tampering, and indications of unauthorized entry.

- **Measure 17.** Implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. If available, use trained EDD teams to inspect suspicious items and conduct periodic screening of mail. Encourage soldiers, civilian employees, and family members to inspect their personal mail, report suspicious items to local LE agencies, and refrain from handling such items until they are cleared by the appropriate authority.
- **Measure 18.** Inspect all deliveries to dining facilities, exchanges, guesthouses, clubs, libraries, schools, and other locally designated common-use facilities to identify explosive and incendiary devices. Use trained EDD teams for inspections, when available, if intelligence is received or a specific threat has been addressed. Encourage family members to report suspicious packages to local LE agencies and refrain from handling them until they are cleared by the appropriate authority.
- **Measure 19.** Increase both overt and covert security force surveillance of dining facilities, commissaries, exchanges, guesthouses, clubs, libraries, schools, chapels, and HRTs to improve deterrence and build confidence among staff and family members.
- **Measure 20.** Inform soldiers, civilian employees, and family members of the general threat situation to stop rumors and prevent unnecessary alarm. Periodically update all personnel as the situation changes.
- **Measure 21.** Brief representatives of all units and activities on the installation concerning the threat and security measures implemented in response to the threat. Implement procedures to provide periodic updates for these unit and activity representatives.
- **Measure 22.** Verify the identity of all personnel entering the installation, HRTs, and other

sensitive activities specified in local plans (inspect identification cards or grant access based on visual recognition). Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase the frequency of detailed vehicle inspections (for example, trunk, undercarriage, and glove box[es]) and the frequency of inspections of suitcases, briefcases, and other containers.

- **Measure 23.** Increase the frequency of random identity checks (inspection of identification cards, security badges, and vehicle registration documents) conducted by security force patrols on the installation.
- **Measure 24.** Increase security provided to off-post personnel in conjunction with HN LE agencies, where required and/or practicable, or transport off-post personnel to protected areas according to local contingency plans. Remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.
- **Measure 25.** Implement additional security measures for HRP, such as the conduct of countersurveillance operations, according to existing plans. Consider providing 24-hour protective services protection for Level I HRP (as defined in *AR 525-13*), if not already provided.
- **Measure 26.** Brief all LE personnel, guards, and security augmentation force personnel concerning the threat and policies governing the use of force/ROE. Repeat this briefing on a periodic basis.
- **Measure 27.** Increase liaison with local police, intelligence, and security agencies to monitor the threat to Army personnel, installations, and facilities. Notify local police agencies concerning FPCON CHARLIE and DELTA measures that, if implemented, could impact on their operations in the local community.

- **Measure 28.** Test attack-warning systems and supporting evacuation plans, ensuring proficiency and appropriate operations security (OPSEC).
- **Measure 29.** Spare for MACOM or installation use.

FPCON CHARLIE

D-4. When in FPCON CHARLIE, implement the following measures:

- **Measure 30.** Continue all FPCON ALPHA and BRAVO measures, or introduce those that have not already been implemented.
- **Measure 31.** Keep all personnel who are responsible for implementing antiterrorism plans at their place of duty.
- **Measure 32.** Reduce installation and HRT access points to the absolute minimum necessary for continued operation.
- **Measure 33.** Verify the identity of all personnel entering US installations, facilities, and activities (to include housing areas, schools, and other facilities that are not located on installations). Inspect identification cards, security badges, or other forms of personal identification. Visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. Increase the frequency of detailed vehicle inspections (such as the trunk, undercarriage, and glove box[es]) and the frequency of inspection of suitcases, briefcases, and other containers.
- **Measure 34.** Remove all vehicles parked within or near MEVAs and HRTs specified in local plans to a distance based upon countering the assessed threat. Implement centralized parking and shuttle bus service, where required.
- **Measure 35.** Issue weapons to all LE personnel, security guards, and guard force augmentation personnel, if not already implemented. Ensure that all personnel have been briefed concerning

the policies governing the use of force/ROE, particularly the criteria for the use of deadly force. Ensure that ammunition is available for immediate issue (for those personnel not already issued ammunition) and that supervisory personnel are familiar with the policies governing the issuance of ammunition.

- **Measure 36.** Increase security patrol activity to the maximum level sustainable. Weight the effort toward HRTs.
- **Measure 37.** Position guard force personnel in the vicinity of all HRTs and MEVAs. In OCONUS areas where permitted by the HN, position additional security personnel in the vicinity of otherwise unprotected housing areas, schools, hospitals, and other soft targets. Request additional security augmentation from HN LE and security agencies, particularly in otherwise unprotected areas.
- **Measure 38.** Erect barriers required to control the direction of traffic flow and to protect facilities vulnerable to a bomb attack by parked or moving vehicles.
- **Measure 39.** Consult local authorities about closing public (and military) roads and facilities that might make sites more vulnerable to terrorist attacks.
- **Measure 40.** Spare for MACOM or installation use.

FPCON DELTA

D-5. When in FPCON DELTA, implement the following measures:

- **Measure 41.** Continue all FPCON ALPHA, BRAVO, and CHARLIE measures or introduce those that have not already been implemented.
- **Measure 42.** Augment guard forces to ensure absolute control over access to the installation, MEVAs, and HRTs.

