FWDA
Permit File
2003

Subject: RE: Submunitions
Date: Mon, 21 Jul 2003 11:40:14 -0400
From: "Stauber, Ricky S Mr BRACO" <Ricky.Stauber@hqda.army.mil>
To: "'julie wanslow'" <julie_wanslow@nmenv.state.nm.us>

Julie,

From the perspective that this property is and will be under Department of the Army control , the answer is yes it does. I am attaching a couple of reference documents that establishes what the Army policy is regarding signs and other precautionary actions that may be used at UXO sites to protect a local population.

Mr. Ricky S. Stauber
Project Manager/UXO Coordinator, J.M. Waller Associates
Base Realignment and Closure Office (DAIM-BA)
Rm 2D673
600 Army Pentagon, Washington DC 20310-0600
Ph: 703-697-0130 DSN: 223-0130 FAX: 703-693-7621

-----Original Message-----
From: julie wanslow [mailto:julie_wanslow@nmenv.state.nm.us]
Sent: Friday, July 18, 2003 4:37 PM
To: Stauber, Ricky S Mr BRACO
Subject: Submunitions

Ricky,

I have a question for you: Do you consider a barbed-wire fence to be an adequate barrier for preventing unknowing entry and minimizing the possibility for unauthorized entry of persons onto a site that contains submunitions?

Julie

Information Paper Fencing & Signage for UXO Sites.doc	**Name:** Information Paper Fencing & Signage for UXO Sites.doc **Type:** WINWORD File (application/msword) **Encoding:** base64

Compendum of Refs on signs and UXO Ed.doc	**Name:** Compendum of Refs on signs and UXO Ed.doc **Type:** WINWORD File (application/msword) **Encoding:** base64

Information Paper

In the context of conducting a risk assessment to determine fencing requirements for retained defense sites containing unexploded ordnance (UXO), you have asked about the potential liability as to trespassers who may breach the security of such sites. A generalized liability risk does exist and should be factored into the decision-making process when determining the degree to which former UXO sites should be secured.

Ordinarily under "tort," or personal injury, law, the owner or occupant of land or premises owes no duty to a trespasser entering the premises except to refrain from willful or wanton injury to him or her. Though the law is generally favorable to a trespassed landowner, courts are nonetheless solicitous of trespassing minors and afford them a special status under what has come to be known as the "attractive nuisance doctrine." The policy of protecting trespassing minors rests on the value of children to society, and the rationale for imposing a higher standard of care upon landowners when dealing with foreseeable child-trespassers is to encourage landowners to take affirmative steps to prevent injury to them. Further, many states elevate the duty of care required on the part of a landowner (from "reasonable" to "highest" or "utmost") when dangerous instrumentalities, such as explosive devices, are involved [note: state law is relevant here because it is the law of the state in which the injury occurred that is applied when suits for personal injury are brought under the Federal Tort Claims Act].

The criteria for application of the attractive nuisance doctrine is set forth in the Restatement of Torts 2d, Sec. 339, which addresses "artificial conditions highly dangerous to trespassing children" and which provides that:

"A possessor of land is subject to liability for physical harm to children trespassing thereon caused by an artificial condition upon the land if,

(a) the place where the condition exists is one upon which the possessor knows or has reason to know that children are likely to trespass, and,

(b) the condition is one of which the possessor knows or has reason to know and which he realizes or should realize will involve an unreasonable risk of death or serious bodily harm to such children, and,

(c) the children because of their youth do not discover the condition or realize the risk involved in intermeddling with it or in coming within the area made dangerous by it, and,

(d) the utility to the possessor of maintaining the condition and the burden of eliminating the danger are slight as compared with the risk to children involved, and,

(e) the possessor fails to exercise reasonable care to eliminate the danger or otherwise to protect the children."

There are a dozen or so reported cases of the attractive nuisance doctrine being applied to minors encountering UXO, either through their own deliberate trespass (including breaches of fence lines) or through the trespass of some third party who then transports the UXO to some other location. Whether the court has applied the doctrine and allowed the plaintiff to recover depends on the specific facts at hand, but, generally speaking, the younger the minor and the more perfunctory the security measures, the more likely the recovery in tort.

What to take from the attractive nuisance doctrine by way of practical advice is that it highlights the necessity of conducting a highly site-specific analysis which factors in local conditions, the local populace, and the likelihood of trespasser interest - and then designing and constructing obstacles commensurate with the degree of access restriction deemed necessary and appropriate. Optimally, because of the higher degree of care expected of a landowner possessing UXO, these areas should be maintained, fenced, posted, inspected, and otherwise secured in a manner in excess of what might otherwise be considered adequate and reasonable for closed property. Ultimately, though, regardless of the specific legal theory of recovery (be it in tort or under CERCLA Section 330), the analysis remains one of evaluating risk, determining reuse, and, of course, executing the requisite level of clean up.

Major Jeanette Stone
Restoration and Natural Resources
U.S. Army Environmental Law Division

UXO Safety Education
and
Guidance on Access Controls to UXO sites

1. **UXO Safety Education.** In response to JC King's query, *"If you have or are aware of guidance on when a UXO Safety Education Program will be implemented, please provide."*

a. AR 385-63, paragraph 2-10. already requires a UXO safety education program (paragraph provided in this paper).

b. VCSA msg 7 Jul 00 also requires UXO safety education (msg provided in this paper).

c. In addition, the upcoming revision to DAP 385-64 will require implementation of UXO Safety Education Programs Army-wide. Here is the applicable text:

2-17. Unexploded Ordnance (UXO) Safety Education Training For Local Schools

UXO Safety Education Training for schools in the general proximity of existing military installations with areas potentially containing UXO will be offered annually by the Safety Office responsible for the installation. The Corps of Engineer District responsible for a given Formerly Used Defense Site (FUDS) will offer training to schools near that FUDS. The parent (caretaker) installation/MACOM of BRAC installations will offer training to schools near that BRAC installation. Obviously, the school may decline the offer. This training shall consist of educating school age children, their parents and teachers, on the hazards of unexploded ordnance. It is the local commands option in how this training reaches the local community. The U. S. Army provides UXO safety training and outreach materials that can be accessed at the Defense Environmental Network and Information Exchange web site at https://128.174.5.51/denix/denix.html The safety office shall ensure that coordination with Public Affairs and the appropriate support personnel is accomplished. EOD and other personnel with technical knowledge of UXO hazards may provide assistance

End of Text

Please continue on next page

2. Guidance on Access Controls to UXO sites. In response to JC King's query, *"If you are aware of other guidance (COE, ACSIM, or ODCSOPS) for site security, please provide to me".*

There are snippets of guidance everywhere. I'm providing as much as I can in this paper
Common threads:

(1) Fences and security patrols are recommended.
(2) Signs are required.
(a) Format (color, letters, shape, etc) will be IAW OSHA "Danger" signs. I've provided the OSHA format later in this paper.
(b) Text will be bi-lingual, if needed in the locale.
(c) Provide pictograms, for kids.
(d) Sign spacing: anywhere from 100 feet to 200 meters, depending on reference.

In response to JC King's remark: *"I would like to see if we need to develop Army policy for security of such sites. If there is a need for such, then I would like to put together a work group to develop. Before doing so, I want to do some reading on the matter."* . The following reading material is provided:

a. VCSA message.

-----Original Message-----
From: AUTODINpostmaster [mailto:apm@ria-ams1.army.mil]
Sent: Wednesday, July 21, 1999 6:35 AM
To: autodin@mcalestr-emh3.army.mil
Subject: [Postmaster: [R] SUBJECT: PROTECTION OF THE PUBLIC FROM UNEXPLODED ORDNANCE (UXO)]

RTAUZYUW RUEADWD0102 2011831-UUUU--RUERAKW RUERNIL.
ZNR UUUUU
R 071647Z JUL 00
FM DA WASHINGTON DC//DACS-ZB//
TO RUFDNTU/CDRUSAREUR HEIDELBERG GE
RUEAHIC/CDRUSARPAC FT SHAFTER HI
RUAGEIG/CDRUSAEIGHT SEOUL KOR
RUERAIX/CDRTRADOC FT MONROE VA
RUEASRB/CDRFORSCOM FT MCPHERSON GA
RUEAOPA/CDRATEC ALEXANDRIA VA
RUEARNG/ARNGRC ARLINGTON VA
RUEAAMC/CDRUSAMC ALEXANDRIA VA
RUEABUC/CDRUSARASO FT BUCHANAN PR
RUEAMDW/CDRMDW WASHINGTON DC
RUERSHA/CDRUSAMEDCOM FT SAM HOUSTON TX
RUEADWD/DA WASHINGTON DC//SAAS//
INFO RUFDNTU/CDRUSAREUR HEIDELBERG GE//AEAGD-LB/-SM-A/AEAGA-S//
RUEAHIC/CDRUSARPAC FT SHAFTER HI//APLG/-MU/-SY/APSL/APPE-SE//

RUAGEIG/CDRUSAEIGHT SEOUL KOR//EAGD-CS/-AM/EASF/FKJ4/-AM/
FKJ3//
RUERAIX/CDRTRADOC FT MONROE VA//ATCS/ATBO-IS/-SO/ATTG//
RUEASRB/CDRFORSCOM FT MCPHERSON GA//AFLG/AFOP/AFPI-SO//
RUEAOPA/CDRATEC ALEXANDRIA VA//CSTE-CS/CSTE-ILE//

PAGE 02 RUEADWD0102 UNCLAS
RUEARNG/ARNGRC ARLINGTON VA//NGB-AVN-S/NGB-ARZ/ARL//
RUEAAMC/CDRUSAMC ALEX VA//AMCLG/AMCSF/AMCAM-LG//
RUEABUC/CDRUSARSO FT BUCHANAN PR//SOSF//
RHMFIUU/CDRUSARSO FT BUCHANAN PR//SOSF//
RUEAMDW/CDRMDW WASHINGTON DC//ANOS//
RUERSHA/CDRUSAMEDCOM FT SAM HOUSTON TX//MCSM//
RUERGAR/CDRUSASC FT RUCKER AL//CSSC-Z//
RUERAKW/DIRDAC MCALESTER OK//SOSAC-DO/-ES/-AV/-AO//
RUERNIL/CDROSC ROCK ISLAND IL//SOSFS-CO/SOSMA-SNS//
RUEADWD/DA WASHINGTON DC//DALO-AMA/DACS-SF/DAMO-TRS/DAIM-ODEP//
BT
UNCLAS
SUBJECT: PROTECTION OF THE PUBLIC FROM UNEXPLODED ORDNANCE (UXO)
A. AR 385-63 POLICIES AND PROCEDURES FOR FIRING AMMUNITION FOR TRAINING, TARGET PRACTICE, AND COMBAT 15 OCT 83
B. AR 210-21 ARMY RANGES AND TRAINING LAND MANAGEMENT 1 MAY 97
C. MY MSG DACS-ZB 101745Z MAR 00 SUBJ AMMUNITION AND EXPLOSIVES SAFETY ON RANGES
1. IT HAS LONG BEEN DOD AND ARMY POLICY TO USE LIVE MUNITIONS AND MANAGE LIVE-FIRE TRAINING RANGES IN A MANNER THAT SUPPORTS NATIONAL

PAGE 03 RUEADWD0102 UNCLAS
SECURITY OBJECTIVES AND MAINTAINS A HIGH STATE OF OPERATIONAL READINESS, WHILE AT THE SAME TIME PROTECTING HUMAN HEALTH AND SAFETY TO THE MAXIMUM EXTENT PRACTICABLE.
2. IN MAR 00, I ASKED COMMANDERS AND SUPERVISORS TO DIRECT THEIR PERSONAL ATTENTION TOWARD SETTING THE EXAMPLE FOR SAFETY ON TRAINING RANGES FOR OUR SOLDIERS AND CIVILIAN WORKERS; AND ENSURING THE ADEQUACY, COMMUNICATION, AND ENFORCEMENT OF EXISTING RANGE SAFETY STANDARDS AND PROCEDURES (REF C). IN LIGHT OF A RECENT TRAGIC DEATH OF A TEENAGER THAT INVOLVED UNEXPLODED ORDNANCE (UXO), IT IS EQUALLY CRITICAL FOR THIS SAME LEVEL OF PERSONAL ATTENTION TO BE DIRECTED TOWARD AGGRESSIVELY REVIEWING THE ADEQUACY, COMMUNICATION, AND ENFORCEMENT OF EXISTING STANDARDS AND PROCEDURES DESIGNED TO MINIMIZE THE POTENTIAL EXPLOSIVES HAZARDS THAT ACCESS TO AREAS KNOWN OR SUSPECTED OF CONTAINING UXO PRESENT.
3. I ASK COMMANDERS AND SUPERVISORS WHO HAVE RESPONSIBILITY FOR MANAGEMENT OF INSTALLATIONS WITH RANGES TO REVIEW CAREFULLY THE ARMY'S PUBLIC ACCESS AND EDUCATION REQUIREMENTS TO ENSURE THAT LOCAL IMPLEMENTING PROCEDURES AND CONTROLS BOTH COMPLY WITH THESE REQUIREMENTS AND ARE SUFFICIENTLY PROTECTIVE OF THE PUBLIC (REF A AND

REF B). IN THIS REGARD, IT IS IMPERATIVE THAT SPECIAL EMPHASIS BE

PAGE 04 RUEADWD0102 UNCLAS
PLACED ON:

A. ENSURING THAT THE SAFETY OF MILITARY AND CIVILIAN PERSONNEL WITHIN AN AREA KNOWN OR SUSPECTED OF CONTAINING UXO, PARTICULARLY RANGE IMPACT AREAS, TAKES PRECEDENCE OVER ALL OTHER ACTIVITIES.

