



**Facilities  
Physical  
Security  
Measures**

**GUIDELINE**

**DRAFT**

# **ASIS INTERNATIONAL COMMISSION ON STANDARDS AND GUIDELINES**

The Commission on Standards and Guidelines was established in early 2001 by ASIS International (ASIS) in response to a concerted need for guidelines regarding security issues in the United States. As the preeminent organization for security professionals worldwide, ASIS has an important role to play in helping the private sector secure its business and critical infrastructure, whether from natural disaster, accidents, or planned actions, such as terrorist attacks, vandalism, etc. ASIS had previously chosen not to promulgate guidelines and standards, but world events have brought to the forefront the need for a professional security organization to spearhead an initiative to create security advisory provisions. By addressing specific concerns and issues inherent to the security industry, security guidelines will better serve the needs of security professionals by increasing the effectiveness and productivity of security practices and solutions, as well as enhancing the professionalism of the industry.

## **Mission Statement**

To advance the practice of security through the development of guidelines within a voluntary, non-proprietary, and consensus-based process utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership and the security industry.

## **Goals and Objectives**

- Assemble and categorize a database of existing security-related guidelines
- Develop methodology for identifying new guideline development projects
- Involve ASIS Councils, interested members, and other participants to support guideline development
- Identify and establish methodology for development, documentation, and acceptance of guidelines thus promulgated
- Build and sustain alliances with related organizations to benchmark, participate in, and support ASIS guideline development
- Produce international consensus-based documents in cooperation with other industries and the Security Industry Standards Council

## **Functions**

- Establish guideline projects
- Determine guidelines for development and assign scope
- Assign participating Council(s), where appropriate
- Approve membership on guideline committees
- Act as a governing body to manage and integrate guidelines from various Councils and security disciplines
- Review and monitor projects and guideline development
- Approve Final Draft Guideline and Final Guideline
- Select guidelines for submission to the Security Industry Standards Council and the American National Standards Institute (ANSI)



# **FACILITIES PHYSICAL SECURITY MEASURES GUIDELINE**

## **Safety Act Designation**

In April 2005, the U.S. Department of Homeland Security (DHS) awarded ASIS International a Designation for its Guidelines Program under the SAFETY Act (Support Anti-Terrorism by Fostering Effective Technology Act of 2002). This Designation is significant in three ways: (1) it establishes that ASIS standards and guidelines are qualified to be a “technology” that could reduce the risks or effects of terrorism, (2) it limits ASIS’ liability for acts arising out of the use of the standards and guidelines in connection with an act of terrorism, and (3) it precludes claims of third party damages against organizations using the standards and guidelines as a means to prevent or limit the scope of terrorist acts.

Copyright © 2008 by ASIS International

ISBN **nmn**

ASIS International (ASIS) disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. In issuing and making this document available, ASIS is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is ASIS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstance.

All rights reserved. Permission is hereby granted to individual users to download this document for their own personal use, with acknowledgment of ASIS International as the source. However, this document may not be downloaded for further copying or reproduction nor may it be sold, offered for sale, or otherwise sold commercially.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

# Facilities Physical Security Measures Guideline

|             |   |           |
|-------------|---|-----------|
| <b>1.0</b>  | <b>Title .....</b>  | <b>1</b>  |
| <b>2.0</b>  | <b>Revision History .....</b>                                   | <b>1</b>  |
| <b>3.0</b>  | <b>Commission Members .....</b>                                 | <b>1</b>  |
| <b>4.0</b>  | <b>Committee Members .....</b>                                  | <b>1</b>  |
| <b>5.0</b>  | <b>Guideline Designation.....</b>                               | <b>2</b>  |
| <b>6.0</b>  | <b>Scope.....</b>   | <b>2</b>  |
| <b>7.0</b>  | <b>Summary .....</b>  | <b>2</b>  |
| <b>8.0</b>  | <b>Purpose .....</b>  | <b>3</b>  |
| <b>9.0</b>  | <b>Keywords .....</b>   | <b>3</b>  |
| <b>10.0</b> | <b>Terms and Definitions .....</b>                              | <b>4</b>  |
| <b>11.0</b> | <b>Recommended Practice Advisory.....</b>                       | <b>9</b>  |
| <b>11.1</b> | <b>Crime Prevention Through Environmental Design (CPTED)...</b> | <b>10</b> |
|             | 11.1.1 Background.....  | 10        |
|             | 11.1.2 Strategies.....  | 10        |
|             | 11.1.3 Risk Assessment Process .....                            | 14        |
| <b>11.2</b> | <b>Physical Barriers and Site Hardening .....</b>               | <b>16</b> |
|             | 11.2.1 Physical Barriers.....                                   | 16        |
|             | 11.2.2 Site Hardening.....                                      | 21        |
| <b>11.3</b> | <b>Physical Entry and Access Control.....</b>                   | <b>22</b> |
|             | 11.3.1 Access Control Barriers .....                            | 23        |
|             | 11.3.2 Electronic Access Control Systems .....                  | 23        |
|             | 11.3.3 Personnel Access Control.....                            | 23        |
|             | 11.3.4 Locks.....   | 23        |
|             | 11.3.5 Contraband Detection .....                               | 25        |
|             | 11.3.6 Vehicle Access Control.....                              | 25        |
|             | 11.3.7 Procedures and Controls .....                            | 26        |
| <b>11.4</b> | <b>Security Lighting.....</b>                                   | <b>27</b> |
|             | 11.4.1 Applications.....  | 27        |
|             | 11.4.2 Intensity.....   | 28        |
|             | 11.4.3 Equipment.....   | 28        |
| <b>11.5</b> | <b>Intrusion Detection Systems.....</b>                         | <b>31</b> |
|             | 11.5.1 Intrusion Detection System Devices .....                 | 32        |
|             | 11.5.2 Alarm Transmission, Monitoring, and Notification.....    | 33        |
|             | 11.5.3 Installation, Maintenance, and Repair.....               | 33        |
| <b>11.6</b> | <b>Closed-Circuit Television .....</b>                          | <b>34</b> |
|             | 11.6.1 Functional Requirements.....                             | 34        |
|             | 11.6.2 Cameras .....  | 36        |
|             | 11.6.3 Transport Medium.....                                    | 38        |

|             |   |           |
|-------------|---|-----------|
| 11.6.4      | Command Center.....                           | 38        |
| 11.6.5      | Recording.....                                | 38        |
| 11.6.6      | Maintenance .....                             | 39        |
| <b>11.7</b> | <b>Security Personnel.....</b>                | <b>40</b> |
| 11.7.1      | Security Managers .....                       | 40        |
| 11.7.2      | Security Officers.....                        | 40        |
| 11.7.3      | Other Employees .....                         | 43        |
| <b>11.8</b> | <b>Security Policies and Procedures .....</b> | <b>44</b> |
| 11.8.1      | Policies.....                                 | 44        |
| 11.8.2      | Procedures.....                               | 45        |
|             | <b>Bibliography.....</b>                      | <b>47</b> |

## 1.0 Title

The title of this guideline is the Facilities Physical Security Measures Guideline.

## 2.0 Revision History

Baseline document.

## 3.0 Commission Members

Jason L. Brown, Thales Australia  
Steven K. Bucklin, Glenbrook Security Services, Inc.  
John C. Cholewa III, CPP, Embarq Corporation  
Cynthia P. Conlon, CPP, Conlon Consulting Corporation  
Michael A. Crane, CPP, IPC International Corporation  
Eugene F. Ferraro, CPP, PCI, CFE, Business Controls Inc.  
F. Mark Geraci, CPP, Bristol-Myers Squibb Co., Chair  
Robert W. Jones, Kraft Foods, Inc.  
Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair  
John F. Mallon, CPP, SC Johnson & Son, Inc.  
Marc H. Siegel, Ph.D., ASIS Security Management System Consultant  
Roger D. Warwick, CPP, Pyramid International

## 4.0 Committee Members

Geoffrey T. Craighead, CPP, Securitas Security Services USA Inc., Committee Chair  
Robert W. Jones, Kraft Foods, Inc.  
Sean A. Ahrens, CPP, Schirmer Engineering  
Randy Atlas, PhD, AIA, CPP, Counter Terror Design Inc.  
Daniel E. Bierman, CPP, PSP, Whitman, Requardt & Associates, LLP  
Elliot Boxerbaum, CPP, Security/Risk Management Consultants, Inc.  
John T. Brady (deceased), ConocoPhillips Company  
Ross D. Bulla, CPP, PSP, The Treadstone Group, Inc.  
Nick Catrantzos, CPP, Metropolitan Water District of Southern California  
BG (Ret.) Jonathan H. Cofer, Defense Information Systems Agency  
Thomas G. Connolly, Red Hawk/UTC Fire/Security Co.  
Frederick J. Coppel, CPP, SAIC  
Joe DiDona, The Reader's Digest Association, Inc.  
Jack F. Dowling, CPP, PSP, JD Security Consultants, LLC  
David R. Duda, PE, CPP, PSP, Newcomb & Boyd  
Alan F. Farley, CPP, CNI Utilities  
Mary Lynn Garcia, CPP, Sandia National Laboratories  
William J. Moore, PSP, ABCP, CAS, Jacobs Facilities Inc.

Patrick M. Murphy, CPP, PSP, CLSD, Marriott International Inc.  
Robert Pearson, PE, Raytheon Co.  
Thomas J. Rohr Sr., CPP, Eastman Kodak Company  
Gregory L. Sanders, CPP, United Nations Development Programme  
Terry Wood, PE, CPP, Wackenhut Consulting and Investigations  
Paul Yung, PhD, Deloitte Touche Tohmatsu

Guideline editor: Peter Ohlhausen, Ohlhausen Research, Inc.