- **Measure 43.** Identify the owners of all vehicles already on the installation and, if in OCONUS, in the vicinity of soft targets off the installation. In those cases where the presence of a vehicle cannot be explained (owner is not present and has no obvious military affiliation), inspect the vehicle for explosive or incendiary devices or other dangerous items and remove the vehicle from the vicinity of HRTs as soon as possible. OCONUS commanders take unilateral action off post only in circumstances where there is a reasonable basis to believe that death, grievous bodily harm, or significant property damage will otherwise occur.
- **Measure 44.** Inspect all vehicles entering the installation, facility, or activity. Inspections should include cargo storage areas, the undercarriage, glove box[es], and any other area where explosive or incendiary devices or other dangerous items could be concealed. Briefcases, suitcases, boxes, and other containers in vehicles should also be inspected.
- **Measure 45.** Limit access to installations, facilities, and activities to those personnel with a legitimate and verifiable need to enter.
- **Measure 46.** Inspect all baggage (such as suitcases, packages, or briefcases) brought on the installation for the presence of explosive or incendiary devices or other dangerous items.
- **Measure 47.** Take measures to control access to all areas under the jurisdiction of the US command or agency.
- **Measure 48.** Implement frequent inspections of the exterior of buildings (to include the roof and subterranean areas) and parking areas. Security force personnel should conduct inspections at HRTs and MEVAs.
- **Measure 49.** Cancel or delay all administrative movement that is not mission-essential.
- **Measure 50.** Request that local authorities close public roads and facilities in the vicinity of

military installations, facilities, and activities that might facilitate the execution of a terrorist attack.

- **Measure 51.** Spare for MACOM or installation use.

Appendix E

Barriers and Blast Mitigation

The goal of employing barriers and blast mitigation techniques is to reduce the number of casualties associated with terrorist bombings. It is imperative that all principles, systems, and processes pertinent to protecting against vehicle bombs be used in concert with one another.

HAZARD TYPES

E-1. The detonation of vehicle bombs generates four primary hazards to personnel in fixed structures, shelters, and in the open. They are as follows:

- **Primary fragments.** Parts, pieces, and fragments of the vehicle and the bomb that are thrown outward from the detonation at moderate to high velocities and generally low trajectories. Primary fragments are generally the most lethal projectiles from a bomb detonation.
- **Secondary fragments from barriers and structures.** Countermobility devices and structures near a large vehicle bomb (LVB) and ACP will be completely involved in the LVB explosion and will produce secondary debris as they are broken up by the force of the blast. This debris will again be launched at relatively low trajectories, but will have significant velocity.
- **Secondary debris in fixed structures.** Objects surrounding a detonation become projectiles and fragments with enough energy to create damage of their own. Secondary debris can be categorized as near-field secondary debris

that results from barriers or ACP structures and building debris that results from the blast wave blowing out windows and walls. Window glass and some structural materials, such as masonry walls, can fall and become debris that is hazardous to personnel occupying perimeter spaces in buildings.

- **Blast.** The force of the explosion as it is transmitted through the air (blast) can cause injury to personnel in the open. It can pick up and translate ground debris and can fail and collapse structures, generating numerous injuries and deaths.

TECHNICAL DEFINITIONS

NEAR FIELD

E-2. Near field refers to the area immediately surrounding a detonation in which blast and fragment damage will be extensive.

BLAST WALLS

E-3. Blast walls are protective walls employed at an occupied position (such as a building) that are designed to reduce reflected pressures to incident pressures on vertical surfaces.

BLAST BARRIERS

E-4. Blast barriers are employed at ACPs near where a potential LVB might be located. Blast barriers can attenuate blast in their “shadow” to levels acceptable for hardened structures. Blast barriers do not reduce blast damage significantly for conventional and expeditionary structures and are ineffective for mitigating blast effects.

FRAGMENT BARRIERS

E-5. Fragment barriers are employed at ACPs close to where a potential LVB might be located and in the far

field adjacent to occupied positions. Fragment barriers provide protection from impacting primary and secondary debris. These barriers should not be employed with the intent to mitigate a blast.

EXPLOSIVE DETECTION

E-6. This section describes a systems approach for detecting a vehicle explosive threat through an access control process. A systems design represents a popular concept for increasing the overall capability to detect explosives across the threat spectrum. The basic idea is to employ traditional vehicle search techniques and explosive detection technology into an overall strategy to detect vehicle bombs at ACPs.

E-7. This concept incorporates the isolation of search stations by exploiting distance and physical barrier methods in an effort to mitigate the effects of blast and fragmentation, respectively. The optimum “generic mix” of traditional vehicle search techniques and explosive detection technology is—

- An MWD and handler—“putting nose on target.”
- An ACP security member doing a physical inspection—“putting eyes on target.”
- Some form of explosive trace detection technology—“putting technology on target.”

E-8. The systems design relies upon successively layering resources and tailoring technologies to address the—

- Site-specific threat.
- Resources available.
- Particular operating environment.

This layering allows security personnel to progressively detect and isolate explosive threats for immediate cordon and evacuation, followed by appropriate response actions by EOD technicians.

BLAST MITIGATION

E-9. The best protection is standoff distance. Barriers at the detonation point are better at mitigating fragments than they are at mitigating a blast. In fact, nothing sufficiently mitigates blast damage to expeditionary shelters except standoff, and every small distance helps. Concrete barriers must be used with the right mind-set—countermobility. If they are used in close proximity to access control areas, they *must* be soil-backed to avoid creating secondary fragmentation hazards. Countermobility involves physical barriers or soil-backed barriers that are used to direct, channel, or prohibit vehicle traffic to a predefined course of entry or exit.

BARRIERS

E-10. This section discusses blast mitigation barrier device employment and the recommended intended uses for these devices.

CONCRETE BARRIERS

E-11. Jersey and Bitburg barriers (*Figures E-1 and E-2*) are typically employed for countermobility or blast/fragment mitigation around ACPs and approach avenues. Concrete barriers employed in this fashion can be effective in stopping primary debris if they are tall enough. However, they may become secondary debris hazards in the immediate vicinity of a large explosion. Instead of protecting assets from blast or fragment damage, concrete barriers can cause additional damage by becoming secondary debris.



Figure E-1. Jersey Barriers Employed for Countermobility



Figure E-2. Bitburg Barriers Employed for Countermobility

Jersey Barriers

E-12. The intended use for Jersey barriers is countermobility. Jersey barriers—

- Should not be used to mitigate blast damage in the near field.
- Should not be used to mitigate fragment damage in the near field.
- May be used to mitigate fragment damage in the far field.
- Must always be interconnected with cables.