B. PROHIBITING UNAUTHORIZED PERSONS FROM ENTERING AN IMPACT AREA OR OTHER AREAS KNOWN OR SUSPECTED OF CONTAINING UXO.

C. RESTRICTING AUTHORIZED ACCESS TO AREAS KNOWN OR SUSPECTED OF CONTAINING UXO TO PERSONNEL TRAINED IN UXO IDENTIFICATION AND THE PROCEDURES TO BE TAKEN SHOULD UXO BE ENCOUNTERED.

D. PROVIDING, WHEN REQUIRED, QUALIFIED ESCORTS FOR PERSONNEL AUTHORIZED ACCESS TO AREAS KNOWN OR SUSPECTED OF CONTAINING UXO.

E. ESTABLISHING AND IMPLEMENTING ACCESS CONTROLS TO DETER UNAUTHORIZED ACCESS (E.G., USE OF INSTALLATION SECURITY PATROLS; USE OF FENCING, GATES AND BARRIERS; POSTING OF UXO WARNING SIGNS; ETC.). THE POSTING OF RANGE BOUNDARIES AND OFF-LIMIT AREAS WITH PERMANENT WARNING SIGNS (BILINGUAL, AS APPROPRIATE) TO PROHIBIT TRESPASS AND ENTRY BY UNAUTHORIZED PERSONNEL INTO IMPACT AREAS AND SURFACE DANGER ZONES IS MANDATORY. SUCH SIGNS MUST CLEARLY INDICATE THAT TRESPASSING OR THE REMOVAL OF ITEMS IS PROHIBITED UNDER PENALTIES PROVIDED BY LAW, EMPHASIZE THE DANGER CONNECTED WITH THE RANGE AREA

PAGE 05 RUEADWD0102 UNCLAS
AND HANDLING OF UXO, AND BE POSTED AT 200 METER INTERVALS OR LESS.

F. ESTABLISHING AND CONDUCTING AN AGGRESSIVE AND PROACTIVE EDUCATION PROGRAM FOR ALL INSTALLATION PERSONNEL, THEIR FAMILIES, AND THE GENERAL PUBLIC ON THE DANGERS OF HANDLING UXO (DUD AMMUNITION). (OCONUS INSTALLATIONS SHOULD COORDINATE THE NEED FOR SUCH WITH THE HOST NATION AND APPLICABLE AGREEMENTS). MAXIMUM USE SHOULD BE MADE OF THE INSTALLATION'S SAFETY OFFICE, THE PUBLIC AFFAIRS OFFICE, RANGE CONTROL ORGANIZATION, ASSIGNED QUALITY ASSURANCE SPECIALISTS (AMMUNITION SURVEILLANCE), AND EOD ORGANIZATIONS. THE IMPORTANCE OF SUCH A PROGRAM CANNOT BE OVER-EMPHASIZED. ELEMENTS OF AN EFFECTIVE PROGRAM INCLUDE:

(1) PERIODIC USE OF THE LOCAL NEWS MEDIA TO WARN NEARBY COMMUNITIES OF THE HAZARDS OF TRESPASSING ON RANGES AND HANDLING UXO.

(2) ESTABLISHING AN OUTREACH PROGRAM TO EDUCATE PERIODICALLY SCHOOL CHILDREN, BOTH ON AND OFF THE INSTALLATION, ON RANGE HAZARDS.

(3) INSTRUCTING INSTALLATION PERSONNEL, THEIR FAMILIES, AND THE GENERAL PUBLIC IN THE LOCAL PROCEDURES FOR REPORTING UXO AND SUSPECTED MILITARY AMMUNITION OR EXPLOSIVES TO MILITARY AUTHORITIES.

4. THE ARMY OWES ITS FORCES AND THE PUBLIC THE HIGHEST POSSIBLE

PAGE 06 RUEADWD0102 UNCLAS
STANDARDS OF SAFETY AND PROTECTION CONSISTENT WITH OPERATIONAL READINESS. I ASK YOU FOR YOUR PERSONAL ATTENTION TO THIS IMPORTANT MATTER AND WIDEST DISSEMINATION TO ALL ACTIVITIES AND ORGANIZATIONS INVOLVED IN RANGE OPERATIONS.
BT

----- End of forwarded messages

b. **Army Safety Center Guidance on Danger Signs**. This guidance complies with OSHA.

Guidance is on the following two pages

Specifications for Accident Prevention Signs

Wording of signs

Ensure that the wording of any sign—

- Is concise and easy to read.
- Contains enough information to be easily understood.
- Is designed for the message to be carried in the form of a picture when appropriate.
- Is bilingual when appropriate.
- Is positive rather than negative when possible. For example, "Wear rubber gloves when handling" is preferable to "Do not handle without rubber gloves."

Sign inspection and maintenance

Signs should be inspected regularly and maintained in good condition. They should be kept clean, well-lit, and legible. Replace damaged or broken signs. All signs should be designed with rounded or blunt corners, with no sharp projections. The ends or heads of bolts or other fastening devices should be located in such a way that they do not constitute a hazard.

Sign size

When choosing a sign, consider dimensions that will permit use of standard-size materials. Base the size of the sign on—

- The location at which the sign will be placed.
- The character of the hazard involved.
- The purpose of the sign.
- The distance from which the sign should be legible.
- The amount of wording the sign will contain.

Required sign colors

All signs require a predominant color that is based on the sign's purpose. Below are the four types of signs and their characteristic color.

- Danger signs—Red
- Caution signs—Yellow
- Safety instruction signs—Green
- Directional signs—Black

Note: Many safety signs, especially international signs, are white on blue background.

Danger signs

- **Use.** Use a danger sign only when an immediate hazard exists. There must be no variations in the type or design of signs posted to warn of specific dangers. All personnel should be taught that danger signs indicate immediate danger and that special precautions are necessary.
- **Design.** Paints with phosphorescent or retroreflective content may be used when safety considerations justify the need for assuring visibility of signs in darkened areas or at night. Design danger signs as follows, and see example at figure 1 and on the front cover.

—Danger signs have a white background with the word "DANGER" appearing in white letters on a red oval. The red oval is placed inside a black rectangular panel. (A white line separating the outside edges of the red oval from the adjacent edge of the black panel may be used.)

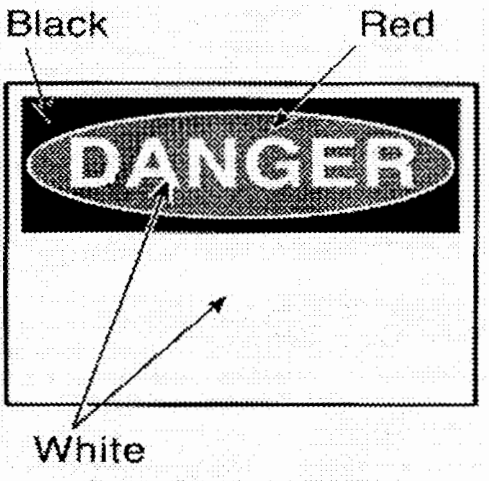


Figure 1. Example of danger sign

—The black rectangular panel should be placed at the top of the sign.

—Wording on the sign should be in black letters on the white background.

—The size of the red oval containing the word **DANGER** and the size of the letters used for the word **DANGER** will vary with the outside dimensions of the sign.

■ **Wording.** Danger signs will be worded to warn of specific dangers only. Keep sign wording as brief as possible, but convey all necessary information. The wording may include what the danger is, where it is, and how to avoid it. For examples of wording, see table 1.

Caution signs

■ **Use.** Use caution signs only to warn against potential hazards or to caution against unsafe practices. All personnel should be taught that a caution sign indicates a possible hazard against which proper precautions will be taken.

Table 1.
Examples of wording for danger signs

DANGER—High Voltage *(State maximum voltage when greater than 500 volts.)*
DANGER—No Smoking, Matches, or Open Light *(See note.)*
DANGER—Men Working Above
DANGER—Keep Away From Transformer
DANGER—Eye Protection Required in This Area
DANGER—Crane Overhead
DANGER—Keep Off Pole
DANGER—Use No Open Light—Flammable
DANGER—Artillery Firing in Progress
DANGER—Small Arms Firing in Progress
DANGER—Ammunition Dud Area
DANGER—Blasting
DANGER—Do Not Operate, Men Working on Repairs
DANGER—Hands Off Switch, Men Working on Line
DANGER—Extremely Noise-Hazardous Area—Both Plugs and Muffs Required
DANGER—Extreme Noise-Hazardous Equipment—Both Plugs and Muffs Required when Operating

NOTE: For "No Smoking" signs, a rectangular sign using white letters on red background is acceptable.

■ **Design.** Design caution signs as follows, and see example at figure 2 and on the front cover.

—Caution signs have a yellow background. The word **CAUTION** appears in yellow letters on a black rectangular panel.

—The black rectangular panel should be placed at the top of the sign.

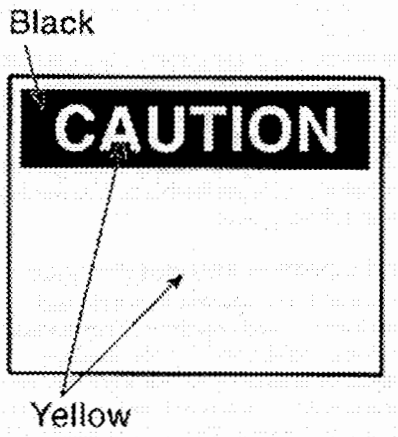


Figure 2. Example of a caution sign

—The size of the black rectangular panel containing the word **CAUTION** and the size of the letters used for the word **CAUTION** vary with the outside dimensions of the sign.

■ **Wording.** Caution signs will be worded to warn of possible dangers or unsafe practices. For examples of wording see table 2.

Safety instruction signs

■ **Use.** Use safety-instruction signs when there is a need for general instructions and suggestions relating to safety.

■ **Design.** Design safety-instruction signs as follows; see example at figure 3 and on the front cover.

—Safety-instruction signs have a white background. Words such as **THINK** or **BE CAREFUL** are in white letters on a green rectangular panel.

—The green panel should be placed at the top of the sign.

c. **Operations Support Command Policy on Access Controls to UXO areas**. The OSC Safety Office took a look at all the regs a while back and came up with an OSC policy:

OSC Safety Policy on Fencing and Signs for UXO Areas

1. This policy outlines the requirements to protect the general public and IOC employees from the hazards associated with unexploded ordnance. Specific safety requirements for fencing do not exist, so a combination of security requirements and common sense must apply. Posting requirements vary and conflict, so we recommend the most restrictive ones for sign spacing and size. This policy does not change existing requirements on UXO cleanup, nor does it change storage or use requirements.

2. Several of the references mandate fencing around UXO/burning/demolition/contaminated areas. References use general terms like "prohibit trespassing" and "prevent entry". Depending on the individual situation, the area may require 3-strand barbed wire, 5-strand barbed wire, or chain link security fencing. The determining factors are whether the general public has unrestricted access to the area, the level of hazard in the area, and whether the area contains security category 1 or 2 material. Fencing will comply with security requirements and will be 3-strand barbed wire, as a minimum, around UXO areas where public access is limited and hazards are low. Always verify with the controlling security office that area fencing is appropriate.

