# Preface

## Introduction

This field manual sets forth guidance for all people responsible for physical security. It's the basic reference for training security personnel. It also covers requesting additional equipment and manpower.

The two primary concerns of this manual are prevention and protection. Both serve the security interest of people, equipment, and property. To be most effective, this interest must be supported at all staff and command levels. This support must be unified.

## Physical Security Responsibilities

Major responsibilities in physical security exist at Department of the Army (DA) through local command levels (AR 190-13). These are as follows:

- Law Enforcement Division, Deputy Chief of Staff for Personnel—DA policy and procedures, Army-wide guidance, assistance, and development of physical security equipment.
- Assistant Chief of Staff for Intelligence—assessment of counterintelligence in physical security plans and programs.
- Chief of Engineers—final technical review and approval of plans and specifications for installing intrusion detection systems estimated to cost more than $5,000.
- Local Commanders—all reasonable precautions are taken to safeguard the people and property of their commands. Each commander must designate a physical security manager to plan, formulate, and coordinate physical security matters (AR 190-13). In short, the physical security manager formulates the plan; supervises physical security inspections, coordinates required support

(personnel and equipment); and reviews all plans for new construction or modification to insure all possible physical security safeguards are built in, and deficiencies eliminated or minimized. Normally, he is also responsible for physical security education programs for all personnel (chapter 3).

## Arrangement of This Manual

You will find the arrangement, of this manual different from that of the previous FM 19-30. It should make physical security easier to understand and easier to apply. There is a brief introduction to each major area; and critical points are highlighted throughout for rapid review or scanning for important items. The guidance permits you the flexibility so critical to effective application (based on location, size of installation, etc.). There are also new checklists for standard security operations in CONUS and overseas.

## How To Use It

This manual is to be used with the policy, doctrine, and training set forth in those references listed in appendix V.

## Considerations

Perfect or absolute security is always our goal. However, a state of absolute security can never be attained. There is no object so well protected that it cannot be stolen, damaged, destroyed, or observed by unfriendly eyes. The purpose, then, of physical security is to make access so difficult that an intruder will hesitate to attempt penetration, or to provide for his apprehension should he be successful. Security must be built upon a system of defense in depth or upon accumulated delay time.

Physical security is only part of the overall defense of an installation. Defense against direct enemy attack and natural disasters must be blended into a system that includes physical security. This blended effort begins with planning.

It is not economically possible or theoretically necessary for installations and activities of every kind and character to achieve the same degree of protection. How much protection is warranted in any particular case depends on certain factors. If the installation is highly critical and highly vulnerable, an extensive physical security program is necessary.

All military installations are valuable in some degree to the national defense structure. Some are more valuable than others. To determine the degree of importance, the effect of partial or complete loss must be calculated. If the influence on the national defense effort is great, then criticality y is high. Within each installation, certain facilities are essential to the mission of that installation. Facilities such as primary and auxiliary power sources are highly critical.

Because of the monetary and manpower costs of physical protection, many commanders will not be able to achieve maximum protection for the entire installation or activity. Therefore, the specific criticality and vulnerability of various areas must be determined, and available resources divided accordingly. Special protection is thus provided for the most critical and vulnerable areas, while areas of less importance and susceptibility are given less protection.

A highly critical area is one in which partial or complete loss would have an immediate and serious impact on the ability of an installation or activity to perform its mission for a considerable time. The relative criticality of such an area may have no direct relationship to its size or whether it produces an end product. This must be determined upon the basis of its importance to the

installation or activity as a whole.

Vulnerability depends on the hazards that could cause sufficient loss, damage, or destruction to influence operation of the activity or installation. If one or more hazards exist that could easily achieve this result, relative vulnerability is high. As it becomes more unlikely that existing hazards will interfere with the mission, vulnerability becomes lower.

## Applicability

All of the general considerations previously discussed are equally applicable to units and other operations. They are applicable to port and harbor security; to docks and wharves; to security escort operations; to POL distribution methods, including pipelines; to postal, finance, and many other operations. They are, in greater or lesser measure and with any necessary modifications, applicable to virtually any physical security situation.

This manual contains doctrine applicable to the security manager and to the guard. There is no need for the guard to know the procedures needed to obtain personnel and equipment. However, the manager—and to a lesser degree, the supervisor—must have this knowledge at his disposal to properly support and train all security personnel.

The techniques described in the following chapters can be readily adapted to a host of systems to be secured. But remember, physical safeguards, like tactical barriers for defense, require the backing of a trained and alert (security) force. Also, there must be proper execution of administrative/operational checks and procedural safeguards.