Bitburg Barriers

E-13. The intended use for Bitburg barriers is countermobility. Bitburg barriers—

- Should not be used to mitigate blast damage.
- Should not be used to mitigate fragment damage in the near field.
- May be used to mitigate fragment damage in the far field.

EARTH-FILLED BARRIERS

E-14. Earth-filled barriers (*Figures E-3, E-4, and E-5* [page E-8]) are typically employed around expeditionary structures to provide blast and fragment damage protection and consist of things like berms, concertainer walls, and sandbags. These barrier types work extremely well for fragment protection; however, for blast mitigation purposes, they will reduce structural damage only slightly by reducing reflected pressures to incident pressure levels.



Figure E-3. Earth-Filled Barrier



Figure E-4. Sandbags Used for Fragment Protection



Figure E-5. Water- or Sand-Filled Barriers

Sandbags

E-15. The intended use for sandbags is fragment mitigation. Sandbags—

- May also be used behind Jersey or Bitburg barriers to reduce or eliminate secondary debris hazards associated with spalling concrete.
- May be used to mitigate blast damage if implemented correctly.

Water- or Sand-Filled Plastic Barriers

E-16. The intended use for water- or sand-filled plastic barriers is limited countermobility for low-speed impact (certified by tests). Water- or sand-filled plastic barriers—

- May be used to mitigate fragment damage in the near field, depending on the threat level.
- May be used in the far field to mitigate fragment damage.

PERMANENT BARRIERS

E-17. Permanent barriers generally refer to structures, such as blast walls, that are intended to remain as a permanent facility-hardening measure (*Figure E-6 and Figures E-7 and E-8*, page E-10). Generally, these structures are employed in one of two locations—

- At the anticipated detonation location.
- Immediately in front of the building they are designed to protect.

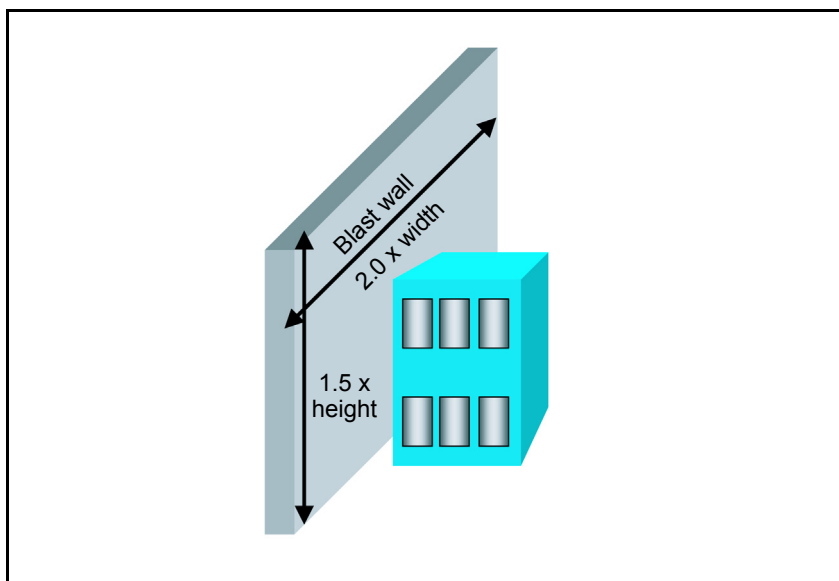


Figure E-6. Permanent Barriers

E-18. Unfortunately, test data indicates that employing a blast barrier at the detonation point provides no appreciable increase in protection in all but a very few building types. However, constructing a blast wall immediately in front of occupied structures can provide significant protection. The blast wall effectively reduces the pressure from a reflected pulse to an incident pulse, permitting reduced safe standoff distances. Blast walls