3. The most restrictive reference requires posting signs at 30.5 meters (100 feet) or less intervals around the UXO area and at all gates/normal entry points. Additionally, this office recommends posting signs within 15 meters (50 feet) on both sides of corners. These are minimum requirements and posting should be at smaller intervals for high hazard areas or restricted access areas.

4. Signs for UXO areas will be of the OSHA standard danger design designated by 29 CFR 1926.200b. (See 29 CFR 1926.200, Figure G-1, for basic sign design.) We recommend the signs be at least 13-inches by 17-inches in overall size and of weather resistant materials. Place the message "UNEXPLODED ORDNANCE - DO NOT ENTER" in two lines of red sans serif capital letters in the lower white section of the sign. Make lettering at least 5 centimeters (2 inches) high and of weather resistant materials.

5. References:

a. TM 9-1300-206, paragraph 10-3b(2) (note: this pub has been rescinded since this OSC Policy was written...Cliff Doyle).
b. TM 9-1300-277, paragraphs 2-3b(2) and 2-8a.
c. AR 385-63, paragraph 2-8f.
d. AR 385-64, paragraph 8.
e. DA Pamphlet 385-64, paragraph 17-3.
f. AMCR 385-100, paragraphs 22-24 and 22-26.

g. 29 CFR 1910, OSHA Industrial Standards, part 1910.145.
h. 29 CFR 1926, OSHA Construction Standards, part 1926.200.
i. ANSI Standard Z535.2 - 1991, Environmental and Facility Safety Signs.
j. FM 19-30 (Physical Security), paragraph 5-11b.

The OSC Safety Team established this policy on July 8, 1998.

End of OSC Policy

---

d. TM 9-1300-277, paragraphs 2-3b(2) and 2-8a. Text of these 2 paragraphs is on next 2 pages.

prior to detonation. The signal for detonation shall be given by the supervisor after all personnel are protected by cover or have reached a safe distance. Safe distances will be observed by all personnel.

(6) If a hazardous situation is encountered, all operations in the immediate vicinity will be shut down, and personnel evacuated to a safe location. Operations will not be resumed until the hazard has been eliminated. Prompt action will be taken to control any hazard.

(7) The demilitarization/disposal of munitions by burning or detonation involves the release of toxic fumes. A covered pit may limit the range of fragments but the control of fumes is dependent upon a number of factors, each of which must be carefully assessed for the particular material being destroyed at the time and place the operation is conducted.

(8) No demilitarization/disposal operation will be conducted during an electrical storm or when such a storm is approaching within 5 kilometers (3 miles). Additionally, disposal by detonation using an electrical firing system will not be conducted during sand, dust, or snow storms.

(9) Demilitarization/disposal by open burning will not be conducted when wind velocity exceeds 15 miles per hour.

2-3. SAFETY AT DEMILITARIZATION/DISPOSAL AREAS

a. TM 9-1300-206 provides information concerning hazards to personnel and damage to facilities that may be expected at given distances. These distances do not provide protection to personnel in the open from fragments and debris.

b. The minimum required signs or warning devices at the entrances and around the perimeter of the demilitarization/disposal are as follows:

(1) Red range flag to be flown or a rotating red beacon light be in operation during demilitarization/disposal operations and removed only after the range has been declared safe. The flag will be a minimum of 0.9 meters (three feet) wide by 1.5 meters (five feet) long.

(2) Danger signs with the legend EXPLOSIVE DISPOSAL RANGE—KEEP OUT imprinted on them, will be posted at the entrances and at 152 meters (500-foot intervals) around the perimeter of the range. The signs will be multilingual when necessary and of sufficient size to incorporate the legend in 5 centimeters (two-inch) red letters on the white background.

(3) Guards, safety signal, and warning signals will be used as required to keep unauthorized personnel from danger areas during destruction operations.

c. In areas where demilitarization/disposal ranges are not under constant control of U.S. Armed Forces, the following safety requirements will be strictly adhered to:

(1) Prior to starting demilitarization/disposal operations, the disposal range will be searched for unauthorized personnel.

(2) Guards will be posted to prevent entry into the area prior to and throughout the demilitarization/disposal operation. Guards will be afforded adequate protection from fragments.

d. A first aid kit, NSN 6545-00-116-1810, or suitable substitute, will be available during disposal operations. An ambulance or first aid vehicle, manned by personnel trained to handle casualties that may occur during demilitarization/disposal of specific munitions, will be on hand. Type of equipment for specific munitions being demilitarized/disposed of will be coordinated with the Base Medical Facility.

e. A means of communication with both Base facilities and demilitarization disposal personnel will be established. Communication may be by the most convenient method (radio, telephone, walkie-talkie, etc.), but the equipment used will be in good working order prior to commencing any operation. The applicable safety distances for electromagnetic devices in TM 9-1300-206 will be followed

f. A pit should be used to limit fragments when demilitarizing by detonati

of flammable dusts, gases, or vapors. Authorized hand tools or other implements used in the vicinity of hazardous materials must be handled carefully and kept clean.

(2) If the use of ferrous metal hand tools are required because of strength characteristics, the immediate area and equipment shall be free from exposed explosives and other highly combustible materials.

(3) Non-sparking or spark-resistant tools of lead or beryllium alloys that require sharpening or shaping shall be replaced rather than ground down, unless adequate exhaust ventilation is available on the grinder being used for this purpose.

2-7. HOUSEKEEPING

Buildings and magazines within a demilitarization/disposal area will be kept clean and orderly at all times.

a. Waste Materials. Oily rags, combustible and explosive scrap, and paper will be kept separate from each other. Each type of waste should be placed in closed, non-combustible containers properly marked and preferably located outside the buildings.

b. Cleaning. A regular cleaning program will be carried on as frequently as required for maintaining safe operations. Extensive cleaning should not be conducted while an explosives operation is being performed.

c. Sweeping Compounds. Hot water or steam should be used wherever practicable for cleaning floors in buildings containing explosives. Sweeping compounds which are non-abrasive and compatible with the explosives involved may be used where the use of steam or hot water is not practicable. Such compounds may be combustible but will not be volatile (closed cup flash point will be more than 230°F). Sweeping compounds containing wax will not be used on conductive flooring. Where nitrated organic explosives are involved, which may form sensitive explosives compounds with caustic alkalies, use of cleaning agents containing caustic alkalies is prohibited.

d. Explosives Recovery and Reuse. All loose explosives recovered as sweepings from floors of operating buildings will be destroyed.

2-8. SECURITY

a. Fencing, Placarding, and Admittance to Demilitarization/Disposal Areas. An explosives area will be placarded at each entrance. Unauthorized persons will not be permitted to enter. Authorized persons must enter and leave ammunition areas at designated points. The placard will require personnel before entering the area to present proper credentials and turn over all prohibited articles to the guard on duty, or to place them in containers provided for that purpose. A demilitarization/disposal area will be separated from administration, residential and entirely unrelated inert and warehouse areas by fences. Fencing (excluding that installed for security reasons only) should not be placed closer to magazines than magazine distance nor closer to explosives operating buildings than intraline distance (See DARCOM-R 385-100/TM 9-1300-206). Reservation boundaries should be fenced. In certain cases, topography and/or other physical considerations may make fencing impossible or impracticable. Security measures will be in accordance with AR 50-6 and AR 190-11. The boundary of each explosives area will be posted at 180 meters (600-foot intervals) to warn against trespassing.

b. Guard Protection.

(1) Magazines and areas in which there are explosives and ammunition will be guarded adequately at all times. Entrances to these areas will be locked unless protected by guards.

(2) Guards and others in charge of explosives and ammunition will be thoroughly instructed in emergency fire fighting procedures and the hazards due to fire and explosions, and the safety precautions to be taken. They will be instructed that their most important duty is to protect explosives and ammunition against fire. Alarms will be given with the greatest possible speed so as to start action instantly. Serious fires and explosions have been avoided by prompt

e. AR 385-63, paragraph 2-8f.

2-7. Warning signals and signs

Persons approaching a firing area in use will be warned. Scarlet danger flags and, when necessary, warning signs will be displayed at appropriate points.

2-8. General limitations

a. Ranges will be located so that personnel engaged in firing activities will not be nearer than inhabited building distance to ammunition storage areas. If available land areas are inadequate, the separation distance from personnel on the firing range to ammunition storage areas may be reduced to not less than public highway distance. These distances may be determined by referring to the tables of quantity-distance in TM 9-1300-206 and volume 1, Naval Sea Systems Command Ordnance Pamphlet 5. Compute quantity distance based on the quantity and class of ammunition in the limiting magazine or storage point within the ammunition area. The limiting magazine or storage point is the one requiring the greater distance based on the quantity and class of ammunition in storage.

b. The scarlet streamer during daylight hours, substituted by blinking red lights during night hours, will be displayed from a prominent point for a range complex and at all times during firing. No firing will take place unless these conditions are met.

c. Individual vehicles, tanks, and armored personnel carriers will display a red flag when firing (para 12-10).

d. Signs warning persons of the danger from projectiles, bombs, and duds will be posted near the firing area at all times.

e. Limit of fire markers both external (outer) and internal (inner) will be emplaced to denote right and left limits of fire. Where cross-firing is to be conducted, internal limit markers will be emplaced to denote internal right or left limits of fire from specific firing positions.

f. Besides the warning signals and signs used to prevent entry to the range during firing, the boundaries of all range areas adjacent to roadways and points of entry, or along the outside limits of ricochet areas, will be posted with permanent signs. They will be placed at 200 meter intervals or less, or in a way that will insure that a person cannot enter the range without seeing at least one sign within a legible distance. The signs will emphasize the danger connected with the range area and the handling of unexploded ammunition. They will prohibit trespassing or the removal of items under penalties provided by law. The design, color, and size will conform to guidance in AR 385-30. (Hilly or wooded terrain may require more signs than would flat, open terrain.)

g. Procedures will be established to cover the turn-in of military ammunition and explosive items by unauthorized persons.

2-9. Range clearance operations

The commander responsible for range clearance operation will—

a. Review all records on an area to be cleared to determine the types of duds present and the degree of contamination.

b. Determine the type of clearance to be done.

c. Request the supporting explosive ordnance disposal (EOD) element to scout the area to confirm the information in the records. This will help in the preparation of a detailed clearance plan.

d. Prepare a detailed plan of operation. It will include—

(1) Number of EOD qualified personnel needed to supervise the operation.

(2) Number of other personnel needed (e.g., searchers, supervisors, and drivers).

(3) Amount and type of equipment needed (such as vehicles and engineer equipment).

(4) Dates and time to conduct the clearance.

(5) Funding for the clearance operation.

(6) Administration and logistical support.

(7) Medical personnel and emergency-type medical vehicles needed.

(8) Safety training for all searchers, markers, and supervisory personnel. Training will be conducted before the start of an operation and as required during operations. All personnel who will participate in range clearance will view Army Training Film 9-6153.

e. Prepare after-action reports, including the information required by AR 405-90, or applicable US Navy or Marine Corps directives, as a permanent part of the range records.

2-10. Education

a. Installation commanders having range impact areas will place special emphasis on aggressive educational programs. All personnel must be properly cautioned on the dangers of dud ammunition and other items of unexploded ordnance. In this regard, maximum use should be made of the US Army Forces Command (FORSCOM) EOD personnel and guidance in FM 9-15.

b. Military family members will be instructed that ranges are off limits and will be cautioned about the hazards.

c. The local news media will be used periodically to warn the nearby communities of the hazards in trespassing on range areas and in handling unexploded ammunition.

d. A program will be established to educate school children, both on and off the installation, on range hazards.

e. Military parents, children, and other personnel will be instructed in the local procedures that provide

f. **AMCR 385-100, paragraphs 22-24 and 22-26.**

22-24. Cleaning of Ranges. Ranges shall be "policed" for live ammunition as soon as practicable after each test (not to exceed 30 calendar days). The disposition/disposal of unexploded (dud) ammunition fired on test ranges is the direct responsibility of the organization firing the item. Ammunition collected as a result of these policing operations shall be disposed of as follows:

a. Slugs and ammunition with inert filler and inert fuzes shall be collected in a separate stack in a designated safe location and the stack identified for future disposition, following Army and local environmental/disposition guidance.

b. Ammunition containing high explosives with live fuzes and all duds shall be detonated in place by personnel certified per AMC-R 350-4.

c. Dud ammunition shall not be left on the range after testing has ceased for the day unless at least one of the following situations exists:

(1) The range has a security fence totally surrounding it.