## **5.0 Guideline Designation**

This guideline is designated as ASIS GDL FPSM **nn** 2008.

## **6.0 Scope**

This guideline assists in the identification of physical security measures that can be applied at facilities to safeguard or protect an organization's assets—people, property, and information. It is not aimed at a specific occupancy, but facilities and buildings in general.

## **7.0 Summary**

The guideline outlines eight main categories of physical security measures used to protect facilities. These categories are:

- Crime Prevention Through Environmental Design (CPTED),
- Physical Barriers and Site Hardening,
- Physical Entry and Access Control,
- Security Lighting,
- Intrusion Detection Systems (Alarms),
- Closed-Circuit Television (CCTV),
- Security Personnel, and Security Policies and Procedures.

## 8.0 Purpose

The purpose of this guideline is to introduce readers, who may or may not have a security background, to the main types of physical security measures that can be applied to minimize the security risks at a facility.

To choose the right physical security measures and apply them appropriately, it is important to first conduct a risk assessment, such as described in the *ASIS General Security Risk Assessment Guideline*. The risk assessment, accompanied by a basic understanding of physical security measures provided by this guideline, makes it possible, either alone or with the help of security consultants or vendors, to select and implement appropriate physical security measures to reduce the assessed risks and accomplish the protective task.

## 9.0 Keywords

Access Control, Alarm System, Asset, Barrier, Camera, Closed-Circuit Television (CCTV), Crime Prevention Through Environmental Design (CPTED), Facility, Intrusion Detection, Lighting, Lock, Perimeter Protection, Physical Security, Physical Security Measure, Policy, Procedure, Security Manager, Security Officer, Site Hardening.

## 10.0 Terms and Definitions

### 10.1

#### *access control*

the control of persons, vehicles, and materials through the implementation of security measures for a protected area

### 10.2

#### *alarm system*

combination of sensors, controls, and annunciators (devices that announce an alarm via sound, light, or other means) arranged to detect and report an intrusion or other emergency

### 10.3

#### *asset*

any tangible or intangible value (people, property, information) to the organization

### 10.4

#### *barrier*

a natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials

### 10.5

#### *camera*

device for capturing visual images, whether still or moving; in security, often part of a closed-circuit television system (see **closed-circuit television**)

### 10.6

#### *closed-circuit television (CCTV)*

video surveillance system; a television installation in which a signal is transmitted to monitors, recording and control equipment.

### 10.7

#### *contract security service*

a business that provides security services, typically the services of security officers, to another entity for compensation.

### 10.8

#### *crime*

an act or omission which is in violation of a law forbidding or commanding it for which the possible penalties for an adult upon conviction include incarceration, for which a corporation can be penalized by a fine or forfeit, or for which a juvenile can be adjudged delinquent or transferred to criminal court for prosecution. The basic legal definition of crime is all punishable acts, whatever the nature of the penalty.

**10.9**

***crime prevention through environmental design (CPTED, pronounced sep-ted)***

an approach to reducing crime or security incidents through the strategic design of the built environment, typically employing organizational, mechanical, and natural methods to control access, enhance natural surveillance and territoriality, and support legitimate activity.

**10.10**

***denial***

frustration of an adversary's failed attempt to engage in behavior that would constitute a security incident (see **security incident**)

**10.11**

***detection***

the act of discovering an attempt (successful or unsuccessful) to breach a secured perimeter (such as scaling a fence, opening a locked window, or entering an area without authorization)

**10.12**

***event***

a noteworthy happening; typically, a security incident (see **security incident**), alarm, medical emergency, or similar occurrence

**10.13**

***facility***

one or more buildings or structures that are related by function and location, and form an operating entity

**10.14**

***lighting***

degree of illumination; also, equipment, used indoors and outdoors, for increasing illumination

**10.15**

***lock***

a piece of equipment used to prevent undesired opening, typically of an aperture (gate, window, building door, vault door, etc.), while still allowing opening by authorized users

**10.16**

***perimeter protection***

safeguarding of a boundary or limit

**10.17**

***physical security***

that part of security concerned with physical measures designed to safeguard people, to prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard them against a security incident (see **security incident**).

**10.18**

***physical security measure***

a device, system, or practice of a tangible nature designed to protect people and prevent damage to, loss of, or unauthorized access to assets (see **assets**)

**10.19**

***policy***

a general statement of a principle according to which an organization performs business functions

**10.20**

***private security***

the nongovernmental, private-sector practice of protecting people, property, and information, conducting investigations, and otherwise safeguarding an organization's assets; may be performed for an organization by an internal department (usually called proprietary security) or by an external, hired firm (usually called contract security)

**10.21**

***private security officer***

an individual, in uniform or plain clothes, employed by a nongovernmental organization to protect assets (see **assets**)

**10.22**

***procedure***

detailed implementation instructions for carrying out security policies; often presented as forms or as lists of steps to be taken prior to or during a security incident (see **security incident**)

**10.23**

***proprietary information***

valuable information, owned by a company or entrusted to it, which has not been disclosed publicly; specifically, information that is not readily accessible to others, that was created or collected by the owner at considerable cost, and that the owner seeks to keep confidential

**10.24**

***proprietary security organization***

typically a department within a company that provides security services for that company

**10.25**

***protection-in-depth***

the strategy of forming layers of protection for an asset (see **assets**)

**10.26**

***protective task***

the goal of the security program for a facility. It may be to keep aggressors out, keep valuable goods in, protect employees and visitors, safeguard information, or satisfy some other requirement

**10.27**

***risk***

the likelihood of loss resulting from a threat, security incident, or event

**10.28**

***risk assessment***

The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel

**10.29**

***risk management***

a business discipline consisting of three major functions: loss prevention, loss control, and loss indemnification

**10.30**

***security incident***

an occurrence or action likely to impact assets

**10.31**

***security manager***

an employee or contractor with management-level responsibility for the security program of an organization or facility

**10.32**

***security measure***

a practice or device designed to protect people and prevent damage to, loss of, or unauthorized access to equipment, facilities, material, and information

**10.33**

***security officer***

an individual, in uniform or plain clothes, employed to protect assets

**10.34**

***security survey***

a thorough physical examination of a facility and its systems and procedures, conducted to assess the current level of security, locate deficiencies, and gauge the degree of protection needed. Sometimes called a security audit.

**10.35**

***security vulnerability***

an exploitable security weakness

**10.36**

***site hardening***

implementation of enhancement measures to make a site more difficult to penetrate

**10.37**

***stand-off distance / set-back***

the distance between the asset and the threat, typically regarding an explosive threat

**10.38**

***surveillance***

observation of a location, activity, or person

**10.39**

***tailgating***

to follow closely. In access control, the attempt by more than one individual to enter a controlled area by immediately following an individual with proper access. Also called piggybacking.

**10.40**

***threat***

an action or event that could result in a loss; an indication that such an action or event might take place

**10.41**

***token***

a device, typically a card or key-fob, that contains coded information capable of being read by electronic devices placed within or at the entry and exit points of a protected facility

**10.42**

***uninterruptible power supply (UPS)***

a system that provides continuous power to an alternating current line within prescribed tolerances; protects against over-voltage conditions, loss of primary power and intermittent brownouts. Usually utilized in conjunction with an emergency generator.

## 11.0 Recommended Practice Advisory

Practice advisories provide the reader with guidance regarding various physical security measures and their functions. This guideline addresses the following topics:

- 11.1 Crime Prevention Through Environmental Design (CPTED)
- 11.2 Physical Barriers and Site Hardening
- 11.3 Physical Entry and Access Control
- 11.4 Security Lighting
- 11.5 Intrusion Detection Systems (Alarms)
- 11.6 Closed-Circuit Television
- 11.7 Security Personnel
- 11.8 Security Policies and Procedures

A bibliography is provided at the end of this document.

## 11.1 Crime Prevention Through Environmental Design (CPTED)

### 11.1.1 Background

Crime prevention through environmental design (see 10.0, Terms and Definitions, crime prevention through environmental design (CPTED), is a concept that seeks to use architectural design and the physical environment as protection against opportunities for crime.\* To provide maximum control, an environment is divided into a smaller, more clearly defined area or zones, or what is known as a “defensible space” (Newman,1972). Crime prevention design solutions should be integrated into the function of the buildings, or at least the location where they are being implemented.

CPTED relies on an awareness of how people use space for legitimate and illegitimate purposes. The approach uses design to discourage those who may be contemplating criminal acts and to encourage activity and witness potential by legitimate users. CPTED concepts and applications can be applied to existing facilities as well as new buildings and renovations.

Underlying CPTED is the understanding that all human space

- has some *designated* purpose,
- has social, cultural, legal, or physical *definitions* (such as expectations or regulations) that prescribe the desired and acceptable behaviors, and
- is *designed* to support and control the desired and acceptable behaviors.

The CPTED approach focuses on

- manipulating the physical environment to produce behavioral effects that reduce the fear and incidence of certain types of criminal acts,
- understanding and modifying people’s behavior in relation to their physical environment, and
- redesigning space or using it differently to encourage desirable behaviors and discourage illegitimate activities.

### 11.1.2 Strategies

In general, there are three primary controls that can be implemented that will supplement or support the strategies mentioned above. As the diagram suggests these controls, overlap or compliment the overall security program and cannot stand alone as a singular method of mitigating a criminal incident.

In general, there are three classifications to CPTED strategies:

---

\* The term crime prevention through environmental design was first used by C. Ray Jeffrey in 1971 in a book by that name.