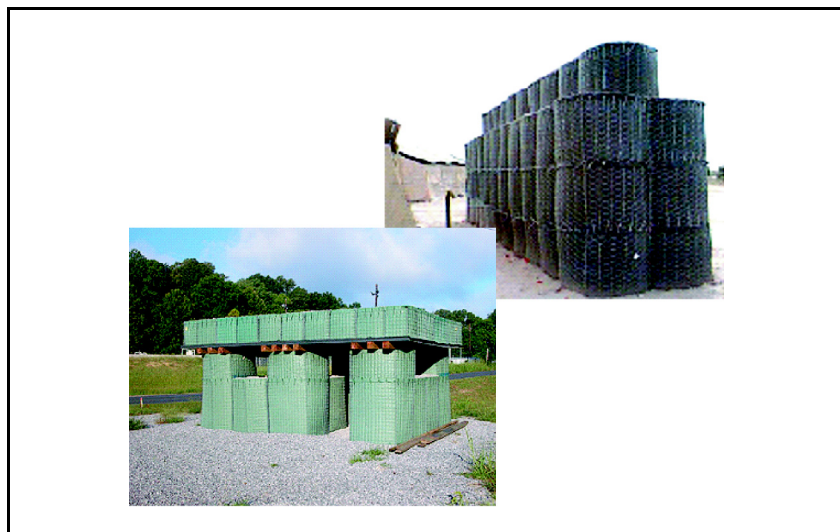


Figure E-7. Concertainer-Type Barriers

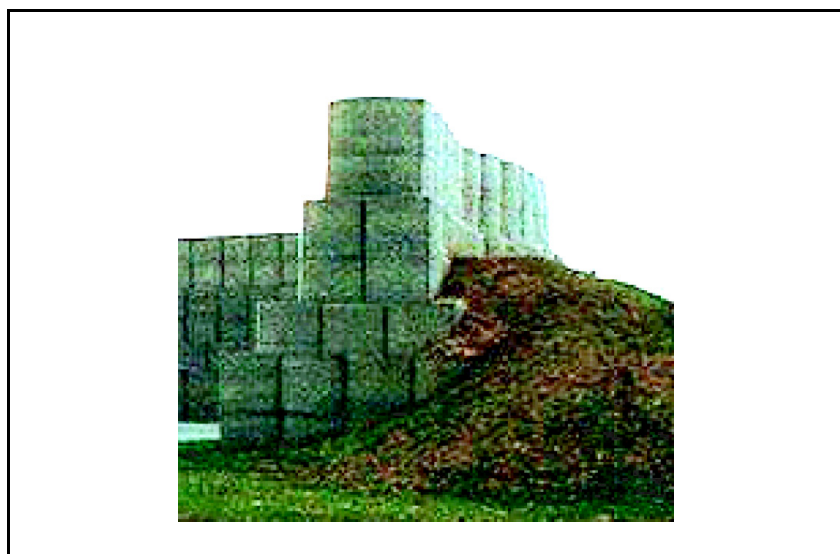


Figure E-8. Soil-Backed, Concertainer-Type Barrier

can be massive, requiring a height equal to 1.5 times the protected structure height and a width equal to 2 times the protected structure width. The wall also must be located no further than one story high from the protected face of the building.

Concertainer-Type Barriers

E-19. The intended use for concertainer-type barriers is blast and fragment mitigation. Concertainer-type barriers—

- May also be used for countermobility purposes.
- May be used as blast walls or for fighting positions.

Soil-Backed Barriers

E-20. The intended use for soil-backed barriers is countermobility. Soil-backed barriers—

- May also be used for fragment mitigation in the near field if implemented correctly.
- May be used for fragment mitigation in the far field.
- May also provide some blast mitigation capability in the far field if implemented correctly.

Glossary

AAFES	Army and Air Force Exchange Service
AC	air conditioning
ACP	access control point
act	active
AFI	Air Force instruction
AO	area of operations
APOE	aerial port of embarkation
AR	Army regulation
ASP	ammunition supply point
AT	antiterrorism
ATO	antiterrorism officer
attn	attention
AWOL	absent without leave
BEQ	bachelor enlisted quarters
bldg	building
BOQ	bachelor officers' quarters
C2	command and control
C4	composition 4 explosive
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosive
CCTV	closed-circuit television
CD-ROM	compact disk read-only memory
CID	Criminal Investigation Division
CS	O-chlorobenzylidene malononitrile
DA	Department of the Army
DAPSRB	Department of the Army Physical Security Review Board

DC	District of Columbia
DD	Department of Defense
DL	distance learning
DOD	Department of Defense
DODD	Department of Defense directive
DOT	Department of Transportation
DUI	driving under the influence
ECP	entry control point
EDD	explosive detector dog
EMS	emergency medical services
EOC	emergency operations center
EOD	explosive ordnance disposal
ERG	emergency response guidebook
FM	field manual; frequency-modulated
FP	force protection
FPCON	force protection condition
ft	foot; feet
gov	government
HAZMAT	hazardous material
HMMWV	high-mobility multipurpose wheeled vehicle
HN	host nation
HQ	headquarters
HRP	high-risk personnel
HRT	high-risk target
htm	hypertext markup language
http	hypertext transfer protocol
ID	identification
IED	improvised explosive device
IO	intelligence operations

IOC	information operations center
IPC	interpersonal communication
IST	installation support team
JTTP	joint tactics, techniques, and procedures
kg	kilogram(s)
lb	pound(s)
ldr	leader
LE	law enforcement
LMTV	lightweight medium tactical vehicle
LOTS	logistics over the shore
LVB	large vehicle bomb
m	meter(s)
MACOM	major Army command
MANSCEN	Maneuver Support Center
mbr	member
METT-TC	mission, enemy, terrain, troops, time available, and civilian considerations
MEVA	mission essential vulnerable area
MI	military intelligence
MO	Missouri
MOA	memorandum of agreement
MOU	memorandum of understanding
MP	military police
MRE	military rule of evidence
MTF	medical-treatment facility
MTMC	Military Traffic Management Command
MTOE	modification table of organization and equipment
MWD	military working dog

NCOIC	noncommissioned officer in charge
O&O	operational and organizational
OC	oleoresin capsicum
OCONUS	outside the continental United States
ODCSDEV	Office of the Deputy Chief of Staff for Developments
OIC	officer in charge
OPCON	operational control
OPSEC	operations security
PIO	police intelligence operations
plt	platoon
PM	provost marshal
POV	privately owned vehicle
PS	physical security
PVC	polyvinyl chloride
PVT	private
QRF	quick-reaction force
RAMP	Random Antiterrorism Measures Program
RCM	rules for courts-martial
RF	radio frequency
res	reserve
ret	retired
ROE	rules of engagement
RO/RO	roll on/roll off
RRT	rapid response team
RTO	radio-telephone operator
RUF	rules for the use of force

SGT	sergeant
SINCGARS	single-channel ground-to-air radio system
SJA	staff judge advocate
SMART	special medical-augmentation response team
SOP	standing operating procedure
SPC	specialist
SPF	special-purpose forces
SPOE	seaport of embarkation
sqd	squad
SRT	special reaction team
SSG	staff sergeant
TC	training circular
tm	team
TNT	trinitrotoluene
TRADOC	United States Army Training and Doctrine Command
TSP	training support package
TSWG	technical support working group
UCMJ	Uniform Code of Military Justice
UFC	unified facilities criteria
US	United States
USACMLS	United States Army Chemical School
USAMPS	United States Army Military Police School
USC	United States Code
VHS	video home system
VIC	vehicle inspection checklist
WMD	weapons of mass destruction