(2) The range has a 24-hour physical security coverage.

(3) Trespassing on the range is not evident or access is not easily gained from public traffic routes (i.e., land, water).

Remainder of para 22-24 not shown

22-26. Function and Trace Test of Ammunition.

a. General.

(1) This paragraph prescribes the safety precautions necessary in conducting tests required by SB 742-1. This includes information relative to establishing surface danger zone data required for the safe firing of the weapons, munitions, and explosive devices involved in these tests. Surface danger zone diagrams (safety fans) indicating specific danger areas are based on the latest available information. The danger areas established are minimum requirements and are adequate only when employed with properly functioning safety equipment and/or devices which are operated by thoroughly trained and certified personnel. Local SOPs and/or regulations designed to minimize the potential for personal injury and property damage shall be established to supplement this regulation. These procedures should prescribe or refer to additional precautions contained in

applicable TMs and FMs for the particular weapon, munition, explosive device and classes of fire being conducted.

(2) The commanders of all installations and activities performing function and trace of small arms ammunition will establish a test range safety program as an addendum to the installation safety program. This program will include consideration of the following: maintenance and policing of ranges; selection of qualified test personnel; preparation of detailed maps; notification of firing; stationing of ambulances, range personnel; wearing of hearing protection devices per AR 40-5; taking suitable precautions to prevent unauthorized trespass or presence on ranges; and other duties and activities associated with the safe operation of ranges. In addition, the range safety planning for the firing of any ammunition or explosives must include the available terrain, purpose of the firing, atmospheric conditions, and the adequacy and accuracy of safety equipment required to ensure that the ammunition and explosives or debris resulting therefrom will not violate the boundaries of the surface danger zone.

(3) Suitable precautions will be taken to assure that all unauthorized persons are excluded from the surface danger zone as set forth in this regulation prior to firing. Livestock will also be excluded unless an agreement in writing has been completed with the owner or owners thereof. After firing is completed, precautions will be taken to prevent entry into the impact area by all unauthorized personnel until a thorough search of the impact area has been made and any unexploded or contaminated items found are destroyed by personnel certified per AMC-R 350-4.

(4) Range guards properly instructed concerning their duties and/or appropriate barriers with signs will be posted to cover all normal approaches to the danger area

Remainder of para 22-26 not shown.

End of text

---

q. FM 3-19-30, paragraphs 4-33 and 4-34.

Warning Signs

4-33. A significant amount of warning signs should be erected to ensure that possible intruders are aware of entry into restricted areas. Warning signs augment control signs. They warn intruders that the area is restricted and that trespassing may result in the use of deadly force.

4-34. Warning signs should be installed along the limited area's physical barriers and at each entry point where they can be seen readily and understood by anyone approaching the perimeter.

In areas where English is one of two or more languages commonly spoken, warning signs must contain the local language in addition to English. The wording on the signs will denote warning of a restricted area. The signs should be posted at intervals of no more than 100 feet. They must not be mounted on fences equipped with intrusion-detection equipment. Additionally, the warning signs prescribed in AR 190-13 should be posted at all entrances to limited, controlled, and exclusion areas. See Chapter 7 for more details.

End of text

---

h. FM 3-19-30, Chapter 7.

Chapter 7

Access Control

Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access-control system must be established and maintained to preclude unauthorized entry. Effective access-control procedures prevent the introduction of harmful devices, materiel, and components. They minimize the misappropriation, pilferage, or compromise of materiel or recorded information by controlling packages, materiel, and property movement. Access-control rosters, personal recognition, ID cards, badge-exchange procedures, and personnel escorts all contribute to an effective access-control system.

DESIGNATED Restricted Areas

7-1. The installation commander is responsible for designating and establishing restricted areas. A restricted area is any area that is subject to special restrictions or controls for security reasons. This does not include areas over which aircraft flight is restricted. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

Degree of Security

7-2. The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas. A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for

administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area. The commander establishes the control of movement.

- A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.
- An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

7-3. The security protection afforded by a restricted area pertains particularly to subversive-activity control; that is, protection against espionage, sabotage, or any such action adversely affecting national defense. Within this context, the designation "restricted area" is not applicable to an area solely for protection against common pilferage or misappropriation of property or material that is not classified or not essential to national defense. For example, an area devoted to the storage or use of classified documents, equipment, or materials should be designated as a restricted area to safeguard against espionage. An installation communications center should also be so designated to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's tool room should not be so designated, although the commander may impose controls to access. This may be a simple matter of posting an "off limits to unauthorized personnel" sign. The PM or the physical-security manager acts as an advisor to the commander. In his recommendations, he must consider evaluating the purpose of designating a restricted area and coordinating with the intelligence officer and the staff judge advocate (SJA).

7-4. A restricted area must be designated in writing by the commander and must be posted with warning signs according to AR 190-13. In areas where English is one of two or more languages commonly spoken, warning signs will be posted in English and in the local language (see Figure 7-1 below).

7-5. An installation may have varying degrees of security. It may be designated in its entirety as a restricted area, with no further restrictions; or it may be subdivided into controlled, limited, or exclusion areas with restrictions of movement and specific clear zones. Figure 7-2 depicts a simplified restricted area and the degrees of security.

RESTRICTED AREA

THIS (INSTALLATION OR ACTIVITY) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF (TITLE, COMMANDING GENERAL OR COMMANDING OFFICER) IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNATHORIZED ENTRY IS PROHIBITED.

ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIVES OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.

Figure 7-1. Sample Restricted-Area Warning

End of Text

g. **AR 190-13, paragraph 6-4.**

6–4. Posting of restricted areas

a. Except when such action would tend to advertise an otherwise concealed area, or when in conflict with Host Nation Agreements, signs or notices will be posted in conspicuous and appropriate places to identify a restricted area. This includes signs posted at each entrance or approach to the area, and on perimeter fences or boundaries of the area.

b. Failure to post conspicuous signs and notices to give people approaching a restricted area actual knowledge of the restriction, may seriously hamper any resulting criminal prosecution.

c. Each sign or notice will be marked with the words, "RESTRICTED AREA," and include the warning notice below.

THIS (INSTALLATION, ACTIVITY, ETC.) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF (TITLE: COMMANDING GENERAL OR COMMANDING OFFICER) IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNAUTHORIZED ENTRY IS PROHIBITED.

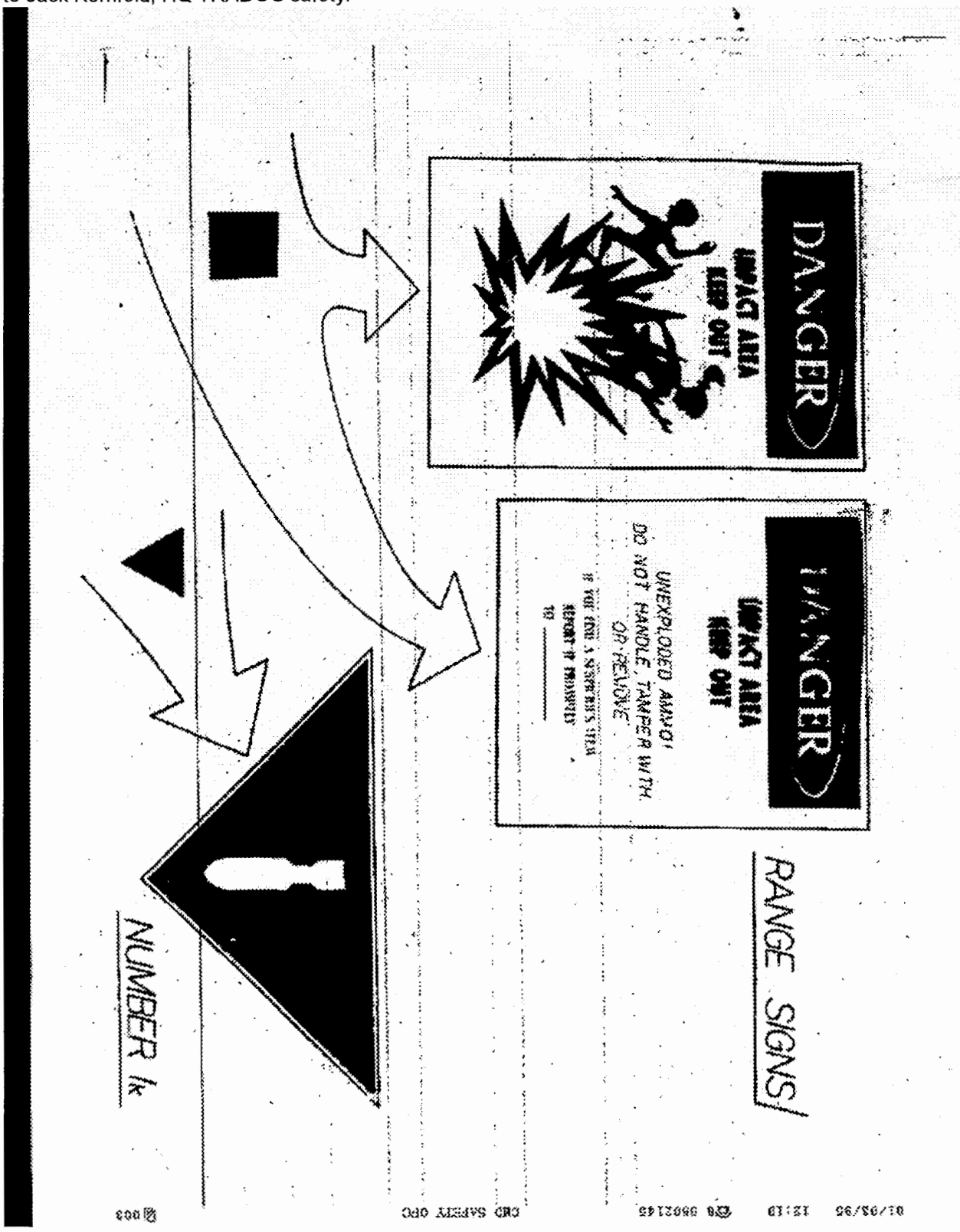
ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIONS OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER.

ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.

d. In areas in which English is but one of two or more languages commonly spoken, warning signs will contain the local languages besides English.

Continued on next page

h. UXO Warning Signs used at Camp Shelby that Camp Shelby successfully used in a lawsuit, according to Jack Kornfeld, HQ TRADOC safety.



Cliff Doyle
Safety and Occupational Health Manager
US Army Technical Center for Explosives Safety
ATTN: SOSAC-ESL
Building 35, 1C Tree Road
McAlester, OK 74501-9053
DSN 956-8741
Comm (918) 420-8741
fax 8503
email Clifford.Doyle@dac.army.mil

Chapter 4

Protective Barriers

Protective barriers are used to define the physical limits of an installation, activity, or area. Barriers restrict, channel, or impede access and are fully integrated to form a continuous obstacle around the installation. They are designed to deter the worst-case threat. The barriers should be focused on providing assets with an acceptable level of protection against a threat.

Overview

4-1. Protective barriers form the perimeter of controlled, limited, and exclusion areas. Utility areas (such as water sources, transformer banks, commercial power and fuel connections, heating and power plants, or air-conditioning units) may require these barriers for safety standards. Protective barriers consist of two major categories—natural and structural.

- Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.
- Structural protective barriers are man-made devices (such as fences, walls, floors, roofs, grills, bars, roadblocks, signs, or other construction) used to restrict, channel, or impede access.

4-2. Barriers offer important benefits to a physical-security posture. They create a psychological deterrent for anyone thinking of unauthorized entry. They may delay or even prevent passage through them. This is especially true of barriers against forced entry and vehicles. Barriers have a direct impact on the number of security posts needed and on the frequency of use for each post.

4-3. Barriers cannot be designed for all situations. Considerations for protective structural barriers include the following:

- Weighing the cost of completely enclosing large tracts of land with significant structural barriers against the threat and the cost of alternate security precautions (such as patrols, MWD teams, ground sensors, electronic surveillance, and airborne sensors).
- Sizing a restricted area based on the degree of compartmentalization required and the area's complexity. As a rule, size should be kept to a minimum consistent with operational efficiency. A restricted area's size may be driven by the likelihood of an aggressor's use of certain tactics. For example, protecting assets from a vehicle bomb often calls for a substantial explosives standoff distance. In these cases, mitigating the vehicle bomb would often be more important than minimizing the restricted area to the extent necessary for operational efficiency. Protective barriers should be established for—
    - Controlling vehicular and pedestrian traffic flow.