1. **Mechanical measures**— this approach emphasizes the use of hardware and technology systems such as locks, security screens on windows, fencing and gating, key control systems, CCTV, electronic access control, including biometrics and electronic visitor management systems. Mechanical measures must not be relied upon solely to create a secure environment, but rather be used in context with people and design strategies.
2. **Organizational measures** — focus on teaching individuals and groups steps they can take to protect themselves or the space they occupy. Methods include security and law enforcement patrols, police officer patrols, or other strategies that use people to observe, report and intervene. Routine activity theory suggests that the presence of capable guardians may deter crime. Criminals generally avoid targets or victims who are perceived to be armed, capable of resistance or potentially dangerous. Criminals generally stay away from areas they feel are aggressively patrolled by police, security guards or nosy neighbors. Likewise, they avoid passive barriers such as alarm systems, fences, locks or related physical barriers.
3. **Natural or Architectural Measures** — designing of space to ensure the overall environment works more effectively for the intended users, while at the same time deterring crime.

A CPTED design recognizes the use of a space, assumes the crime problem or threats in the space, formulates a solution compatible with the designated use of the space, and incorporates an appropriate crime prevention strategy that enhances the effective use of the space. CPTED employs these strategies to make a site less desirable for illegitimate activity to develop or occur:

- **Natural access control:** employing real and symbolic barriers (including doors, fences, shrubbery, and other obstacles) to limit access to a building or other defined space and that prevent the criminal from committing a crime and having access to a target.

For example, to deter intruders from entering lower-story windows, a choice can be made between planting dense, thorny bushes near the windows and installing locking devices or an alarm system. The decision should rest on the calculated/assumed risks associated with the particular facility.

- **Natural surveillance:** increasing visibility by occupants and observers (such as security officers, law enforcement and pedestrians) to increase witness potential of trespassing, misconduct, or criminal behavior within a facility or its grounds. Natural Surveillance increases the residents' or building users' awareness of who leaves and enters the property or buildings. Criminal choice is often influenced by the perception of target availability and vulnerability. Criminals often choose certain neighborhoods for crimes because they are familiar and well traveled, because they appear more open and vulnerable, and because they offer more potential escape routes. Thus, the more suitable and accessible the target, the more likely the crime will occur. The ability to see how persons come and go off a property becomes a deterrent factor for criminal behavior.

For instance, if a loading dock is enclosed with a high, concrete wall, thieves may be attracted to the concealment. Conversely, the use of chain-link fencing that allows an unobstructed view of the area by workers or passersby may discourage thieves and aggressors.

- **Natural territorial reinforcement/boundary definition:** establishing a sense of ownership by facility owners or building occupants to define territory to potential aggressors and to assist legitimate occupants or users to increase vigilance in identifying who belongs on the property and who doesn't. This sends the message that would-be-offenders can be identified. In addition, the theory holds that people will pay more attention to and defend a particular space or territory from trespass if they feel a form of "psychological ownership" in the area. Thus, it is possible, through real or symbolic markers, to encourage tenants or employees to defend property from incursion.

An example might be low edging shrubbery along pedestrian walkways in an apartment complex marks the territory of individual buildings and discourages trespassers from cutting through the area. In addition, people are more likely to defend a particular space against trespassing if they feel a psychological ownership of the area.

- **Management and maintenance:** maintaining spaces to look well tended and crime free.

The "broken windows" theory (Wilson & Kelling, 1982) suggests that an abandoned building or car can remain unmolested indefinitely, but once the first window is broken, the building or car is quickly vandalized. Maintenance of a building and its physical elements (such as lighting, landscaping, paint, signage, fencing, and walkways) is critical for defining territoriality.

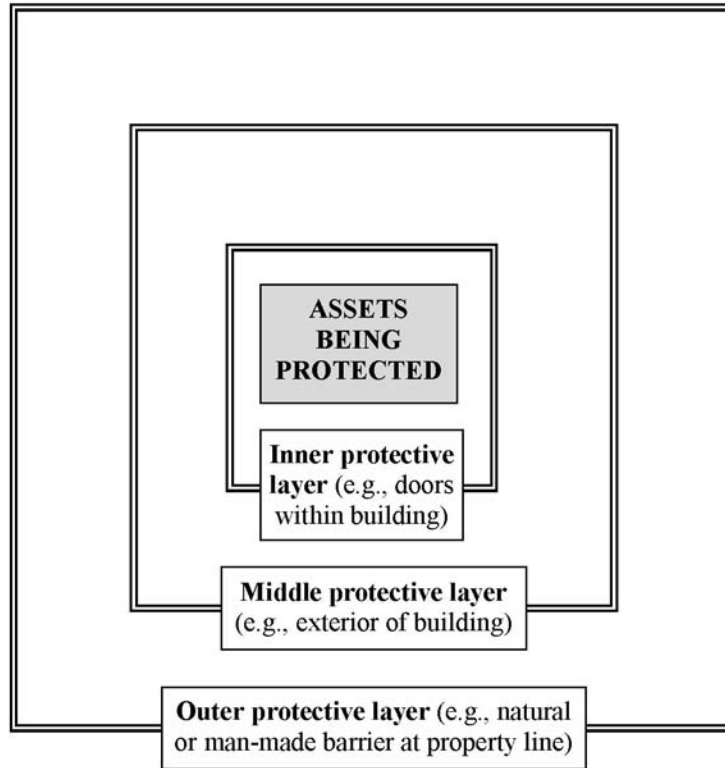
- **Legitimate activity support:** engaging legitimate occupants, residents, customers, or visitors in the desired or intended uses of the space.

Criminal activity thrives in spaces that occupants and desired users do not claim and that offer no legitimate activities that can undermine or replace the criminal activities. CPTED suggests adding enticements to draw legitimate users to a space, where they may in effect crowd out undesirable illegitimate users of the space.

- **Compartmentalization:** One of the basic CPTED strategies is to design multiple layers or concentric layers of security measures so that highly protected assets are behind multiple barriers. These layers of security strategies or elements start from the outer perimeter and move inward to the area of the building with the greatest need for protection. Each layer is designed to delay an attacker as much as possible. This strategy is known as protection-in-depth (Fay, 1993, p. 672). If properly planned, the delay should either discourage a penetration or assist in controlling it by providing time for an adequate response.

The illustration below shows a model of layered security.

**Layers of Security**



In some facilities, such as urban multi-story buildings, structures may cover the entire property area up to the property line. In those cases, it may be impossible to establish a separate outer protective layer. The building's envelope may need to be considered as the outer layer, elevator lobby security as the middle layer, and tenant space security as the inner layer.

**Outer Layer**

Physical controls at the outer protective layer or perimeter may consist of fencing or other barriers, protective lighting, signs, and intrusion detection systems. It is the outermost point at which physical security measures are used to deter, delay detect, delay, and respond (or defend) to illegitimate and unauthorized activities. Controls at this layer are generally designed to define the property line and channel people and vehicles through designated and defined access points. Intruders or casual trespassers will notice these property definitions and may decide not to proceed to avoid trespassing charges or merely just being noticed.

If early detection and identification are vital, intrusion detection and audio and video assessment technology can be applied at the perimeter.

### ***Middle Layer***

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself. Protection of skylights and ventilation ducts can discourage penetration from the roof.

Locations under a structure, like manholes and sewers, are also vulnerable to penetration. Floors, too, must be protected, particularly in a multi-story building where an intruder may be able to enter from lower levels. Walls and openings (such as air intake vents) on the sides of buildings should also be examined for vulnerability to penetration.

### ***Inner Layers***

Usually, several inner layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting.

The value of an asset being protected affects the amount of protection required. A high value asset being housed in an inner area might require signs defining access requirements for the area, specially reinforced walls, a structurally reinforced door with a biometric lock, intrusion detection systems, closed circuit television (CCTV) to monitor access, and safes and vaults to house the asset itself.

In general, there are three primary controls that can be implemented that will supplement or support the strategies mentioned above. As the diagram suggests, these controls overlap or compliment the overall security program and cannot stand alone as a singular method of mitigating a criminal incident.

### **11.1.3 Risk Assessment Process**

The key to success with risk assessment, the process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel, is problem seeking before problem solving. The right questions should be asked and the facility surveyed before developing security recommendations or implementing security enhancements.

The ASIS International *General Security Risk Assessment Guideline* uses a systematic and comprehensive approach to do the following:

- Understand the risk.
- Specify loss risk events and vulnerabilities.
- Establish the probability of loss risk and the frequency of events.
- Determine the impact of the events.
- Develop options to mitigate risks.
- Study the feasibility of implementing various measures or controls.
- Perform a cost-benefit analysis.

In problem seeking, the following tasks should be carried out:

- Assess crime reporting data.
- Gather demographic data.
- Gather land use information.
- Conduct site inspections.
- Observe and note user behavior patterns.

## 11.2 Physical Barriers and Site Hardening

### 11.2.1 Physical Barriers

Barriers may be natural or structural (man-made). Natural barriers include fields, creeks, rivers, lakes, mountains, cliffs, marshes, deserts, or other terrain difficult to traverse. Structural (man-made) barriers include berms, ditches, artificial ponds, canals, planted trees and shrubs, fences, walls, doors, roofs, and glazing materials. Natural and structural barriers physically and psychologically deter the undetermined, delay the determined, and channel authorized traffic through specified entrances.

Where possible and practical, a clear zone, whose width will depend on the threat that is being protected against, should separate a perimeter barrier from structures inside the protected area, except when a building wall constitutes part of the perimeter barrier.