Bibliography

- 2000 Emergency Response Guidebook*. Transport Canada, the US Department of Transportation, and the Secretariat of Transport and Communications of Mexico. 2000.
- Air Force instruction (AFI) 31-101. *The Air Force Installation Security Program*. 1 March 2003.
- AFI 31-210. *The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards*. 5 April 2000.
- AR 25-30. *The Army Publishing Program*. 15 January 2004.
- AR 190-13. *The Army Physical Security Program*. 30 September 1993.
- AR 190-14. *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*. 12 March 1993.
- AR 190-16. *Physical Security*. 31 May 1991.
- AR 190-30. *Military Police Investigations*. 1 June 1978.
- AR 190-56. *The Army Civilian Police and Security Guard Program*. 21 June 1995.
- AR 190-58. *Personal Security*. 22 March 1989.
- AR 195-1. *Army Criminal Investigation Program*. 12 August 1974.
- AR 195-2. *Criminal Investigation Activities*. 30 October 1985.
- AR 381-10. *US Army Intelligence Activities*. 1 July 1984.
- AR 525-13. *Antiterrorism*. 4 January 2002.
- AR 600-20. *Army Command Policy*. 13 May 2002.
- AR 600-8-14. *Identification Cards for Members of the Uniformed Services, Their Family Members, and Other Eligible Personnel*. 20 December 2002.
- CID 195-1. *Criminal Investigation Operational Procedures*. 15 January 2004.
- DA Form 1602. *Civilian Identification*. 1 January 1956.
- DA Form 2028. *Recommended Changes to Publications and Blank Forms*. 1 February 1974.
- DA Form 4137. *Evidence/Property Custody Document*. 1 July 1976.

- DD Form 2 (RES). *Armed Forces of the United States Geneva Convention Identification Card*. 1 October 1993.
- DD Form 2 (RET). *United States Uniformed Services Identification Card (Retired)*. 1 October 1993.
- DD Form 2A (ACT). *Active Duty Military ID Card*. July 1974.
- DD Form 1173. *United States Uniformed Services Identification and Privilege Card*. 1 October 1993.
- DD Form 1173-1. *DOD Guard and Reserve Family Member Identification Card*. 1 July 1989.
- DD Form 2574. *Armed Forces Exchange Services Identification and Privilege Card*. 1 March 2000.
- DD Form 2765. *Department of Defense/Uniformed Services Identification and Privilege Card*. 1 April 1998.
- DODD 1325.6. *Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces*. 1 October 1996.
- DODD 5200.8. *Security of DOD Installations and Resources*. 25 April 1991.
- DODD 5210.56. *Use of Deadly Force and the Carrying of Firearms by DOD Personnel Engaged in Law Enforcement and Security Duties*. 1 November 2001.
- FM 3-19.1. *Military Police Operations*. 22 March 2001.
- FM 3-19.11. *Military Police Special-Reaction Teams*. 31 October 2000.
- FM 3-19.30. *Physical Security*. 8 January 2001.
- Installation Commanders' Blueprint, Installation Preparedness for Weapons of Mass Destruction*. Department of the Army. May 2001.
- Installation Commander's Force Protection Handbook*. HQ TRADOC. July 2002.
- Installation Force Protection Operational and Organizational (O&O) Plan*. HQ TRADOC, Office of the Deputy Chief of Staff for Developments (ODCSDEV). 30 July 2002.
- Internal Security Act of 1950*.
- Joint Publication 3-07.2. *JTTP for Antiterrorism*. 17 March 1998.

- Manual for Courts-Martial, United States*. 2000 Edition.
- Manual on Uniformed Traffic Control Devices for Streets and Highways*. US Department of Transportation, Federal Highway Administration. 2003.
- Public Law 107-295. *Maritime Transportation Security Act*. 25 November 2002.
- Standard Highway Signs, 2002 Edition (English)*. US Department of Transportation, Federal Highway Administration. 2002.
- TC 19-138. *Civilian Law Enforcement and Security Officer Training*. 1 August 2001.
- TSP 191-95B-004. *Quick Reaction Training*. 19 October 2001.
- Unified Facilities Criteria (UFC) 4-010-01. *DOD Minimum Antiterrorism Standards for Buildings*. 31 July 2002.
- USC, Title 10, Subtitle A, Part II, Chapter 47. *Armed Forces, General Military Law, Personnel, Uniform Code of Military Justice*.
- USC, Title 18, Part I, Chapter 67, Section 1382. *Crimes and Criminal Procedures; Crimes; Military and Navy; Entering Military, Naval, or Coast Guard Property*.
- USC, Title 23. *Highways*.
- USC, Title 50, Chapter 23, Subchapter I, Section 797. *War and National Defense, Internal Security, Control of Subversive Activities, Security Regulations and Orders; Penalty for Violation*.
- Vehicle Inspection Checklist*. Technical Support Working Group, Combating Terrorism Technology Support Office. 23 October 2000.

Index

A

- access control, 1-1
 - electrical, 1-9
 - installation boundary, 1-2, 6-5
 - response zone, 1-5
 - traffic and traffic control, 1-7
 - zone, 1-3
- access control point inspections, 2-1
 - commanders, 2-1
 - Court of Military Appeals, 2-1
 - jurisdiction, 2-1
 - procedures, 2-1
- access control zone, 1-3
 - design considerations, 1-5
 - safety zone, 1-5
 - cantonment area, 1-1
 - installation boundary, 1-1
 - RAMP. *See* Random Antiterrorism Measures Program (RAMP).
 - restricted, 1-1, 6-3, 6-4
 - traffic control devices, 1-10
- access controllers, 7-2
 - first physical line of defense, 7-2
 - procedures, 7-3
 - use of force, 7-3
- access to military installations, 3-1
 - authority, 3-2
 - bar letter, 3-2
 - jurisdiction, 3-2
 - restricted-access plan, 3-1
 - statutory authority, 3-2
- aerial ports of embarkation (APOE), 5-1, 7-5
- airfields, 6-4
 - aircraft, 6-4
 - helicopters, 6-4
 - landing strips, 6-4
- ALPHA, 4-2, D-1
- ALPHA, photographing, D-1
- antiterrorism, 7-1
- APOE. *See* aerial ports of embarkation (APOE).
- AR 190-56, 3-10
- Army law enforcement authority over military personnel, 3-10
 - AR 190-30, 3-10
 - jurisdiction, 3-10
 - UCMJ, Article 7, 3-10.
 - See also* Uniform Code of Military Justice (UCMJ), Article 7.
- augmentation guard force, 5-7
 - HRT, 5-8. *See also* high-risk target (HRT).
 - MEVAs, 5-8. *See also* mission essential vulnerable areas (MEVAs).
 - sentry duties, 5-8
 - use of force, 5-8
- authority on installations, 3-9