- Providing entry-control points where ID can be checked.
- Defining a buffer zone for more highly classified areas.
- Precluding visual compromise by unauthorized individuals.
- Delaying forced entry.
- Protecting individual assets.

4-4. If a secured area requires a limited or exclusion area on a temporary or infrequent basis, it may not be possible to use physical structural barriers. A temporary limited or exclusion area may be established where the lack of proper physical barriers is compensated for by additional security posts, patrols, and other security measures during the period of restriction. Temporary barriers (including temporary fences, coiled concertina wire, and vehicles) may be used. Barriers are not the only restrictive element, and they may not always be necessary. They may not be ideal when working with limited or exclusion areas or when integrated with other controls.

4-5. Because barriers can be compromised through breaching (cutting a hole through a fence) or by nature (berms eroded by the wind and rain), they should be inspected and maintained at least weekly. Guard-force personnel should look for deliberate breaches, holes in and under barriers, sand dunes building up against barriers, and the proper functioning of locks.

FENCING

4-6. Three types of fencing are authorized for use in protecting restricted areas—chain link, barbed wire, and barbed tape or concertina. The type used for construction depends primarily on the threat and the degree of permanence. It may also depend on the availability of materials and the time available for construction. Fencing may be erected for other uses besides impeding personnel access. It can impede observation, can serve as a means to defeat standoff-weapon systems (such as rocket-propelled grenades [RPGs]), and can serve as a barrier to hand-thrown weapons (such as grenades and firebombs).

4-7. Generally, chain-link fencing will be used for protecting permanent limited and exclusion areas. All three types of fencing may be used to augment or increase the security of existing fences that protect restricted areas. Examples would be to create an additional barrier line, to increase existing fence height, or to provide other methods that effectively add to physical security. It is important to recognize that fencing provides very little delay when it comes to motivated aggressors, but it can act as a psychological deterrent.

Chain link

4-8. Chain-link fence (including gates) must be constructed of 6-foot material, excluding the top guard. Fence heights for conventional arms and ammunition security must be 6 feet for standard chain-link, wire-mesh fencing. Chain-link fences must be constructed with 9-gauge or heavier wire. They must be galvanized with mesh openings not larger than 2 inches per side and have twisted and barbed selvages at the top and the bottom. The wire must be taut and securely fastened to rigid metal or reinforced-concrete posts set in concrete. It must reach within 2 inches of hard ground or pavement. On soft ground, it must reach below the surface deep enough to compensate for shifting soil or sand. Materials and construction must meet with the US Army Corps of Engineers (USACE) guide specifications shown in the USACE Standard (STD) 872-90 series. Weaknesses in the chain-link fence occur as a result of weather (rusting) or failure to keep it fastened to the post that affects the desired

tightness. Damage to the fence and fence fabric may be the result of allowing vegetation and trees to grow on or near the fence. The interaction between the fence and the overgrowth often leads to fence damage and reduces the integrity and continuity of the fence as a perimeter boundary and barrier. The perimeter fence is the most obvious protective measure. A well-maintained fence indicates that the asset owner is dedicated to physical security.

Barbed Wire

4-9. Standard barbed wire is twisted, double-strand, 13.5-gauge wire, with four-point barbs spaced an equal distance apart. Barbed-wire fencing (including gates) intended to prevent human trespassing should not be less than 6 feet high and must be affixed firmly to posts not more than 6 feet apart. The distance between strands should not exceed 6 inches, and at least one wire should be interlaced vertically and midway between posts. The ends must be staggered or fastened together, and the base wire must be picketed to the ground.

Barbed Tape OR CONCERTINA

4-10. A barbed-taped obstacle (BTO) is fabricated from 0.025-inch stainless steel and is available in 24-, 30-, 40-, and 60-inch-diameter coils. The barbs shall have a minimum length of 1.2 inches, and the barb cluster's width shall be 1.21 inches. A BTO deploys tangle-free for fast installation. It may be recovered and used again. Fifty feet (plus or minus 2 inches) can be covered by 101 coil loops. Handling barbed tape requires the use of heavy barbed-tape gauntlets instead of standard barbed-wire gauntlets.

Barbed-Tape Concertina

4-11. Barbed-tape concertina (standard concertina barbed tape) is a commercially manufactured wire coil of high-strength-steel barbed wire that is clipped together at intervals to form a cylinder. When opened, it is 50 feet long and 3 feet in diameter. When used as the perimeter barrier for a restricted area, the concertina must be laid between poles with one roll on top of another or in a pyramid arrangement (with a minimum of three rolls).

4-12. Reinforced barbed-tape concertina consists of a single strand of spring-steel wire and a single strand of barbed tape. The sections between barbs of the barbed tape are securely clinched around the wire. Each coil is about 37 1/2 inches in diameter and consists of 55 spiral turns connected by steel clips to form a cylindrical diamond pattern when extended to a coil length of 50 feet. One end turn is fitted with four bundling wires for securing the coil when closed and each end turn is fitted with two steel carrying loops. The concertina extends to 50 feet without permanent distortion. When released, it can be retracted into a closed coil.

4-13. When possible, a top guard should be constructed on all perimeter fences and may be added on interior enclosures for additional protection. A top guard is an overhang of barbed wire or tape along the top of a fence, facing outward and upward at about a 45-degree angle. Placing barbed wire or tape above it can further enhance the top guard. Top-guard supporting arms will be permanently affixed to the top of fence posts to increase the overall height of the fence by at least 1 foot. (Due to liability issues in some locations, the top guards will not be allowed to face outward where the fence is adjacent to public areas.) Three strands of barbed wire spaced 6 inches apart must be installed on the supporting arms. The number of strands of wire or tape may be increased when required. The top guard of fencing

adjoining gates may range from a vertical height of 18 inches to the normal 45-degree outward protection but only for sufficient distance along the fence to open the gates adequately. Bottom and top tension wires should be used in lieu of fence rails. A concrete sill may be cast at the bottom of the fence to protect against soil erosion. A bottom rail is used on high-security fences to prevent intruders from lifting the fence.

Gates and Entrances

4-14. The number of gates and perimeter entrances must be the minimum required for safe and efficient operation of the facility. Active perimeter entrances must be designed so that the guard force maintains full control. Semiactive entrances, such as infrequently used vehicular gates, must be locked on the inside when not in use. When closed, gates and entrances must provide a barrier structurally comparable to their associated barriers. Care must be afforded against the ability to crawl under gates. Top guards, which may be vertical, are required for all gates.

Triple-Standard Concertina (TSC) Wire

4-15. This type of fence uses three rolls of stacked concertina. One roll will be stacked on top of two rolls that run parallel to each other while resting on the ground, forming a pyramid. In many situations, this fence has been used effectively in place of a chain-link fence. (If perimeter fencing consists of TSC, a top guard is not feasible.)

Tangle-Foot Wire

4-16. Barbed wire or tape may be used in appropriate situations to construct a tangle-foot obstruction either outside a single perimeter fence or in the area between double fences to provide an additional deterrent to intruders. The wire or tape should be supported on short metal or wooden pickets spaced at irregular intervals of 3 to 10 feet and at heights between 6 and 12 inches. The wire or tape should be crisscrossed to provide a more effective obstacle. The space and materials available govern the depth of the field.

Aircraft Cable

4-17. Although not used very often, aircraft cable can be used as a temporary barrier. Refer to FM 5-34 for information required for determining the barrier's strength. The barrier is created using wire rope. Clips are spaced six times the diameter of the wire rope. Aircraft cable (deployed as described above or attached to a chain-link fence) can also be made to act as a barrier to moving vehicles. To do so, the cable must be anchored into the ground at both ends at about 200-foot intervals (see TM 5-853-1).

Utility Openings

4-18. Sewers, air and water intakes and exhausts, and other utility openings of 10 inches or more in diameter that pass through perimeter barriers must have security measures equivalent to that of the perimeter (see TM 5-820-4). Specific requirements of various openings are discussed below:

- Manhole covers 10 inches or more in diameter must be secured to prevent unauthorized

opening. They may be secured with locks and hasps, by welding them shut, or by bolting them to their frame. Ensure that hasps, locks, and bolts are made of materials that resist corrosion. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available.

- Drainage ditches, culverts, vents, ducts, and other openings that pass through a perimeter and that have a cross-sectional area greater than 96 square inches and whose smallest dimension is greater than 6 inches will be protected by securely fastened welded bar grilles (refer to TM 5-853-3, Figure 8-1). As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. Ensure that any addition of grilles or pipes to culverts or other drainage structures is coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.

Other Perimeter Barriers

4-19. Buildings less than two stories high that form part of a perimeter must have a top guard along the outside edge to deny access to the roof. When using masonry walls as part of a perimeter barrier, they must be at least 7 feet high and have a barbed-wire top guard. The top guard should be sloped outward at a 45-degree angle and carry at least three strands of barbed wire. This will increase the vertical height of the barrier by at least 1 foot.

4-20. Protect windows, active doors, and other designated openings by securely fastening bars, grilles, or chain-link screens. Fasten window barriers from the inside. If hinged, the hinges and locks must be on the inside. Building elements that provide delay against forced entry have stringent requirements. These elements should be designed according to TM 5-853-1.

Security TowerS

4-21. It is not acceptable to observe a perimeter from towers only. However, all towers should be located to provide maximum observation and should be constructed for protection from small-arms fire.

4-22. Mobile towers are useful in some temporary situations such as a large, open storage area where receiving and storing activities take place. All facilities using towers must have a support force available for emergencies. Tower personnel should be rotated at frequent intervals.

4-23. The height of a tower increases the range of observation during daylight hours and at night with artificial illumination. However, during inclement weather and during a blackout, towers lose this advantage and must be supplemented by on-ground observation.

4-24. The following considerations should be made when planning for the use of towers:

- Hardening the tower against small-arms effects by using sandbags, salvaged armor, or commercially fabricated bullet-resistant construction. This may require strengthening the tower supports, which should be performed only under the supervision of an engineer. The level of protection required must equate to the threat level identified during the IPB or the military decision-making process (MDMP). The best approach is to design for the worst identified threat rather than to try and modify the tower at a later date on short notice.

- Installing communications and alarm systems, both audible and visual (primary and alternate).
- Using appropriate surveillance, target-acquisition, and night-observation (STANO) equipment with the tower and perimeter barriers being surveilled. Infrared (IR) items may be especially valuable. Considerations for the selection and use of STANO equipment must be made while evaluating the effects of perimeter protective lighting.
- Providing security lighting for route protection to the tower. Security lighting also allows for support of the guard force entering or exiting the perimeter.
- Ensuring that the tower's height is determined according to the area of observation.
- Ensuring that towers have overlapping, mutually supporting fields of observation and fire.
- Providing towers with a backup fortified defensive fighting position, as appropriate.

Installation Entrances

4-25. The number of installation or activity gates and perimeter entrances in active use should be limited to the minimum number required for safe and efficient operations. When necessary, install vehicle barriers in front of vehicle gates. Security lighting should be considered at entry points (see Chapter 5). Refer to TM 5-853-1 for the application and selection of these barriers.

4-26. Plans to use guards for controlling entry to an installation or activity must be predetermined based on the threat conditions (THREATCON). The construction of the guard post must be included in the security plan.

Perimeter Entrances

4-27. Active perimeter entrances should be designated so that security forces maintain full control without an unnecessary delay in traffic. This is accomplished by having sufficient entrances to accommodate the peak flow of pedestrian and vehicular traffic and having adequate lighting for rapid and efficient inspection. When gates are not operational during nonduty hours, they should be securely locked, illuminated during hours of darkness, and inspected periodically by a roving patrol. Additionally, warning signs should be used to warn drivers when gates are closed. Doors and windows on buildings that form a part of the perimeter should be locked, lighted, and inspected.

Entry-Control Stations

4-28. Entry-control stations should be provided at main perimeter entrances where security personnel are present. Considerations for construction and use should be based on the information outlined in USACE STD 872-50-01.

4-29. Entry-control stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches. Additional considerations at entry-control stations include—

- Establishing a holding area for unauthorized vehicles or those to be inspected further. A turnaround area should be provided to keep from impeding other traffic.
- Establishing control measures such as displaying a decal on the window or having a specially marked vehicle.