Barriers are commonly used to discourage unauthorized access that takes place by accident, by force, or by stealth. In general, a barrier should explicitly or implicitly describe territory. Barriers should not provide concealment for surprise attacks, enable intruders to gain access to upper levels, or obstruct lighting, video surveillance, or intrusion detection systems. However, barriers may be used to prevent views of the facility and the introduction of clandestine listening devices.

Since barriers can be breached, they should be accompanied where practical and appropriate by a means of determining when a breach has occurred or is occurring.

Barriers also keep people and property within a given area. For example, a barrier could prevent people inside a facility from conveniently throwing materials outside the facility for later retrieval.

Barriers are also used to direct pedestrian or vehicle traffic in predictable patterns that can be anticipated, which present opportunities to detect abnormal and potentially illegitimate activities. The barriers should be designed to address the threat they are designed to protect against.

#### ***Fences***

The most common perimeter barrier is fencing. A fence defines an area, may stop a casual trespasser, and tells people they are at a protected property line. However, fences usually only deter or delay entry—they do not prevent it entirely. Over time, fences must be maintained if they are to retain their deterrent value.

A fence can do the following:

- Give notice of the legal boundary of the premises.
- Help channel entry through a secured area by deterring entry elsewhere along the boundary.
- Provide a zone for installing intrusion detection equipment and closed-circuit television (CCTV).

- Deter casual intruders from penetrating a secured area.
- Force an intruder to demonstrate his or her intent to enter the property.
- Cause a delay in access, thereby increasing the possibility of detection.
- Create a psychological deterrent.
- Reduce the number of security officers required.
- Demonstrate a facility's concern for security.

#### Chain-Link Fences

Chain-link fences are quick to install; can be effective against pedestrian trespassers and animals; and provide visibility to both sides of the fence.

Chain-link fence fabric is made from steel or aluminum wire, which may be coated and which is wound and interwoven to provide a continuous mesh (Chain Link Fence Manufacturers Institute, 2004). It can be breached easily with a blanket, wire cutter, or bolt cutter.

To be effective, chain-link fencing must avoid overly large mesh fabric, undersized wire, lightweight posts and rails, and shallow post holes. The following are some design features that enhance security (Chain Link Fence Manufacturers Institute,<sup>♦</sup> 1997):

- **Height.** The higher the barrier, the more difficult and time-consuming it is to breach. For low security requirements, a 5-6 ft. (1.5-1.8 meter) fence may be sufficient; for medium security, a 7 ft. (2.1 meter) fence may be appropriate; and for high security (such as a prison), an 18-20 ft. (5.4-6.0 meter) fence may be required.
- **Barbed wire.** Using three or six strands at the top of a fence further delays an intruder. A site using a three- or six-strand, 45-degree arm should angle the arm outward from the secured area to keep people out and inward to keep people in.
- **Bottom rail.** Properly anchored, this prevents an intruder from forcing the mesh up to crawl under it.
- **Top rail.** A horizontal member of a fence top to which fabric is attached with ties or clips at intervals not exceeding two feet. A top rail generally improves the appearance of a fence, but it also offers a handhold to those attempting to climb over. A top tension wire should be provided if a top rail is not installed.
- **Burying /Mow strip.** Burying or installing a mow strip (concrete) in addition to a chain-link fabric 1 ft. (0.3 meters) or more prevents an intruder from forcing the mesh up.
- **Color fabric.** Color polymer-coated chain-link fabric enhances visibility, especially at night.

---

<sup>♦</sup> In the United States, the Chain Link Fence Manufacturers Institute and the American Society for Testing and Materials, among others, have published useful specifications for fencing. Equivalent organizations do the same in other countries.

- **Double fence.** An additional line of security fencing a minimum of 10 ft. to 20 ft. (3 meters to 6 meters) inside the perimeter fence creates a controlled area and room for sensors or a perimeter patrol road between the fences.

Chain-link fencing can also be used indoors to secure a compartment that merits special protection.

#### Expanded Metal and Welded Wire Fabric Fences

These fences are generally more expensive than chain-link but less expensive than perforated metal or iron grillwork. They look somewhat like netting.

Expanded metal does not unravel and is tough and extremely difficult to cut. It is available in uncoated, painted, or galvanized steel, as well as aluminum and stainless steel. Expanded metal comes in four basic types: standard or regular, grating, flattened, and architectural or decorative.

Welded wire fabric, cheaper than expanded metal, is generally used for lower-risk applications.

#### Ornamental Fences

Ornamental fences made of wrought-iron, steel, or aluminum can be effective barriers. The application for which the fence is being used will determine its type, style, height, spacing between vertical bars or rods, and the type of fence top (either a top rail covering the tops of the vertical bars or rods, or bars or rods located above the top rail).

#### Barbed Wire

Barbed wire varies in grade, coating weight, number of barbs, and spacing of barbs. If they are intended to discourage human trespassing, fences constructed entirely of barbed wire, should be at least 7 ft. (2.1 meters) tall, not counting the top guard. The strands should be tightly stretched and attached firmly to posts spaced less than 6 ft. (1.8 meters) apart.

Barbed wire may also be formed into concertina coils, which may be used for top guards on barriers or as fencing in itself. Temporary or tactical barriers of barbed concertina wire can be laid quickly. Local building codes may address the use of this type of application with barbed wire.

#### Concrete Fences

Concrete block fences are less expensive than cast-in-place concrete but offer poor to moderate protection against penetration as they can be scaled easily. Adding deterrents at the top, such as a top guard, barbed wire or razor ribbon, or metal spikes, can make concrete fences more effective barriers. It should be noted, that concrete fences can enhance concealment.

#### Wooden Fences

Generally, wooden fences are used for low-security applications. They must be difficult to climb and have sufficient strength for the desired level of protection. A wooden fence's effectiveness can be enhanced by adding barbed wire, razor ribbon, or metal spikes. When utilizing a wooden fence to delay entry, the vertical picket sections must be

no wider than 1-3/4" with and the horizontal sections should be 50" apart; located on the protected side of the building.

### ***Planters, Bollards, Concrete Barriers, and Steel Barricades***

Large, heavy planters—made of concrete reinforced with glass-fiber, strengthened with steel bars, and spaced about 3 ft. (0.9 meters) apart (and sometimes anchored to the ground)—can be effective vehicle barriers.

Bollards are waist-high cylindrical posts, usually made of steel or concrete, which are anchored to the ground. They may be fixed position, removable posts for emergency access, or can be raised or lowered as needed.

Concrete barriers may be cast in place and anchored into the ground so that removal would be difficult. Reinforced park benches and large concrete blocks can also serve as concrete barriers. Another form is the concrete highway median barrier, also known as the Jersey Barrier or T-rail. These barriers are more effective in stopping a vehicle when they are joined together and bolted to the ground.

Standard highway metal guard rails may also be used as vehicle barriers apart from motorcycles.

### ***Premises Openings***

Most building intrusions are effected through doors and windows. Where practical, openings should be made as difficult to penetrate as the building surfaces themselves.

#### Gates

The number of pedestrian and vehicular gates should be kept to the minimum consistent with efficient operation and safety. The size and means of opening the gates must comply with local codes. All gates should be provided with locks.

Gates come in many types: single-swing gates for walkways, double-swing gates for driveways, multifold gates for any opening up to 60 ft. (18.2 meters), and overhead single- and double-slide gates for use where there is insufficient room for gates to swing. Cantilever slide gates, both single and double, are available for driveways where an overhead track would be in the way. Vertical-lift gates are made for special purposes such as loading docks.

#### Turnstiles

Turnstiles are designed to control pedestrian traffic and minimize tailgating (piggybacking). They are made in various heights—low, waist high (about 3 ft. or 0.9 meters), and full height (about 7 ft. or 2.1 meters). Low turnstiles, are easy to hurdle, offer little protection unless attended. Security officers and video surveillance with motion sensing may be used to detect when a person hurdles a turnstile. Turnstiles can be automated using a card access control system. In deploying circular turnstiles, it is important to remember that when a turnstile is added to a fence, the turnstile itself may provide a means for an intruder to climb over and enter the fenced area.

#### Doors

Personnel doors, in both outer and inner building walls, may be single, double, revolving, sliding, or folding. In normal security settings, their function is to provide a barrier at a point of entry or exit. In high security settings, a door must offer the maximum delay time before penetration by extraordinary means (i.e., by the use of cutting tools, hard-carried tools, and some explosives)” (Giglotti & Jason, 2004, p. 149). Solid wood or sturdy hollow metal doors can be covered with metal to strengthen them against a tool attack.

Doors create several vulnerabilities. A door is sometimes weaker or stronger. than the surface into which it is set, including the door frame. Moreover, hinges may be defeated.

Vehicular doors may be single, double, hanging, rolling, or folding. They can usually be penetrated with hand tools or vehicles. They can also serve secondarily as passageways for personnel. Their existence creates a vulnerability to unrestricted pedestrian access.

#### Windows

The following are some different types of glass:

- **Tempered glass** is treated to resist breakage. Building codes require tempered glass for safety reasons as when the glass breaks it fragments into small pieces rather than shards.
- **Wired glass** provides resistance against large objects but may still shatter.
- **Laminated glass** is composed of two sheets of ordinary glass bonded to a middle layer or layers of plastic sheeting material. When laminated glass is stressed or struck, it may crack and break but the pieces of glass tend to adhere to the plastic material. It should be noted that for laminated glass to be effective, it should be secured to the frame of the window. It is also the preferred glass type for mitigating blast forces. It will aid in the protection of building occupants from glass shattering in the event of an explosion.
- **Bullet-resistant glass** provides stronger resistance to attack. It is laminated and consists of multiple plies of glass, polycarbonate, and other plastic films to provide many levels of ballistic resistance.