B

- barriers, E-1
 - Bitburg, E-6
 - concertainer, E-11
 - concrete, E-4
 - earth-filled, E-6
 - hazard types, E-1
 - Jersey, E-6
 - permanent, E-9
 - primary hazards, E-1
 - sandbags, E-8
 - soil-backed, E-11

- technical definitions, E-2
- water- or sand-filled plastic, E-8
- blast mitigation, E-1, E-4
 - barriers, E-4
 - hazard types, E-1
 - primary hazards, E-1
 - technical definitions, E-2
- boundaries, 6-3
 - barriers, 6-3
 - keep-out (exclusion) zone, 6-3
 - reaction zone, 6-3
 - restricted waters, 6-4
 - security zones, 6-3
- BRAVO, 4-2, D-3
 - covert, D-4
 - HRP, D-5. *See also* high-risk personnel (HRP).
 - Level I HRP, D-5
 - surveillance, D-4
 - warning systems, D-6

C

- cargo, 6-5
- carried firearms, 2-4
- carried items, 2-4
- CBRNE concepts, 5-10. *See also*
 - chemical, biological, radiological, nuclear, and high-yield explosive installation support team (CBRNE-IST).
 - CBRNE-rapid response team (RRT), 5-10
 - Chemical Corps, 5-10
 - decontamination, 5-11
 - initial hot line, 5-11
 - reconnaissance, 5-10
 - special medical-augmentation response team (SMART), 5-10
 - surveillance, 5-10
- CBRNE-IST. *See* chemical, biological, radiological, nuclear,

- and high-yield explosive installation support team (CBRNE-IST).

CHARLIE 4-2

Charlie 4-2

CHARLIE, D-6

Charlie, 4-2

- chemical, biological, radiological, nuclear, and high-yield explosive installation support team (CBRNE-IST), 5-8
- casualties, 5-9
- hazards, 5-9
- manning, 5-8
- organization, 5-9
- civil disturbance control gear, 5-16
- civil disturbance, 5-16
- civilian lawful detention, 3-6
- closed-circuit television (CCTV), 7-3
- commercial vehicle, 2-6

- EOD, 2-7. *See also* explosive ordnance disposal (EOD).

- procedures, 2-6

- TSP, 2-6. *See also* training support package (TSP),

- VIC, 2-6. *See also* vehicle inspection checklist (VIC).

- communications interoperability, 5-6
- critical, 5-6
- damage, 5-6
- control gear, 5-16

D

- dangerous items, 2-5
- deadly force, 3-12, C-1
 - apprehension or detention, 3-13
 - assets involving national security, 3-13
 - assets not involving national security, but inherently dangerous to others, 3-13
 - escape, 3-13

RUF, 3-14. *See also* rules for the use of force (RUF).
 self-defense and defense of others, 3-12
 serious offense against persons, 3-13

DELTA 4-3
 HRT, D-8. *See also* high-risk target (HRT).
 jurisdiction, D-8
 MEVAs, D-8. *See also* mission essential vulnerable areas (MEVAs).
 soft targets, D-8

DELTA, 4-3, D-7
 denial of entry, 2-4
 denied access, 2-1
 design considerations, 1-5
 access control zone, 1-6
 approach zone, 1-6
 general, 1-6
 guidelines, 1-5
 layout, 1-5
 response zone, 1-7

distance, 5-5
 Emergency Response Guidebook (ERG2000), 5-5
 Secretariat of Communications, 5-5
 Transport Canada, 5-5
 Transportation of Mexico, 5-5
 US DOT, 5-5

DOD identification card, 2-2
 DA Form 1602, 2-2
 DD Form 1173, 2-2
 DD Form 1173-1, 2-3
 DD Form 2 (RET) 2-2
 DD Form 2, 2-2
 DD Form 2574, 2-3
 DD Form 2765, 2-3
 DD Form 2A, 2-2

driver's license, 2-3

E

electrical power and lighting, 1-9
 barrier systems, 1-10
 CCTV, 1-9
 crash cushions, 1-10
 external, 1-9
 guard booth, 1-10
 interior, 1-9
 lighting, 1-9
 protection from the elements, 1-10
 requirements, 1-9
 telephone capabilities, 1-10
 work environment, 1-10

elements, 7-1
 emergency medical services (EMS), 5-4
 emergency responders, 5-3
 911-operator system, 5-4
 assistance, 5-3
 CBRNE-IST, 5-4. *See also* chemical, biological, radiological, nuclear, and high-yield explosive installation support team (CBRNE-IST).
 DA civilian police or guards, 5-4
 EMS, 5-4. *See also* emergency medical services (EMS).
 EOD personnel, 5-4. *See also* explosive ordnance detection (EOD).
 fire department, 5-4
 HAZMAT personnel, 5-4
 legal parameters, 5-4
 local, 5-3
 MPs, 5-4
 MWD teams, 5-4
 support, 5-3

entry control points, 6-1
 airfield, 6-1

- boundaries, 6-3
- infrastructure, 6-1
- pedestrian gates, 6-1
- railroad, 6-1
- special access control, 6-1
- vulnerabilities, 6-1
- water ports, 6-1
- water, 6-1
- establishment, 1-1
 - Access Control Working Group, 1-1
 - access control zone, 1-2
 - approach zone, 1-2, 1-3
 - construction, 1-1
 - installation boundary, 1-2
 - lane control markings, 1-3
 - RAMP, 1-3. *See also* Random Antiterrorism Measures Program (RAMP).
 - standoff distance, 1-3
- explosive dangerous items, 2-5
- explosive detection, E-3
 - detection technology, E-3
 - MWDs *See* military working dogs (MWDs).
- explosive detector dog searches 5-6
- explosive detector dog searches, explosive detector dog (EDD) teams, 5-6
- MWD handler, 5-6. *See also* military working dogs (MWDs).
- procedures, 5-6
- explosive device, 2-7
 - hot spots, 2-7, B-1
 - improvised, 2-7
- explosive materials, 2-5
- explosive ordnance disposal (EOD), 2-7
- exterior inspection, 2-8