4-30. Entry-control stations that are manned 24 hours each day should have interior and exterior

lighting, interior heating (where appropriate), and a sufficient glassed area to afford adequate observation for personnel inside. Where appropriate, entry-control stations should be designed for optimum personnel ID and movement control. Each station should also include a telephone, a radio, and badge racks (if required).

4-31. Signs should be erected to assist in controlling authorized entry, to deter unauthorized entry, and to preclude accidental entry. Signs should be plainly displayed and be legible from any approach to the perimeter from a reasonable distance. The size and coloring of a sign, its letters, and the interval of posting must be appropriate to each situation.

4-32. Entry-control stations should be hardened against attacks according to the type of threat. The methods of hardening may include—

- Reinforced concrete or masonry.
- Steel plating.
- Bullet-resistant glass.
- Sandbags, two layers in depth.
- Commercially fabricated, bullet-resistant building components or assemblies.

Warning Signs

4-33. A significant amount of warning signs should be erected to ensure that possible intruders are aware of entry into restricted areas. Warning signs augment control signs. They warn intruders that the area is restricted and that trespassing may result in the use of deadly force.

4-34. Warning signs should be installed along the limited area's physical barriers and at each entry point where they can be seen readily and understood by anyone approaching the perimeter. In areas where English is one of two or more languages commonly spoken, warning signs must contain the local language in addition to English. The wording on the signs will denote warning of a restricted area. The signs should be posted at intervals of no more than 100 feet. They must not be mounted on fences equipped with intrusion-detection equipment. Additionally, the warning signs prescribed in AR 190-13 should be posted at all entrances to limited, controlled, and exclusion areas. See Chapter 7 for more details.

Other Signs

4-35. Signs setting forth the conditions of entry to an installation or area should be plainly posted at all principal entrances. The signs should be legible under normal conditions at a distance not less than 50 feet from the point of entry. Such signs should inform the entrant of the provisions (search of the person, the vehicle, packages, and so forth) or prohibitions (such as against cameras, matches, and lighters and entry for reasons other than official business) that may be prescribed by the installation commander.

4-36. Signs or notices legibly setting forth the designation of restricted areas and provisions of entry should be plainly posted at all entrances and at other points along the perimeter line as necessary. The wording of these signs or notices is prescribed in AR 190-13.

Installation Perimeter Roads and Clear Zones

4-37. When the perimeter barrier encloses a large area, an interior all-weather perimeter road should be provided for security-patrol vehicles. Clear zones should be maintained on both sides of the perimeter barrier to provide an unobstructed view of the barrier and the ground adjacent to it. Roads within the clear zone should be as close to the perimeter barrier as possible without interfering with it. The roads should be constructed to allow effective road barriers to deter motor movement of unauthorized personnel during mobilization periods.

4-38. Clear zones should be kept clear of weeds, rubbish, or other material capable of offering concealment or assistance to an intruder attempting to breach the barrier. A clear zone of 20 feet or more should exist between the perimeter barrier and exterior structures, parking areas, and natural or man-made features. When possible, a clear zone of 50 feet or more should exist between the perimeter barrier and structures within the protected area, except when a building's wall constitutes part of the perimeter barrier. Ammunition supply points (ASPs) will have clear zones 12 feet outside of the ASP and 30 feet inside, and the vegetation will not exceed 8 inches (4 inches for high-threat and highly controlled areas). Refer to AR 190-11 and DOD 0-2000.12-H, Appendix EE, for further information.

4-39. When it is impossible to have adequate clear zones because of property lines or natural or man-made features, it may be necessary to increase the height of the perimeter barrier, increase security-patrol coverage, add more security lighting, or install an intrusion-detection device along that portion of the perimeter.

4-40. When considering the construction of a new site or perimeter, ensure that the plans include a fence located well inside the property line, thus permitting control of enough space outside the fence to maintain at least a minimal clear zone. The following considerations apply:

- On a large installation (such as a proving ground), it is unreasonable to construct an expensive perimeter fence and keep it under constant observation. Such an installation is usually established in a sparsely inhabited area. Its comparative isolation and the depth of the installation give reasonable perimeter protection. Under these circumstances, it is usually sufficient to post warning signs or notices, reduce access roads to a minimum, and periodically patrol the area between the outer perimeter and the conventionally protected vital area of the installation.
- An alternative to erecting new or replacing old chain-link fence involving an entire installation perimeter is to relocate or isolate the sensitive area or item by—
    - Relocating the item within a safe perimeter.
    - Consolidating the item with other items.
    - Erecting a chain-link fence (regulations permitting) around individual assets rather than the installation's perimeter.

Arms-Facility Structural Standards

4-41. It is next to impossible to build a protective barrier that cannot be penetrated by a human or heavy armor. Therefore, as opposed to protecting a facility using only one barrier, enhance security by using a combination of barriers to increase delay. Multiple barriers also cause aggressors to expend more energy trying to breach all of the barriers. They also provide the appearance of additional security and may further deter some aggressors.

4-42. The interest of security must be kept in mind when constructing walls, ceilings, floors, and roofs. Facilities that house arms and ammunition are constructed as security barriers in the interest of deterring and delaying penetration. Construction guidelines for arms facilities are outlined in AR 190-11. AR 190-11 requires coordination with the engineer office, the safety office, the provost marshal office (PMO), or the security-force office when definitive drawings and specifications for new construction or upgrades or modifications of AA&E storage structures are proposed. This coordinated effort ensures that safety and physical-security requirements are met. AR 190-11 also addresses waivers and exceptions for AA&E storage structures, as well as the requirements for a tactical (training or operational) or shipboard environment. Waivers and exceptions are not discussed in this manual. The following guidelines are provided for securing AA&E in tactical and shipboard environments:

- The criteria and standards for protecting AA&E will be developed by the major Army command (MACOM) according to AR 190-11.
- The deploying commander will establish and enforce procedures for securing deployed AA&E based on the assessment of the threat, the objectives, the location, and the duration of the deployment.
- The AA&E in the tactical environment will be secured at all times.
- The AA&E will be under continuous positive control.
- Persons charged with the custody of AA&E will have the capability to sound the alarm if a forceful theft is attempted.
- A response force will be available to protect the AA&E.
- A system of supervisory checks will be established to ensure that all personnel comply with security measures. Supervisory checks of the AA&E holding area will be made to ensure that the AA&E being guarded have not been tampered with.
- All officers, noncommissioned officers (NCOs), or civilian equivalents will closely monitor the control of ammunition and explosives during field training or range firing.
- Selection of personnel to perform guard duties at AA&E holding areas will be closely monitored by commanders to ensure that only responsible individuals are assigned duties.

Chapter 7

Access Control

Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access-control system must be established and maintained to preclude unauthorized entry. Effective access-control procedures prevent the introduction of harmful devices, materiel, and components. They minimize the misappropriation, pilferage, or compromise of materiel or recorded information by controlling packages, materiel, and property movement. Access-control rosters, personal recognition, ID cards, badge-exchange procedures, and personnel escorts all contribute to an effective access-control system.

DESIGNATED Restricted Areas

7-1. The installation commander is responsible for designating and establishing restricted areas. A restricted area is any area that is subject to special restrictions or controls for security reasons. This does not include areas over which aircraft flight is restricted. Restricted areas may be established for the following:

- The enforcement of security measures and the exclusion of unauthorized personnel.
- Intensified controls in areas requiring special protection.
- The protection of classified information or critical equipment or materials.

Degree of Security

7-2. The degree of security and control required depends on the nature, sensitivity, or importance of the security interest. Restricted areas are classified as controlled, limited, or exclusion areas.

- A controlled area is that portion of a restricted area usually near or surrounding a limited or exclusion area. Entry to the controlled area is restricted to personnel with a need for access. Movement of authorized personnel within this area is not necessarily controlled since mere entry to the area does not provide access to the security interest. The controlled area is provided for administrative control, for safety, or as a buffer zone for in-depth security for the limited or exclusion area. The commander establishes the control of movement.
- A limited area is a restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access within limited areas.
- An exclusion area is a restricted area containing a security interest. Uncontrolled movement permits direct access to the item.

7-3. The security protection afforded by a restricted area pertains particularly to subversive-activity control; that is, protection against espionage, sabotage, or any such action adversely affecting national defense. Within this context, the designation "restricted area" is not applicable to an area solely for protection against common pilferage or misappropriation of property or material that is not classified or not essential to national defense. For example, an area devoted to the storage or use of classified documents, equipment, or materials should be designated as a restricted area to safeguard against espionage. An installation communications center should also be so designated to safeguard against sabotage. On the other hand, a cashier's cage or an ordinary mechanic's tool room should not be so designated, although the commander may impose controls to access. This may be a simple matter of posting an "off limits to unauthorized personnel" sign. The PM or the physical-security manager acts as an advisor to the commander. In his recommendations, he must consider evaluating the purpose of designating a restricted area and coordinating with the intelligence officer and the staff judge advocate (SJA).

7-4. A restricted area must be designated in writing by the commander and must be posted with warning signs according to AR 190-13. In areas where English is one of two or more languages commonly spoken, warning signs will be posted in English and in the local language (see Figure 7-1 below).

7-5. An installation may have varying degrees of security. It may be designated in its entirety as a restricted area, with no further restrictions; or it may be subdivided into controlled, limited, or exclusion areas with restrictions of movement and specific clear zones. Figure 7-2 depicts a simplified restricted area and the degrees of security.

RESTRICTED AREA

THIS (INSTALLATION OR ACTIVITY) HAS BEEN DECLARED A RESTRICTED AREA BY AUTHORITY OF (TITLE, COMMANDING GENERAL OR COMMANDING OFFICER) IN ACCORDANCE WITH THE PROVISIONS OF THE DIRECTIVE ISSUED BY THE SECRETARY OF DEFENSE ON 20 AUGUST 1954, PURSUANT TO THE PROVISIONS OF SECTION 21, INTERNAL SECURITY ACT OF 1950. UNATHORIZED ENTRY IS PROHIBITED.

ALL PERSONS AND VEHICLES ENTERING HEREIN ARE LIABLE TO SEARCH. PHOTOGRAPHING OR MAKING NOTES, DRAWINGS, MAPS, OR GRAPHIC REPRESENTATIVES OF THIS AREA OR ITS ACTIVITIES ARE PROHIBITED UNLESS SPECIFICALLY AUTHORIZED BY THE COMMANDER. ANY SUCH MATERIAL FOUND IN THE POSSESSION OF UNAUTHORIZED PERSONS WILL BE CONFISCATED.