Other window-related security materials include the following:

- **Window bars.** Steel bars, where permitted by building and fire codes, can add to the protection of windows.
- **Security window film (sometimes called safety window film)** adheres to the interior surface of glass and holds broken glass in place to minimize lethal projectiles. Security window film does not protect a facility from intrusion but is a safety measure.
- **Blast curtains** are made of reinforced fabrics that provide protection from flying materials in an explosion. Blast curtains do not protect a facility from intrusion but are a safety measure.
- **Security Shutters** can add to the protection of windows. They can be either the roll-up type, with horizontal interlocking slats (usually made of aluminum or

polyvinyl chloride) which roll up into a box located at the top of the window; or the accordion type, with vertical interlocking slats which slide to the sides of the window. These shutters can be operated manually, or electrically using remote controls, weather sensors, or timers.<sup>2</sup>

#### Other Openings

Other openings include shafts, vents, ducts, or fans; utility tunnels; channels for heat, gas, water, electric power, and telephone; and sewers and other drains. Such openings can be fortified with steel bars or grills, wire mesh, expanded metal, and fencing (and/or possibly protected with intrusion detection devices).

#### **Locks**

(See Section 11.3.4, Locks, in Section 11.3, Physical Entry and Access Control.)

### **11.2.2 Site Hardening**

Key factors in hardening a facility include the following:

- stand-off distance, which is the distance between a critical asset and the nearest point of attack (usually using an explosive device)
- structural integrity of the premises against attacks (such as forced entry, ballistic attack, or bomb blast) and natural disasters (such as earthquakes, hurricanes or tornadoes)
- redundancy of operating systems, such as power, heating, ventilating, and air-conditioning (HVAC) systems and communications systems

Consideration should be given to protecting HVAC systems to prevent the introduction of harmful materials into exterior air intakes. Many buildings place air intakes high above ground or on the roof. Other premises use physical barriers to prevent unauthorized access to air intakes. It may also be appropriate to use intrusion detection devices, video surveillance, and security officers to monitor access to air intakes and to HVAC and mechanical rooms.

Measures to manage power generation and distribution systems include the use of redundant power feeds, emergency generators, and uninterruptible power supplies.

Security command centers and control stations may warrant special protection, such as wall hardening, installation of bullet-resistant windows, protection of HVAC systems serving the center, and provision of emergency power and backup communications.

There is also the need to protect utilities such as water, gas services, and telecommunications.

---

<sup>2</sup> Abacus Construction Index “About security shutters” <<http://www.construction-index.com/usa-security-shutters.asp>> (3 July 2008).

## 11.3 Physical Entry and Access Control

Before discussing physical entry and access control, it is important to realize that there are certain issues that to be considered in designing such a system. There are as follows:

- Will the access control system be integrated with other systems, such as alarms and CCTV, and elevator systems?
- Will the various components of the access control system operate together effectively?
- Is the likely throughput rate at each controlled access point acceptable?
- Should people's entries and exits be viewed and recorded by a CCTV system?
- Does the access control system comply with all applicable building and fire codes?

A comprehensive access control system is designed to:

- permit only authorized persons and vehicles to enter and exit,
- detect and prevent the entry of contraband material,
- detect and prevent the unauthorized removal of valuable assets, and
- provide information to security officers to facilitate assessment and response.

Included in an access control system are the technologies, procedures, databases, and personnel used to monitor the movement of people, vehicles, and materials into and out of a facility. Access control elements may be found at a facility boundary or perimeter, such as personnel and vehicle portals, at building entry points, in elevators, or at doors into rooms or other special areas within a building. Certain items may be of particular interest upon entry (e.g., drugs, weapons, or explosives) or exit (e.g., precious metals, manufactured product, or laptop computers).

Different access control technologies and procedures have different strengths. Metal detectors are appropriate when the defined threat involves metal objects, such as weapons or tools, but are not effective against explosives.

An adversary may use several types of attacks to defeat an access control point:

- **Deceit.** The adversary employs false pretenses in an attempt to convince security personnel or an employee to permit entry.
- **Direct physical attack.** The adversary uses tools to force entry into an area.
- **Technical attack.** The adversary forges a credential, guesses a personal identification number, or obtains another persons credential.

Access control systems may be manual, machine-aided manual, or automated. Manual systems use personnel to control who or what may enter. Machine-aided manual systems

use tools (such as metal detectors) to help a security officer make the access decision. Automated access control systems use technology to control the entire access process, potentially eliminating the need for personnel to authenticate manual access.

### **11.3.1 Access Control Barriers**

Section 11.2, Physical Barriers, and Site Hardening, focuses on keeping unwanted parties out. This section (11.3, Physical Entry and Access Control) emphasizes the means of allowing some people in and keeping others out. Access control barriers include doors, gates, turnstiles, and elevators. Locks and security personnel secure the movable portions of barriers. Like perimeter protection barriers, access control barriers are often applied in multiple layers.

### **11.3.2 Electronic Access Control Systems**

Electronic access control systems have several main parts: credentials in the form of something you know, something that is inherent to you and something you carry. Other essential parts of the access control system include the credential reader, communication cabling, distributed processor, central database, software and supplementary interfaces to alarm monitoring and request-to exit for associated access controlled doors.

It is possible for a business that has several sites to use a single electronic access control system to control access to all the sites, even if they are widely separated.

### **11.3.3 Personnel Access Control**

To decide whom to let into a facility and whom to keep out, it is necessary to consider measures such as:

- tokens or other items in the person's possession (such as a metal key, a proximity, insertion or swipe card, or a photo identification card)
- private information known by the individual (such as a password or personal identification number)
- biometric features of the person (such as fingerprint, hand geometry, iris and retinal patterns, signature, or speech patterns)

The most secure systems use several of these methods to authenticate and validate access. Using too many, however, could significantly decrease throughput and slow down access through an access control portal.

### **11.3.4 Locks**

Locks vary by physical type, application, and mode of opening.

#### Mechanical Locks

Mechanical locks, such as door locks, cabinet locks, and padlocks, use an arrangement of physical parts to prevent the opening of the bolt or latch. The two major components in

most mechanical locks are the coded mechanism and the fastening device. The coded mechanism may be a key cylinder in a key lock or a wheel pack in a mechanical combination lock.

The fastening device is usually a latch or bolt assembly. A latch automatically retracts as the door is closed, whereas a bolt stays in the same position unless it is intentionally moved. Latches are more convenient but more vulnerable than bolts.

#### Electrified Locks

Electrified locks allow doors to be locked and unlocked by a remote device. That device may be an electric push button, a motion sensor, a card reader, a digital keypad or a biometric device. Electrified locks may be mechanical or electromagnetic.

#### Electromagnetic Locks

An electromagnetic lock consists of an electromagnet (attached to the door frame) and an armature plate (attached to the door). A current passing through the electromagnet attracts the armature plate and thereby holds the door shut. Electromagnetic locks are useful on doors that are architecturally significant, and where mechanical latching otherwise could not be achieved. Electromagnetic locks should be coordinated with life-safety code as there are specific and additional requirements with these doors that must be provided.

#### Card-Operated Locks

Card-operated locks rely on a unique card or credential being presented to a card reader at a location where the access is being controlled. The system electronically checks the information (including the identification of the cardholder and the time period when access is permitted) on the card and compares it with that already stored in the system, and either activates the lock to permit entry or denies access.

#### Combination Locks

A combination lock operates either mechanically or electrically. An alphanumeric keypad, part of the locking mechanism, is used to select a series of numbers or letters in a predetermined sequence to release the locking mechanism. Sometimes these locks are combined with a key that only will work when the correct sequence of numbers or letters has been selected, a card reader, or a biometric feature.

#### Biometric Locks

Biometric operated locks function by verifying a person's specific physical characteristic, such as fingerprint, hand geometry, face, and iris and retina characteristics. If the specific characteristic is verified, the locking device is activated to permit access.

#### Rapid Entry Systems

Rapid entry systems enable emergency responders to enter a facility when no one is available to provide access. A rapid entry key vault is a specially designed, weatherproof, fixed box containing essential keys to the facility. A key to the box should be supplied to emergency responders ahead of time.

Key System

In a master key system, a single key operates a series of mechanical locks, and each of those locks is also operated with another key specific to that lock. Since the compromise of a master key can compromise an entire facility, the use of any master key must be strictly controlled.

Key management systems help managers control and account for keys. Typically, managers conduct initial and periodic inventories of keys, maintain records of who has which keys, and maintain a secure key storage facility.

Because locks can be compromised, they should be complemented with other measures, such as intrusion detection sensors, video surveillance, and periodic checks by security officers. The time required to defeat the lock should approximate the penetration delay time of the rest of the secured barrier. In other words, it does not make sense to put a strong lock on a weak door or vice versa.

### **11.3.5 Contraband Detection**

Contraband consists of prohibited items, such as weapons, explosives, drugs, audio recording devices, cameras, or even tools. Where these items are a part of the threat definition, all personnel, materials, and vehicles should be examined for contraband before entry is allowed. In addition to physical searches by security officers or trained canines, methods of contraband detection include metal detectors, X-ray machines, and explosive detectors. Contraband detection is time-consuming and can reduce throughput significantly.

In some higher-security facilities, vehicles might be searched before they are allowed to enter a controlled area. Vehicle searches should be conducted in a portal or monitoring station by trained security officers. The search location should include a way to detain the vehicle, such as using vehicle gates or barriers, until searches are completed.

### **11.3.6 Vehicle Access Control**

Vehicles can be identified by devices such as cardboard placards, stickers, radio frequency identification (RFID) tags, bar codes, special license plates, and electronic tags.