F

- firearms, 2-4
- force protection conditions, 4-1
 - ALPHA, 4-1
 - BRAVO, 4-1
 - CHARLIE, 4-1
 - DELTA, 4-1
 - FPCON, 4-1
 - Homeland Security Advisory System, 4-1
 - NORMAL, 4-1
- force protection, 4-1, 7-1
 - intelligence operations (IO), 7-1
 - procedural measures, 7-1
- FPCON, 4-1, D-1
 - ALPHA, D-1
 - BRAVO, D-3
 - CHARLIE, D-6
 - DELTA, D-7
 - HRT, D-6. *See also* high-risk target (HRT).
- levels, 4-1
- MEVAs, D-6. *See also* mission essential vulnerable areas (MEVAs).
- NORMAL, D-1
- requirements, D-1
- threat, 4-1

H

- hazard types, E-1
 - debris, E-1
 - fragments, E-1
 - large vehicle bomb (LVB), E-1
 - primary, E-1
- high-risk personnel (HRP), 7-1
- high-risk target (HRT), 5-8
- hot spots, 2-7
 - procedures, 2-7
 - tampering, 2-7, B-1

I

identification card
 denial of entry, 2-4
 expired 2-4
 unserviceable, 2-4
 identification card, 2-3. *See also*
 photo identification checks.
 identification documents, 2-2
 implied consent, 3-4
 incident to lawful apprehension, 3-6
 inspection hot spots, B-1
 installation security, 5-1
 installation support teams (ISTs), 5-3
 intelligence fusion cell, 7-5
 intruders 6-4

K

knives, 2-4

L

large vehicle bomb (LVB), E-1
 lawful detention, 3-6
 legal considerations, 3-1
 access, 3-1
 searches, 3-2
 use of force, 3-11

M

metric conversion chart, A-1
 military incident to lawful
 apprehension, 3-6
 Military Rule of Evidence (MRE), 3-3
 military working dogs (MWDs), 3-3,
 6-2
 mission essential vulnerable areas
 (MEVAs), 5-1
 APOEs, 5-1. *See also* aerial
 ports of embarkation
 (APOE).
 debarkation, 5-1

SPOEs, 5-1. *See also* seaports
 of embarkation (SPOEs).

troop billets, 5-1

water points, 5-1

mission, enemy, terrain, troops, time
 available, and civilian
 considerations (METT-TC), 5-12

N

NORMAL, 4-2, D-1

O

objection, 2-1
 one-team concept, 7-4
 includes, 7-4
 intelligence fusion cell, 7-5
 responsibility, 7-5
 special staff, 7-5
 operations, 5-3
 augmentation, 5-3
 biological, 5-3
 CBRNE, 5-3
 chemical, 5-3
 emergency responders, 5-3
 explosive, 5-3
 memorandums of agreement
 (MOAs), 5-3
 memorandums of understanding
 (MOUs), 5-3
 nuclear, 5-3
 QRF, 5-3. *See also* quick-
 reaction force (QRF).
 radiological, 5-3
 SRT, 5-3. *See also* special
 reaction team (SRT).
 support, 5-3
 other law enforcement personnel's
 authority, 3-10
 AR 190-56, 3-10

P

- pedestrian gates, 6-6
 - access controllers, 6-6
 - barriers 6-6
- perimeter, 6-4
- photo identification checks, 2-3
 - denial of entry, 2-4
 - expired, 2-4
 - unserviceable, 2-4
- photographing, D-1
- probable cause, 3-4
 - consent to search, 3-5
 - government property, 3-5
 - inspections, 3-5
- procedures, 2-1
 - denied access, 2-1
 - hot spots, B-1
 - objection, 2-1
- provost marshal, 5-2
 - deterrent, 5-2
 - dissemination, 5-2
 - intelligence collection, 5-2
 - intelligence fusion cell, 5-2
 - police intelligence operations (PIO), 5-2
 - situational awareness, 5-2

Q

- quick-reaction force (QRF), 5-12, 5-15
 - armor, 5-16
 - augmentation forces, 5-13
 - battle drills, 5-14
 - breaches, 5-13
 - characterized, 5-12
 - circumstances, 5-13
 - collective tasks, 5-14
 - communications equipment, 5-15
 - equipment, 5-15
 - issued, 5-16

- lethal, 5-15
- MEVAs, 5-13. *See also* mission essential vulnerable areas (MEVAs).
- minimum composition, 5-12
- mission, enemy, terrain, troops, time available, and civilian considerations (METT-TC), 5-12
- nonlethal, 5-15
- organization, 5-13
- patrolling, 5-13
- perimeter, 5-13
- priorities, 5-14
- skills, 5-14
- special equipment, 5-16
- tactical, 5-16
- tacticians, 5-14
- tactics, 5-14
- training, 5-14
- vehicles, 5-16
- weapons, 5-15

R

- rail yards, 6-5, 6-6
 - capabilities, 6-5
 - cargo, 6-5
 - in-transit cargo, 6-5
 - railcars, 6-6
 - vulnerabilities, 6-5
- Random Antiterrorism Measures Program (RAMP), 4-1, 4-3
- reaction zone, 6-4
- reaction zone perimeter, 6-4
- response force capabilities, 5-1
 - concepts, 5-10
 - control gear, 5-16
 - hostile intent, 5-1
 - MEVAs. *See* mission essential vulnerable areas (MEVAs).
- QRF, 5-15. *See also* quick-reaction force (QRF).

training, 5-11

US Army Chemical School

(USACMLS), 5-11

vulnerabilities, 5-1

response zone, 1-5

rules for the use of force (RUF), C-1

S

seaports of embarkation (SPOE), 5-1

searches, 3-2, 3-4

abandoned property, 3-7

absent without leave (AWOL),

3-6

destruction of evidence, 3-7

emergencies, 3-8

exigent circumstances, 3-7

hot pursuit, 3-7

implied consent, 3-4

inspections, 3-3

inventories, 3-6

location, 3-4

military judges, 3-4

MRE. *See* Military Rule of Evidence (MRE).