Figure 7-1. Sample Restricted-Area Warning

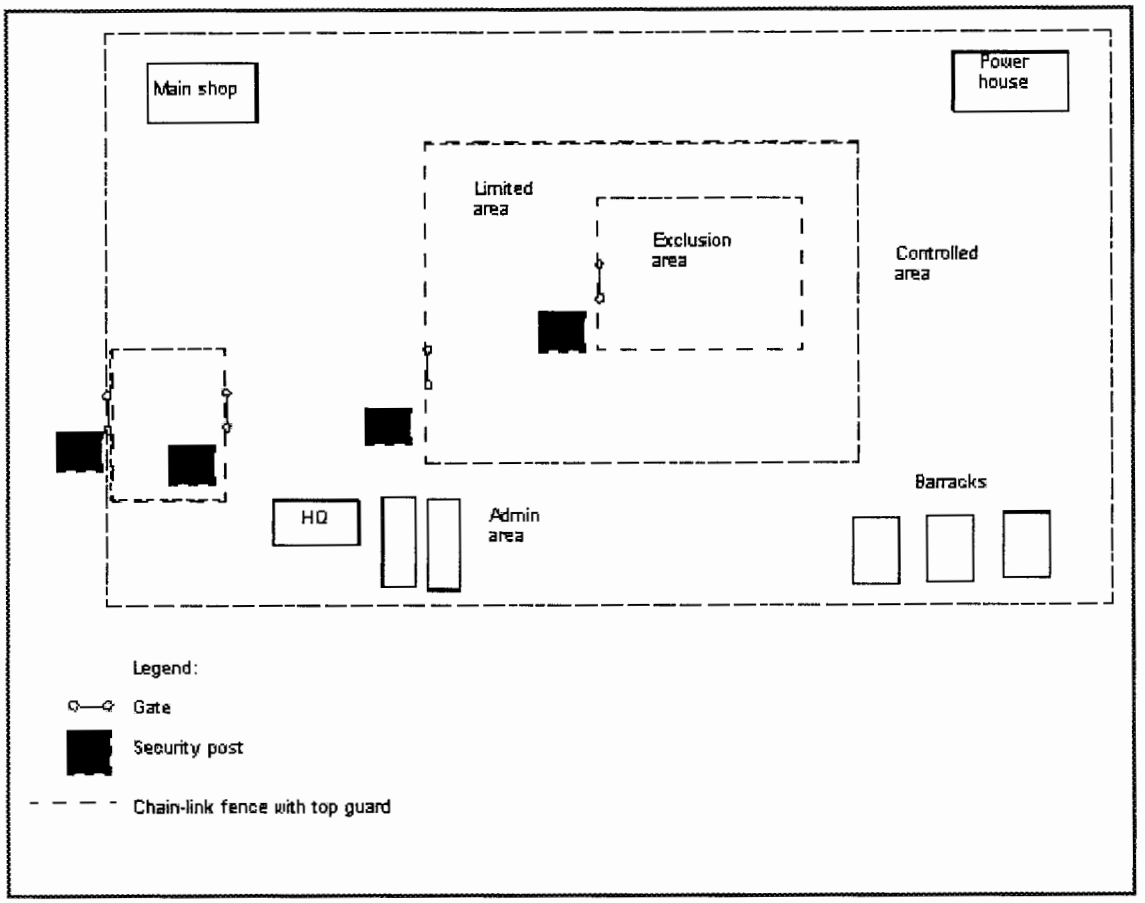


Figure 7-2. Schematic Diagram of a Simplified Restricted Area and the Degrees of Security

Considerations

7-6. There are other important considerations concerning restricted areas and their lines of division. These considerations include the following:

- A survey and analysis of the installation, its missions, and its security interests. This can determine immediate and anticipated needs that require protection. Anticipated needs are determined from plans for the future.
- The size and nature of the security interest being protected. Safes may provide adequate protection for classified documents and small items; however, large items may have to be placed within guarded enclosures.
- Some security interests are more sensitive to compromise than others. Brief observation or a simple act by an untrained person may constitute a compromise in some cases. In others, detailed study and planned action by an expert may be required.
- All security interests should be evaluated according to their importance. This may be indicated by a security classification such as confidential, secret, or top secret.
- Parking areas for privately owned vehicles (POVs) are established outside of restricted areas. Vehicle entrances must be kept at a minimum for safe and efficient control.
- Physical protective measures (such as fences, gates, and window bars) must be installed.

Employee Screening

7-7. Screening job applicants to eliminate potential acts of espionage and sabotage and other security risks is important in peacetime and is critical during a national emergency. Personnel screenings must be incorporated into standard personnel policies.

7-8. An applicant should be required to complete a personnel security questionnaire, which is then screened for completeness and used to eliminate undesirable applicants. A careful investigation should be conducted to ensure that the applicant's character, associations, and suitability for employment are satisfactory. The following sources may be helpful in securing employment investigative data:

- State and local police (including national and local police in overseas areas).
- Former employers.
- Public records.
- Credit agencies.
- Schools (all levels).
- References. (These references should include those names not furnished by the applicant. These are known as throw offs, and they are obtained during interviews of references furnished by applicants.)
- Others as appropriate. (These may include the FBI, the US Army Criminal Records Repository, and the Defense Investigative Agency).

7-9. Medical screening considerations should be made (based on an applicant's position [such as a guard]) to evaluate physical and mental stamina. Once an applicant has been identified for employment, he is placed on an access-control roster.

Identification System

7-10. An ID system is established at each installation or facility to provide a method of identifying personnel. The system provides for personal recognition and the use of security ID cards or badges to aid in the control and movement of personnel activities.

7-11. Standard ID cards are generally acceptable for access into areas that are unrestricted and have no security interest. Personnel requiring access to restricted areas should be issued a security ID card or badge as prescribed in AR 600-8-14. The card's/badge's design must be simple and provide for adequate control of personnel.

7-12. A security ID card/badge system must be established for restricted areas with 30 or more employees per shift. Commanders may (at their discretion) authorize a card/badge system in restricted areas for less than 30 people.

ID Methods

7-13. Four of the most commonly used access-control ID methods are the personal-recognition system, the single-card or -badge system, the card- or badge-exchange system, and the multiple-card or -badge system.

Personal-Recognition System

7-14. The personal-recognition system is the simplest of all systems. A member of the security force

providing access control visually checks the person requesting entry. Entry is granted based on—

- The individual being recognized.
- The need to enter has been established.
- The person is on an access-control roster.

Single-Card or -Badge System

7-15. This system reflects permission to enter specific areas by the badge depicting specific letters, numbers, or particular colors. This system lends to comparatively loose control and is not recommended for high-security areas. Permission to enter specific areas does not always go with the need to know. Because the ID cards/badges frequently remain in the bearer's possession while off duty, it affords the opportunity for alteration or duplication.

Card- or Badge-Exchange System

7-16. In this system, two cards/badges contain identical photographs. Each card/badge has a different background color, or one card/badge has an overprint. One card/badge is presented at the entrance to a specific area and exchanged for the second card/badge, which is worn or carried while in that area. Individual possession of the second card/badge occurs only while the bearer is in the area for which it was issued. When leaving the area, the second card/badge is returned and maintained in the security area. This method provides a greater degree of security and decreases the possibility of forgery, alteration, or duplication of the card/badge. The levels of protection described in TM 5-853-1 require multiple access-control elements as the levels of protection increase. In the case of the badge exchange, this system counts as two access-control elements.

Multiple-Card or -Badge System

7-17. This system provides the greatest degree of security. Instead of having specific markings on the cards/badges denoting permission to enter various restricted areas, the multiple card/badge system makes an exchange at the entrance to each security area. The card/badge information is identical and allows for comparisons. Exchange cards/badges are maintained at each area only for individuals who have access to the specific area.

Mechanized/Automated Systems

7-18. An alternative to using guards or military police (MP) to visually check cards/badges and access rosters is to use building card-access systems or biometric-access readers. These systems can control the flow of personnel entering and exiting a complex. Included in these systems are—

- Coded devices such as mechanical or electronic keypads or combination locks.
- Credential devices such as magnetic-strip or proximity card readers.
- Biometric devices such as fingerprint readers or retina scanners.

7-19. Access-control and ID systems base their judgment factor on a remote capability through a routine discriminating device for positive ID. These systems do not require guards at entry points; they identify an individual in the following manner:

- The system receives physical ID data from an individual.
- The data is encoded and compared to stored information.
- The system determines whether access is authorized.
- The information is translated into readable results.

7-20. Specialized mechanical systems are ideal for highly sensitive situations because they use a controlled process in a controlled environment to establish the required database and accuracy. One innovative technique applied to ID and admittance procedures involves dimension comparisons. The dimension of a person's full hand is compared to previously stored data to determine entry authorization. Other specialized machine readers can scan a single fingerprint or an eye retina and provide positive ID of anyone attempting entry.

7-21. An all-inclusive automated ID and access-control system reinforces the security in-depth ring through its easy and rapid change capability. The computer is able to do this through its memory. Changes can be made quickly by the system's administrator.

7-22. The commercial security market has a wide range of mechanized and automated hardware and software systems. Automated equipment is chosen only after considering the security needs and the environment in which it operates. These considerations include whether the equipment is outdoors or indoors, the temperature range, and weather conditions. Assessment of security needs and the use of planning, programming, and budgeting procedures greatly assist a security manager in improving the security posture.

Card/Badge Specifications

7-23. Security cards/badges should be designed and constructed to meet the requirements of AR 600-8-14. Upon issuing a card/badge, security personnel must explain to the bearer the wear required and the authorizations allowed with the card/badge. This includes—

- Designation of the areas where an ID card/badge is required.
- A description of the type of card/badge in use and the authorizations and limitations placed on the bearer.
- The required presentation of the card/badge when entering or leaving each area during all hours of the day.
- Details of when, where, and how the card/badge should be worn, displayed, or carried.
- Procedures to follow in case of loss or damage of the card.
- The disposition of the card/badge upon termination of employment, investigations, or personnel actions.
- Prerequisites for reissuing the card/badge.

Visitor Identification and Control

7-24. Procedures must be implemented to properly identify and control personnel. This includes visitors presenting their cards/badges to guards at entrances of restricted areas. Visitors are required to stay with their assigned escort. Guards must ensure that visitors stay in areas relating to their visit; an uncontrolled visitor, although conspicuously identified, could acquire information for which he is not authorized. Foreign-national visitors should be escorted at all times.

7-25. Approval for visitors should be obtained at least 24 hours in advance (if possible). Where appropriate, the installation should prepare an agenda for the visitor and designate an escort officer. Measures must be in place to recover visitor cards/badges on the visit's expiration or when they are no longer required.

7-26. Physical-security precautions against pilferage, espionage, and sabotage require the screening, ID, and control of visitors. Further information about visiting requirements and procedures are found in ARs 12-15 and 381-20. Visitors are generally classed in the following categories:

- Persons with whom every installation or facility has business (such as suppliers, customers, insurance inspectors, and government inspectors).
- Individuals or groups who desire to visit an installation or facility for personal or educational reasons. Such visits may be desired by educational, technical, or scientific organizations.
- Individuals or groups specifically sponsored by the government (such as foreign nationals visiting under technical cooperation programs and similar visits by US nationals). Requests for visits by foreign nationals must be processed according to AR 380-10.
- Guided tours to selected portions of the installation in the interest of public relations.

7-27. The ID and control mechanisms for visitors must be in place. They may include the following:

- Methods of establishing the authority for admitting visitors and any limitations relative to access.
- Positive ID of visitors by personal recognition, visitor permit, or other identifying credentials. Contact the employer, supervisor, or officer in charge to validate the visit.
- The use of visitor registration forms. These forms provide a record of the visitor and the time, location, and duration of his visit.
- The use of visitor ID cards/badges. The cards/badges bear serial numbers, the area or areas to which access is authorized, the bearer's name, and escort requirements.

7-28. Individual groups entering a restricted area must meet specific prerequisites before being granted access. The following guidance is for group access into a restricted area:

Visitors

7-29. Before allowing visitors into a restricted area, contact the person or activity being visited. After verifying the visitor's identity, issue a badge, complete the registration forms, and assign an escort (if required). Visitors may include public-utility and commercial-service representatives.

Very Important Persons

7-30. The procedures for admitting very important persons (VIPs) and foreign nationals into restricted areas are contained in AR 12-15. Special considerations and coordination with the protocol office are necessary. A 24-hour advance notice is desirable for these requests, along with an agenda for the visit and the designation of an escort, if appropriate.

Civilians Working on Jobs Under Government Contract

7-31. To allow these personnel to conduct business in restricted areas, the security manager must coordinate with the procurement office. The security manager must also identify movement-control

procedures for these employees.

Cleaning Teams

7-32. Supervisors using cleaning teams must seek technical advice from the physical-security office on internal controls for each specific building. This may include providing escorts.

DOD Employees in Work Areas After Normal Operating Hours

7-33. Supervisors establish internal controls based on coordination with the security manager. They also notify security personnel of the workers' presence, type, and duration of work.

Enforcement Measures

7-34. The most vulnerable link in any ID system is its enforcement. Security forces must be proactive in performing their duties. A routine performance of duty will adversely effect even the most elaborate system. Positive enforcement measures must be prescribed to enhance security. Some of these measures may include—

- Designating alert and tactful security personnel at entry control points.
- Ensuring that personnel possess quick perception and good judgment.
- Requiring entry-control personnel to conduct frequent irregular checks of their assigned areas.
- Formalizing standard procedures for conducting guard mounts and posting and relieving security personnel. These measures will prevent posting of unqualified personnel and a routine performance of duty.
- Prescribing a uniform method of handling or wearing security ID cards/badges. If carried on the person, the card must be removed from the wallet (or other holder) and handed to security personnel. When worn, the badge will be worn in a conspicuous position to expedite inspection and recognition from a distance.
- Designing entry and exit control points of restricted areas to force personnel to pass in a single file in front of security personnel. In some instances, the use of turnstiles may be advisable to assist in maintaining positive control.
- Providing lighting at control points. The lighting must illuminate the area to enable security personnel to compare the bearer with the ID card/badge.
- Enforcing access-control measures by educating security forces and employees. Enforcement of access-control systems rests primarily with the security forces; however, it is essential that they have the full cooperation of the employees. Employees must be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where access is limited to a particular zone, employees must report unauthorized individuals to the security force.
- Positioning ID card/badge racks or containers at entry control points so that they are accessible only to guard-force personnel.
- Appointing a responsible custodian to accomplish control procedures of cards/badges according to AR 600-8-14. The custodian is responsible for the issue, turn in, recovery, and renewal of security ID cards/badges.