Vehicle access control may be manual (for example, using a security officer to decide whether to allow the vehicle in or out) or electronic (for example, allowing the driver to use a proximity card to open a gate).

### **11.3.7 Procedures and Controls**

The following are some of the important access issues that should be addressed through procedures and controls:

- |   |  |
|---|--|
| wearing of badges                                 | calibration of metal detectors                   |
| sharing of personal identification numbers (PINs) | use of explosives detectors                      |
| sharing of access cards                           | list of prohibited materials                     |
| tailgating or piggybacking                        | access hours and levels of access                |
| challenging of unbadged persons                   | credential tampering and replacement             |
| number of access attempts allowed                 | accommodation of disabled or handicapped persons |
| searching of packages, briefcases, and purses     | preventive maintenance of equipment              |

For example, all but the smallest or simplest facilities need a procedure to provide for authorized visitor access. A security officer or trained employee should request access permission for the visitor and specify the date and time of the visit, the point of contact, and the purpose of the visit. It is common to issue visitor badges (sometimes bearing the visitor’s photograph and usually showing the date to prevent reuse). Access control procedures will also be needed for couriers, contractors, and other non-employees who regularly visit a site.

Likewise, access database management requires special consideration. The database should be continually updated—by authorized persons only—to reflect employee separations, leaves of absence, or suspensions. In addition, the database may track visitor access passes and assign a time period for their use. It may be useful, as well, to periodically check the access history for unusual access hours or attempts to gain entry to areas where the access card holder is not authorized to go. Access to the database should be strictly limited.

## 11.4 Security Lighting

Security lighting can augment other security measures such as physical barriers, intrusion detection systems, CCTV, and security personnel activities.

Security lighting can provide several advantages such as:

- possible deterrence of adversaries and suspicious activities
- improved surveillance and security response
- reduced liability
- witness potential

The disadvantages are as follows:

- cost of installation and maintenance
- light pollution and light trespass, which could result in neighbor complaints
- lighting fixtures that are not aesthetically pleasing

The purposes of security lighting—discouraging unauthorized entry and detecting intruders—are served both outdoors and indoors. Outdoors, security lighting can be applied to the perimeter of a site, private roadways, parking areas, building entrances and exits, equipment yards, loading docks, storage spaces, large open work areas, piers, docks, utility control points, and other sensitive and critical areas. Indoors, security lighting is also beneficial.

### 11.4.1 Applications

Basic exterior security lighting consists of the following application types (United States Department of the Army, 2001):

- **Continuous.** In this application, illumination devices in a series maintain uniform lighting during hours of darkness.
- **Glare projection.** This deters potential intruders by making it difficult to see into an area. It also illuminates the intruders themselves.
- **Standby.** Lights are not on continuously but are either automatically or manually turned on randomly or when suspicious activity is detected or suspected by security personnel or an intrusion detection system.
- **Controlled.** This lighting illuminates a limited space (such as a road) with little spillover into other areas.
- **Portable (movable).** This consists of manually operated, movable searchlights that may be lit during darkness or as needed.
- **Emergency.** This system of lighting may duplicate any of the systems above. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative source of power.

Where practical, security lighting during the hours of darkness should be continuous and equipped with an alternative power source. In addition, the system's wiring and controls should be protected against tampering or vandalism.

### **11.4.2 Intensity**

The right level or intensity of lighting depends on a site's overall security requirements. Lighting intensity<sup>♦</sup> can be measured with instruments, but for a rule of thumb, "at night, outside of a building or at a parking lot, one should be able to read a driver's license or newspaper with some eyestrain" (Purpura, 1998). In addition, lighting levels must meet local codes or standards. A CCTV system's needs may also dictate the proper level of lighting and Kelvin rating.

### **11.4.3 Equipment**

General security lighting equipment falls into the following categories:

- **Streetlight.** This uses various sources of illumination.
- **Searchlight.** This uses a very narrow high-intensity beam of light to concentrate on a specific area. It is used in correctional, construction, and industrial settings to supplement other types of lighting.
- **Floodlight.** This projects a medium to wide beam on a larger area. It is used in a variety of settings, including the perimeters of commercial, industrial, and residential areas.

---

<sup>♦</sup> Details on appropriate lighting intensity can be found in publications written for various countries and regions—for example, in the U.S., the *Guideline for Security Lighting for People, Property, and Public Spaces* (Illuminating Engineering Society of North America, 2003).

- **Fresnel.** This lighting typically projects a narrow, horizontal beam. Unlike a floodlight, which illuminates a large area, the fresnel can be used to illuminate potential intruders while leaving security personnel concealed. It is often used at the perimeters of industrial sites.

The main lighting sources (that is, fixtures or lamps) are as follows (Fennelly, 2004):

- **Incandescent.** These lamps are the least efficient and are the most expensive to operate and have a short life span.
- **Fluorescent.** Fluorescent lamps are more efficient than incandescent lamps but are not used extensively outdoors, except for underpasses, tunnels and signs.
- **Halogen and quartz halogen.** They provide about 25 percent better efficiency and life than ordinary incandescent bulbs.
- **Mercury vapor.** The lamps take several minutes to produce full light output, but they have a long life.
- **Metal halide.** They are often used at sports stadiums because they imitate daylight; for the same reason, they work well with CCTV systems. They are expensive to install and maintain.
- **High-pressure sodium.** These lamps are energy efficient and have a long life span. They are often applied on streets and parking lots, and their particular quality of light enables people to see more detail at greater distances in fog.
- **Low-pressure sodium.** These lamps are even more efficient than high-pressure sodium but are expensive to maintain.

**[LED (light-emitting diodes).** These lamps are one of the newest lighting sources and have the potential of furnishing a cost effective alternative that lasts longer without sacrificing illumination.]

**[Induction.** Induction lamps have a long life and, similar to fluorescent lamps, are utilized mainly indoors, except for parking structures, underpasses and tunnels.]

Each of the preceding illumination sources has specific characteristics related to color rendition, life span, and startup times. In addition, some applications call for infrared lighting, which is invisible to the naked eye but is useful for CCTV scene illumination.

Lighting equipment must be inspected and maintained regularly. In that process, one should do the following:

- Check electrical circuits and test all connections.
- Ensure proper lamp functionality.
- Ensure that lamps are kept clean and maintain their proper lighting angle.
- Ensure that the lighting intensity continues to meet security requirements.

- Ensure that batteries are charged for emergency lighting in compliance with regulations.

Regarding placement, in outdoor applications “high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles (less hazardous to the driver), and is more aesthetically pleasing than standard lighting” (FEMA, 2003).

## 11.5 Intrusion Detection Systems

Intrusion detection systems (IDSs), sometimes called alarm systems, employ various sensors that trigger alarms, or notifications. These systems are integral factors in a security program's effort to:

- **Deter.** The presence of an IDS may deter intruders when signs are posted warning that a site is protected by such a system.
- **Detect.** Most IDSs are designed to detect an impending or actual security breach.
- **Delay.** By activating other systems, such as locks, doors, gates, and other physical barriers.
- **Respond.** IDSs facilitate security responses by pinpointing where an intrusion has occurred and possibly where the intruder has moved within the site.

The quality of an IDS and its components greatly affects its usefulness. Deficiencies can harm a security program by causing the system to:

- fail to detect an intruder,
- falsely report breaches which generate costly and repeated deployment of security or law enforcement personnel, and
- create excessive false activations so that alarms are ignored or security and law enforcement officers are called unnecessarily. (Many jurisdictions levy fines for excessive numbers of false alarm calls to police.)
- provide a false sense of security

When considering IDSs, the security manager should ensure that the system (Fay, 2008, p. 258)

- meets the security needs of the facility,
- operates in harmony with other systems,
- does not interfere with business operations, and
- is cost-effective (i.e., that the value of benefits derived from the system is at least equal to the costs of the system).

The IDS should be installed according to any applicable codes and standards.

### 11.5.1 Intrusion Detection System Devices

Several types of IDS devices are used to detect intrusions:

- **Position detection devices.** These devices, often magnetic, detect when one part of the device is moved away from the other. They may be specially made to permit different types of mounting and for use in different environments. An example of this type of device would be a door position switch.
- **Motion detectors.** These devices create an alarm when the static conditions of the protected area change. Different detectors are made for interior and exterior use, long and short range use, and different types of movement by different types of targets.
  - **Microwave detection** relies on a constant reception level of its transmitted or reflected energy. When the energy level changes due to reflection or deflection, an alarm is transmitted.
  - **Infrared detectors**, sometimes called passive infrared detectors (PIRs), absorb invisible light energy and compare the energy absorbed to the background energy. When the received energy fluctuates from ambient levels, an alarm is transmitted.
  - **Dual-technology motion detectors** typically employ both microwave and infrared technologies in a single package. They require disturbances in both technologies before an alarm is transmitted.
  - **Ultrasonic detectors** transmit in the ultrasonic range. When the received signal changes from its expected level (due to sound deflection or absorption), an alarm is transmitted.
  - **Beam detectors** operate similarly, transmitting an alarm when the beam is not detected at the receiving unit or the beam's energy falls below the threshold.
- **Sound detectors.** Sound detectors transmit an alarm when sounds outside a selectable ambient range are received by the detector. They are normally used where audible sounds are stable and quiet, such as in a vault.
- **Vibration sensors.** These react to motions such as shaking or physical shocks. Typically these sensors are utilized to detect a tool attack.
- **Heat sensors.** These devices trigger alarms when the air or surface temperature changes.
- **Capacitance devices.** Often used with safes and vaults, these devices detect changes in electrical capacitance in protected items to which low voltage has been applied. If an object or person approaches or touches the protected which alters the , the sensor levels change and an alarm is transmitted.
- **Impact sensors.** These detect sudden changes in air pressure.