MWDs. *See* military working dogs (MWDs).

plain view, 3-6

probable cause, 3-4

purpose, 3-2

sanctuary, 3-7

stop and frisk, 3-8

vehicle searches, 3-8

security force, 7-3

security measures, 4-1

security reaction zone, 6-4

security zones, 6-4

self-protection measures, 5-5

shielding, 5-5

special events, 6-7

crowds, 6-7

parking requirements, 6-7

vulnerabilities, 6-7

special reaction team, 5-6

disruption, 5-6

principal response force, 5-6

team organization, 5-7

threat situation, 5-6

SPOE. *See* seaports of embarkation (SPOE).

standoff distances, 1-4

stop and frisk, 3-8

suspicious dangerous items, 2-5

systems approach, 7-1, 7-2

APOE, 7-5. *See also* aerial ports of embarkation (APOE).

elements, 7-1

force multiplier, 7-2

SPOE, 7-5

systematic process, 7-2

T

tampering, 2-7

technical definitions, E-2

blast barriers, E-2

blast walls, E-2

fragment barriers, E-2

near field, E-2

technology, 7-3, 7-4

barriers, 7-3

CCTV, 7-3

lighting, 7-3

protective measures, 7-3

tiered response, 5-3

augmentation guard forces, 5-3

biological, 5-3

chemical, 5-3

installation support teams (ISTs),

5-3. *See also* chemical,

biological, radiological,

nuclear, and high-yield

explosive installation

support team (CBRNE-IST).

nuclear, 5-3

QRF, 5-3. *See also* quick-

- reaction force (QRF).
 - radiological, 5-3
 - responders, 5-3
 - SRT, 5-3. *See also* special reaction team (SRT).
- time, 5-5
- traffic and traffic control, 1-7
 - Department of Transportation (DOT), 1-7
 - pedestrians, 1-8
- traffic control devices, 1-10
- training support package (TSP), 2-6
 - VIC, 2-6. *See also* vehicle inspection checklist (VIC).
- training, 5-11

U

- UCMJ, Article 7. *See* Uniform Code of Military Justice (UCMJ), Article 7.
- US Army Chemical School (USACMLS), 5-11
- use of force, 3-11, C-1
 - chemical-aerosol, 3-11
 - deadly force, 3-12, C-1
 - degree of force, 3-12
 - degrees, C-1
 - example, C-1
 - firearms, 3-11
 - MP club, 3-11
 - prevent, C-1
 - procedures, 3-12
 - unarmed defense techniques, 3-11

V

- vehicle inspection
 - trunk, 2-10
- vehicle inspection checklist (VIC), Forward
- vehicle inspection, 2-5
 - commercial vehicle, 2-6
 - compartment inspection, 2-11

- considerations, 2-6
 - engine, 2-8
 - hidden compartments, 2-10
 - packages/devices, 2-10
 - passenger compartment, 2-11
 - polyvinyl chloride (PVC) pipe, 2-10
 - pull-off area, 2-6
 - random vehicle content inspection, 2-6
 - trunk 2-10
 - visitor, 2-6

W

- water ports, 6-1
 - CCTV, 6-4. *See also* closed-circuit television (CCTV), 7-3.
- harbors, 6-2
- internal security, 6-4
- intruders 6-4
- lighting, 6-4
- logistics over the shore (LOTS), 6-2
- Maritime Transportation Security Act of 2002, 6-2
- maritime, 6-3
- MWDs. *See* military working dogs (MWDs).
- perimeter, 6-4
- ports, 6-2
- protected assets, 6-4
- reactions zone, 6-4
- roll on/roll off (RO/RO), 6-2
- security measures, 6-2
- security zones, 6-4
- weapons of mass destruction (WMD), 5-5

TC 19-210
4 OCTOBER 2004

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:











JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
0425203

DISTRIBUTION:

Active Army, Army National Guard, and U.S. Army Reserve: To be distributed in accordance with distribution number 095696, requirements for TC 19-210.

Terrorist Bomb Threat Standoff Distances

Threat	Threat Description	Explosives Capacity ¹ (TNT Equivalent)	Building Evacuation Distance ²	Outdoor Evacuation Distance ³
	Pipe bomb	5 lbs 2.3 kg	70 ft/ 21 m	850 ft/ 259 m
	Briefcase/ suitcase bomb	50 lbs 23 kg	150 ft/ 46 m	1,850 ft/ 564 m
	Compact sedan	500 lbs 227 kg	320 ft/ 98 m	1,500 ft/ 457 m
	Sedan	1,000 lbs 454 kg	400 ft/ 122 m	1,750 ft/ 534 m
	Passenger/ cargo van	4,000 lbs 1,814 kg	640 ft/ 195 m	2,750 ft/ 838 m
	Small moving van/ delivery truck	10,000 lbs 4,536 kg	860 ft/ 263 m	3,750 ft/ 1,143 m
	Moving van/ water truck	30,000 lbs 13,608 kg	1,240 ft/ 375 m	6,500 ft/ 1,982 m
	Semitrailer	60,000 lbs 27,216 kg	1,570 ft/ 475 m	7,000 ft/ 2,134 m