7-35. The degree of compromise tolerable in the ID system is in direct proportion to the degree of security required. The following control procedures are recommended for preserving the integrity of a

card/badge system:

- Maintenance of an accurate written record or log listing (by serial number) all cards and badges and showing those on hand, to whom they are issued, and their disposition (lost, mutilated, or destroyed).
- Authentication of records and logs by the custodian.
- A periodic inventory of records by a commissioned officer.
- The prompt invalidation of lost cards/badges.
- The conspicuous posting at security control points of current lists of lost or invalidated cards/badges.
- The establishment of controls within restricted areas to enable security personnel to determine the number of persons within the area.
- The establishment of the two-person rule (when required).
- The establishment of procedures to control the movement of visitors. A visitor-control record will be maintained and located at entry control points.

Sign/Countersign and Code word

7-36. This method of verifying identity is primarily used in a tactical environment. According to the local SOP, the sign/countersign or code-word procedures must be changed immediately if compromised.

Duress Code

7-37. The duress code is a simple word or phrase used during normal conversation to alert other security personnel that an authorized person is under duress. A duress code requires planning and rehearsal to ensure an appropriate response. This code is changed frequently to minimize compromise.

Access-Control Rosters

7-38. Admission of personnel to a restricted area is granted to those identified and listed on an access-control roster. Pen-and-ink changes may be made to the roster. Changes are published in the same manner as the original roster.

7-39. Rosters are maintained at access control points. They are kept current, verified, and accounted for by an individual designated by the commander. Commanders or their designated representatives authenticate the rosters. Admission of persons other than those on the rosters is subject to specific approval by the security manager. These personnel may require an escort according to the local SOP.

Methods of Control

7-40. There are a number of methods available to assist in the movement and control of personnel in limited, controlled, and restricted areas. The following paragraphs discuss the use of escorts and the two-person rule:

Escorts

7-41. Escorts are chosen because of their ability to accomplish tasks effectively and properly. They possess knowledge of the area being visited. Escorts may be guard-force personnel, but they are normally personnel from the area being visited. Local regulations and SOPs determine if a visitor requires an escort while in the restricted area. Personnel on the access list may be admitted to restricted areas without an escort.

Two-person Rule

7-42. The two-person rule is designed to prohibit access to sensitive areas or equipment by a lone individual. Two authorized persons are considered present when they are in a physical position from which they can positively detect incorrect or unauthorized procedures with respect to the task or operation being performed. The team is familiar with applicable safety and security requirements, and they are present during any operation that affords access to sensitive areas or equipment that requires the two-person rule. When application of the two-person rule is required, it is enforced constantly by the personnel who constitute the team.

7-43. The two-person rule is applied in many other aspects of physical-security operations, such as the following:

- When uncontrolled access to vital machinery, equipment, or materiel might provide opportunity for intentional or unintentional damage that could affect the installation's mission or operation.
- When uncontrolled access to funds could provide opportunity for diversion by falsification of accounts.
- When uncontrolled delivery or receipt for materials could provide opportunity for pilferage through "short" deliveries and false receipts.
- When access to an arms or ammunition storage room could provide an opportunity for theft. Keys should be issued so that at least two people must be present to unlock the locks required under the provisions of AR 190-11.

7-44. The two-person rule is limited to the creativity of the PM and the physical-security manager. They should explore every aspect of physical-security operations in which the two-person rule would provide additional security and assurance and include all appropriate recommendations and provisions of the physical-security plan. An electronic-entry control system may be used to enforce the two-person rule. The system can be programmed to deny access until two authorized people have successfully entered codes or swiped cards.

Security Controls of Packages, Personal PropertY, and Vehicles

7-45. A good package-control system helps prevent or minimize pilferage, sabotage, and espionage. The local SOP may allow the entry of packages with proper authorization into restricted areas without inspection. A package-checking system is used at the entrance gate. When practical, inspect all outgoing packages except those properly authorized for removal. When a 100 percent inspection is impractical, conduct frequent unannounced spot checks. A good package-control system assists in the movement of authorized packages, material, and property.

7-46. Property controls are not limited to packages carried openly, but they include the control of anything that could be used to conceal property or material. Personnel should not be routinely searched except in unusual situations. Searches must be performed according to the local SOP.

7-47. All POVs on the installation should be registered with the PM or the installation's physical-security office. Security personnel should assign a temporary decal or other temporary ID tag to visitors' vehicles to permit ready recognition. The decal or the tag should be distinctly different from that of permanent-party personnel.

7-48. When authorized vehicles enter or exit a restricted area, they undergo a systematic search, including (but not limited to) the—

- Vehicle's interior.
- Engine compartment.
- External air breathers.
- Top of the vehicle.
- Battery compartment.
- Cargo compartment.
- Undercarriage.

7-49. The movement of trucks and railroad cars into and out of restricted areas should be supervised and inspected. Truck and railroad entrances are controlled by locked gates when not in use and are manned by security personnel when unlocked. The ID cards/badges are issued to operators to ensure proper ID and registration for access to specific loading and unloading areas.

7-50. All conveyances entering or leaving a protected area are required to pass through a service gate manned by security forces. Drivers, helpers, passengers, and vehicle contents must be carefully examined. The examination may include—

- Appropriate entries in the security log (including the date, operator's name, load description, and time entered and departed).
- A check of the operator's license.
- Verification of the seal number with the shipping document and examination of the seal for tampering.

7-51. Incoming trucks and railroad cars must be assigned escorts before they are permitted to enter designated limited or exclusion areas. Commanders should establish published procedures to control the movement of trucks and railroad cars that enter designated restricted areas to discharge or pick up cargo (escorts will be provided when necessary).

7-52. The best control is provided when all of these elements are incorporated into access-control procedures. Simple, understandable, and workable access-control procedures are used to achieve security objectives without impeding operations. When properly organized and administered, access-control procedures provide a method of positively identifying personnel who have the need to enter or leave an area.

TACTICAL-ENVIRONMENT CONSIDERATIONS

7-53. Access-control procedures during tactical operations may establish additional challenges for the commander. In some instances, the commander cannot provide a perimeter barrier (such as a fence) based on METT-TC. Commanders are still required to provide security measures for restricted areas, although they may not always have the necessary assets. Early-warning systems and the use of guards become crucial. A restricted area may become a requirement without prior notice during an operation.

Figure 7-3 and Figure 7-4 below are examples of temporary tactical restricted and exclusion areas.

7-54. Commanders must plan for these considerations when developing their budget. Funding must be requested and set aside to support physical-security requirements during tactical operations. Resources will not always be available; therefore, commanders must implement procedures that support access-control measures. Improvising will become common practice to overcome shortfalls concerning access-control equipment in the field.

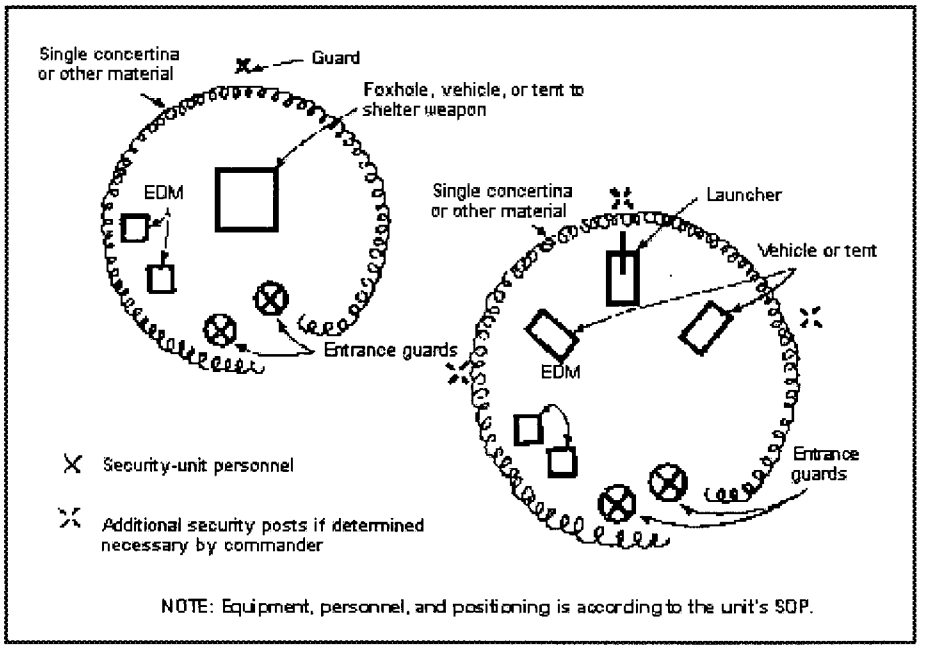


Figure 7-3. Sample Layout of Temporary Tactical Restricted Areas

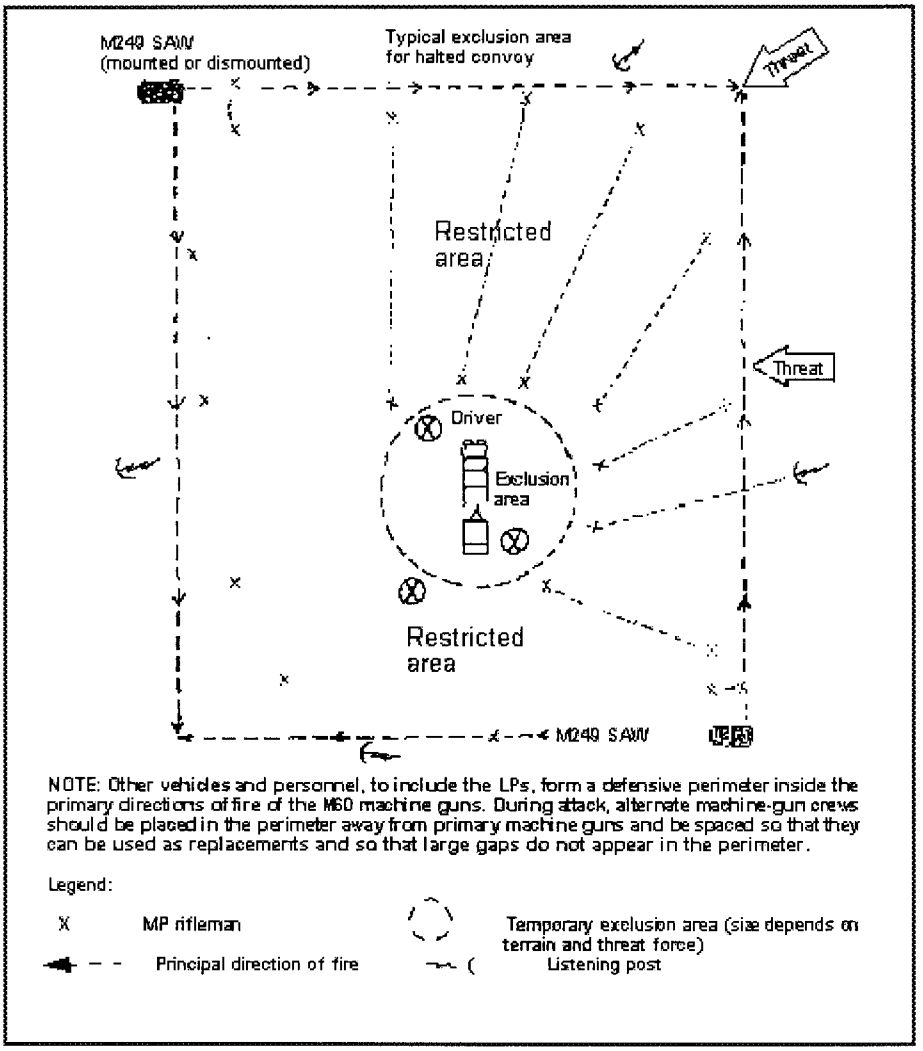


Figure 7-4. Sample Layout for a Temporary Tactical Exclusion Area