- **Glass break sensors.** These sensors detect the frequency of breaking glass. To limit false alarms, they have been combined with pressure sensors to avoid false alarms.

Other security systems can also play the role of an IDS, and IDS devices can be integrated into video and access control systems.

### 11.5.2 Alarm Transmission, Monitoring, and Notification

Alarms signals can be transmitted to alarm monitoring systems and personnel. They may be transmitted via wire or wirelessly and by zone or by an individual alarm point. Being able to identify a particular alarm point may reduce security officer's response time and make it easier to identify malfunctioning alarm points.

Alarm monitoring may be performed by the user organization or by an outside service, such as an alarm monitoring company or a central station (high-end monitoring service). With the right transmission method, the monitoring can take place over any distance.

Whether alarm monitoring is done in-house (proprietary) or on a contract basis, the user can arrange to be notified by several methods, including telephone, e-mail, and pager, and can develop a list of all persons to be notified.

### 11.5.3 Installation, Maintenance, and Repair

Several steps are involved in the installation, maintenance, and repair of alarm systems:

- **Engineering and installation.** These are essential for a properly functioning alarm system. Even if all the devices, panels, and annunciators are of good quality, the system will fail if those components are not installed properly or are not the correct ones for the application.
- **Commissioning.** This is the process of testing every alarm point and each automatic function of a new system.
- **Auditing.** This ongoing process tests and documents a security system's operations to ensure that all parts are functioning properly.
- **Maintenance.** Alarm systems require regular maintenance, which can be provided by facility staff (such as an in-house security systems specialist) or system vendors.
- **Repair.** Repairs can be handled in the same way as maintenance issues.

## 11.6 Closed-Circuit Television

Video surveillance can be a valuable component of a facility's security program. The systems that provide such surveillance are usually called closed-circuit television (CCTV) systems. They are primarily used to:

- detect activities that call for a security response
- collect images of an incident for later review and use as evidence if needed
- assist in alarm analysis.

The main elements of a CCTV system are as follows:

- **Field of View** The area visible through the camera lens.
- **Scene.** This is the location or activity to be observed.
- **Lens.** The lens determines the clarity and size of the field of view.
- **Camera.** The camera converts the optical image produced by the lens to an electronic signal for transmission. The camera requires mounting hardware and sometimes a housing for protection against physical or environmental damage.
- **Transmission medium.** The signal generated from the camera must be transmitted to equipment for viewing or recording, typically over coaxial cable, twisted-pair wire, network cable, optical fiber, or a microwave signal.
- **Monitor.** The monitor can display one or more video images with the appropriate equipment.
- **Recording equipment.** This includes recorders and equipment for selecting which images to record, the speed at which the images will be recorded, the resolution of the capture and the compression format for the capture. Recording equipment is available in two formats. These include:
  - analog, requiring the use of a cassette
  - digital, which can either capture analog video or raw digital video.
- **Control equipment.** Items include switchers, quads, recorders, multiplexers, signal processors, intelligent software, motion detectors, and devices for moving cameras to view different parts of a scene (pan, tilt, and zoom).

### 11.6.1 Functional Requirements

Once the system's purpose is determined (for example, by using the *ASIS General Security Risk Assessment Guideline*), a functional requirement for each component of the system should be written. A functional requirement is like a job description. A CCTV system's functional requirements can be discerned by asking these questions:

- What is the purpose of the system?
- What specifically is each camera supposed to view?

- What is the access for real-time or recorded video?

### ***Camera Functional Requirements***

Different functions require different fields of view. One must consider three factors:

- **Target.** This may consist of
  - persons (individuals or groups)
  - packages or objects
  - vehicles (individual)
  - traffic
- **Activity.** This could be
  - assault
  - vandalism
  - trespassing
  - robbery
  - package or vehicle left unattended
- **Purpose.** This may be to identify an individual or show the direction a suspect exited from a parking lot. The first purpose requires a defined focal view that includes the person's face, while the second purpose requires a wider focal length, to include the parking lot view.

### ***Monitoring Functional Requirements***

If the purpose of the CCTV system is to generate a response to specific incidents, then a trained person should monitor the system and respond accordingly. The average person can only monitor a limited number of cameras simultaneously, and needs frequent breaks to maintain comprehension of the scene. Certain technology can help with the human factor:

- **Motion detection.** Digital recording systems may be programmed to alert personnel by initiating an alarm and a full screen view if a person or object enters the scene in question.
- **Access control system integration.** A CCTV system can be integrated with a security alarm system so that, for example, a door alarm can trigger a nearby pan/tilt/zoom (PTZ) camera to pre-position, aim at and zoom in on the person walking through the door.
- **Intelligent video analytics.** Video analytics comes in many sizes, however, all video analytics measure/monitor changes in a digitized video scene and compare these changes internally utilizing an algorithm. Uses can include the recognition of certain events and conditions, such as an unattended package or vehicle, or movement by an animal versus a human being.

One needs to be aware of liability/risk that may be assumed when cameras are not monitored and persons being viewed by the cameras have an expectation of a security response if they are attacked.

### ***Recording Functional Requirements***

If a video recording is to be useful as evidence, it must clearly show the incident, target, or action it was meant to record, and, of course, the recording itself must be available. When writing the functional requirements for a recording device, it is important to consider these factors:

- **Resolution.** This is picture clarity, which must be sufficient on playback to distinguish the scene's key features.
- **Length of storage.** This is the length of time for which recorded video is kept before being recorded over or destroyed.
- **Frames Per Second (FPS).** Recorders may discard image frames to save storage space. If too many are discarded—that is, if the system records only one or two frames per second—then fast-moving action may not be captured or items in the scene may seem simply to appear or disappear.
- **Compression type (codec).** The video codec identifies the particular encoding /decoding method utilized for digital video data compression. Choices affect image quality and data storage space.

≈

When selecting CCTV system equipment, it is important to use a systems approach as opposed to a components approach. A systems approach examines how equipment will work with other elements of the CCTV system, with other workplace systems, and with the environment in which it is needed. This approach results in a CCTV system that operates effectively and satisfies a facility's needs. By contrast, buying components separately and without an integration plan often results in a system that does not perform as expected, or to its fullest capacity.

## **11.6.2 Cameras**

The following are key considerations in camera selection:

### ***Lighting***

CCTV manufacturers specify the amount of illumination needed for minimum function and for maximum performance. Image quality is also affected by excessive shadows, lens glare, and backlighting.

### ***Lens Selection***

The focal length of the lens determines the size (width and height) of the scene viewed. The longer the focal length, the smaller the scene captured. Lens focal lengths are typically measured in millimeters and are characterized as telephoto, standard, or wide angle. These lenses have either a fixed or varifocal (adjustable) focal length. Varifocal

lenses are often used in applications that require a zoom capability. The lens's iris, which opens and closes to control the quantity of light that reaches the camera's sensing element, may be manual or automatic.

### **Camera Types**

The following are the major types of CCTV cameras:

- **Analog.** These may be black-and-white or color. The most common type of camera, they work well in all indoor and many outdoor applications. They are analog based and may or may not have digital effects. Resolution ranges from 220 horizontal lines (very low) to 580 horizontal lines (very high). Light sensitivity varies between .005 lux (.00046 foot-candles), which is very low, to 10 lux (.929 foot-candles), which is very high. Color cameras are the most restricted by low-light situations. To compensate for that limitation, manufacturers have developed hybrid analog cameras. Some use infrared sensitivity to capture more light. Others combine color and black-and-white capability in one unit, capturing color images during daylight hours and black-and-white images at night when the light is low. Other cameras use an intensifier between the lens and the CCD (charge-coupled device) to amplify the available light tens of thousands of times.
- **IP (Internet protocol).** These digital cameras come in black-and-white or color and utilize the Transmission Control Protocol (TCP)/ Internet protocol (IP) for signal transmission over a network. Like their analog counterparts, IP cameras require visible light to create an image. These cameras are available in either standard, or megapixel resolutions. All IP cameras measure their resolution as a multiple of the common intermediate format (CIF), which is a resolution of 352 x 240. Standard IP cameras range from one-quarter CIF to four times CIF. Megapixel cameras range from 16 to 32 times CIF or higher.
- **Infrared (IR).** These cameras require an IR light source to create an image. They are used where visible light is not an option.
- **Thermal.** These require no visible or IR light to produce an image. Using special filters and lenses, the cameras monitor the temperatures of the objects in their field of view and use colors to represent temperatures. Cold objects are shown in varying shades of blue, while hot objects are shown in varying shades of red. Thermal cameras are often used in long-range surveillance, such as monitoring ships in a harbor five miles out. Since these cameras require no light to create an image, they are popular with police and border patrols.
- **Internet Protocol (IP).** IP cameras, utilize Transmission Control Protocol (TCP)/ Internet protocol (IP) or Ethernet cabling to send uncompressed, lossless images via a computer Local Area network (LAN) / Wide Area Network (WAN) or Global Area Network (GAN).

### **Power and Mounting**

The availability of power can greatly affect a CCTV system budget. Typically, separate power and video cables are pulled through conduit to a camera's location. Some IP cameras receive power over the same cable on which the digital video is transmitted.

Interior cameras may require housings for physical protection or aesthetic reasons. Specialized enclosures are also available to protect cameras used outdoors in extreme weather or explosive environments.

### 11.6.3 Transport Medium

The video signal generated by the camera must be transmitted to equipment to be viewed or recorded. Selection of the optimal transport medium may be difficult for a typical security manager, who might prefer to leave it to the bidding contractor. Coaxial cable is generally sufficient for analog cameras but does not work for IP-based systems. For distances of 1,000 ft. or more between the camera and the control point, it may be best to use fiber-optic cable, regardless of the type of camera. Many transmission methods are available, and each has its advantages, disadvantages, and costs. Among those methods are coaxial cable, fiber-optic cable, twisted pair (two-wire) cable, Category 5 (networking) cable, microwave and radio frequency technologies, infrared transmission, and transmission over existing telephone lines, the Internet, or an intranet. A system might use more than one method of video transmission. Encryption techniques can secure both wired and wireless transmissions against hackers and unauthorized viewers, however the speed of video can be affected.

### 11.6.4 Command Center

A command center is a central location from which staff can view, record, retrieve, or respond to video from one or more surveillance cameras. It may be a closet that serves a single camera watching a cash register at a convenience store, solely for after-the-fact investigations. Alternatively, a command center might collect images from hundreds, or even thousands, of cameras and be housed in a facility that integrates CCTV with other systems, such as access control and intrusion detection.

### 11.6.5 Recording

Basic types of recorders include:

- **Time-lapse (analog).** These recorders are designed to make a two-hour cassette record up to 900 hours by allowing time to lapse between recorded images. The chosen duration dictates how much information is recorded. Instead of a full 25 frames (PAL) or 30 frames (NTSC) of video information being recorded each second, a time-lapse recorder may capture only a fraction as many frames. The strongest market for the time-lapse machine is retail, industrial, and long-term surveillance.
- **Event (analog).** Event recorders are designed to record triggered events and can cost less than time-lapse recorders. They remain in standby mode, waiting for an event to record. Since the number and duration of events recorded determines how much videotape is used, the recorder may run out of tape if it is not closely monitored. These units are most popular for covert surveillance, entrance monitoring, and other applications where a particular event is the desired subject.

- **24-hour/72-hour high-density (analog).** These units capture a larger number of recorded images over a 24- or 72-hour period than do time-lapse machines. By changing the angle of the recording head and reducing the space between recorded images, the units capture three times as much information on an inch of video tape.
- **Digital video recorders (DVRs) (digital).** DVRs capture digital video signals, not analog (unless the analog signal is first converted to digital format and compressed). These recorders store video data on a hard drive, CD, DVD, or other medium. The challenge is that the video data requires a great deal of storage space. Therefore, DVRs compress the video image, using a particular codec (a compression engine or command sequence that causes the unit to combine colors, drop resolution, or both). Once compressed, however, the image quality may be poor. It is important to test DVRs before purchase. A more popular means of compression is to record fewer images per second. If the application is watching a dealer with a deck of cards, the DVR should record 30 or more images per second. If the application is watching people walk across a lobby, two or three images per second may be sufficient. Most DVRs can be programmed to record a different number of images per second from each camera input.

#### **11.6.6 Maintenance**

When a CCTV system (i.e., cameras, recording devices, monitors) is not operating as it should, the organization may be vulnerable, incident response may be delayed, and liability may be incurred. Camera maintenance must be considered before system implementation. Having adequate spare parts available and trained staff or a service agreement with a vendor or systems integrator is advisable

## 11.7 Security Personnel

The physical security measures in this guideline are typically implemented, monitored, or maintained by security personnel. Those personnel range from security managers to security officers, and—to varying degrees—all other personnel in the organization. This section presents highlights of security personnel's responsibilities. Two other ASIS International guidelines address this topic in greater detail:

*Chief Security Officer (CSO) Guideline*

*Private Security Officer (PSO) Selection and Training Guideline*

### 11.7.1 Security Managers

Security managers—those who manage security systems, policies, procedures, and other security personnel—are known by various names, including chief security officer (CSO), vice president–security, security director, chief of security, account manager security supervisor, and post commander and may be employees of or contractors to the organization.

A security manager's responsibilities may include, but are not limited to any or all of the following:

- physical security of the organization's assets
- development and enforcement of security policy and procedures
- crisis management
- business continuity planning
- executive protection
- investigation of security incidents
- employee security awareness
- information protection
- workplace violence prevention
- security officer employment and supervision
- security systems management

When security managers are employees of an organization, it is preferable that they be part of senior management. Such placement helps demonstrate that the organization considers security an important function by involving the security manager in the planning and the decision-making process.

### 11.7.2 Security Officers

Organizations use security officers to supplement or amend other controls/measures where human presence and human decision making is needed.

### **Organization**

Security officers, sometimes called guards, may be proprietary/in-house (employed directly by the organization) or contract (employed by a security services firm). The choice of whether to use proprietary or contract security officers depends on many factors, such as the type of organization to be protected, the nature of the organization's business, its location, and security personnel wages, benefits, training, and functional responsibilities. Each organization must weigh the advantages and disadvantages of the two approaches. Some organizations use both proprietary and contract officers, which is described as a hybrid force.

Proprietary security officer programs tend to offer more direct control of personnel selection, screening, training, and supervision. However, the proprietary approach is usually more expensive than the contract approach.

Contract security programs shift the burden of hiring, training, and supervising from the organization to the security services firm. They also provide greater flexibility in staffing levels.

Local ordinances and state laws may solely regulate contract security officers, proprietary security officers, both, or neither.

### **Responsibilities**

Security officers may carry out various responsibilities including, but not limited to, screening employees and visitors in reception areas; controlling access to the facility at other points; monitoring security and life safety equipment; conducting patrols on foot or using some type of vehicle; responding to security incidents; documenting incidents; escorting visitors; assisting with parking issues; inspecting packages and vehicles; and utilizing various security measures (doors, locks, alarms, CCTV cameras, lighting, etc.).

### **Legal Issues**

Security managers should be aware of legal issues such as officer selection and screening, authority to detain or arrest, and use of force.

### **Preemployment Screening**

The ASIS *Private Security Officer (PSO) Selection and Training Guideline* recommends that both proprietary and contract security guards meet the following criteria and requirements:

- minimum age of 18 years for unarmed positions and 21 years for armed positions
- legal working status
- verified Social Security number (in the United States) and addresses and telephone numbers for the preceding seven years
- high school diploma or equivalent
- criminal history check
- verified employment history for at least the preceding seven years

- verified license or certification to work as a security officer, if appropriate
- drug screening

***Training***

Security officers should be trained and tested on the following topics (among others), as appropriate to the assignment:

- ethics and professionalism
- security policies and procedures
- investigation
- observation techniques
- challenging techniques
- crowd control
- relations with law enforcement
- legal authority
- human relations
- public relations
- patrol procedures
- report writing
- ingress and egress control
- emergency medical assistance and first aid
- terrorism issues
- workplace violence
- use of force
- criminal and civil law
- operation of security systems
- general fire prevention and safety

If security officers are to be equipped with any weapons (such as firearms, batons, chemical sprays, or electrical weapons), they must be properly trained in their use. Officers who will be equipped with firearms need extensive, ongoing training.

Security officers should be given regular training reviews, as well as periodic proficiency testing.

***Post Orders***

Post orders, which are sometimes called standard operating procedures, state the essential elements of security officers' work assignments. They should contain at least the following minimum information:

- date of revision
- notice of confidentiality
- emergency contact information (internal and external), including after-hours contact information
- description of the facility and its users (and floor plans if possible)
- discussion and review of subjects such as access control, keys and equipment control, property removal, escort of facility users, mobile patrols, arrest policy and other policies and procedures
- specific instructions on the handling of emergency situations
- security staffing levels, hours of coverage, and specific functions and duties
- proper operation of all emergency and non emergency communication equipment
- instructions on public relations
- code of ethics and standards of conduct

**11.7.3 Other Employees**

In a broad sense, every employee should be considered part of the security program. Through a security awareness effort, employees should be taught to understand the relationship between security and the organization's success, learn their obligations under the security program, understand how various security measures support security program objectives, and become familiar with available resources to help with security concerns.

## 11.8 Security Policies and Procedures

The physical security measures described in this guideline are typically managed and employed in accordance with policies and procedures.

Security *policies* establish strategic security objectives and priorities for the organization, identify the organization representatives primarily accountable for physical security, and set forth responsibilities and expectations for managers, employees, and others in the organization. A policy is a general statement of a principle according to which an organization performs business functions. Security *procedures* are detailed implementation instructions for staff to carry out security policies. Procedures are often presented as forms or as lists of steps to be taken.

Policies and procedures must be communicated effectively to staff members, who will then be expected to perform accordingly. Policies and procedures can also form the basis for corrective action in the event of inappropriate behavior or underperformance.

### 11.8.1 Policies

Policies are generally reviewed, approved, and issued at the executive level of an organization. Once established, they tend to remain in place for an extended period. Therefore, they should be aligned with the overall business objectives of the organization.

Policy documents may affect decision making throughout the organization, even beyond the immediate subject of a policy. Moreover, the existence of a security policy tends to emphasize top management's commitment, thereby increasing the probability of employees' compliance with the policy.

An organization may increase its liability if it ignores the policy or applies it inconsistently. However, a concerted effort to address security issues on a policy level shows due-diligence and that management was aware of such issues and attempted to address them.

#### ***Subjects to Address***

Organizations may choose to develop policies that address general issues, people, property, and information. The following are some subjects that may be appropriate:

##### General

- organization's general objectives in security matters
- accountability of top management in security matters
- general responsibilities of line management
- general responsibilities of all staff
- specific responsibilities relating to the development of subsidiary policies
- reporting, auditing, and review arrangements

People

- workplace violence
- emergency evacuation and shelter/defend-in-place
- use and display of badges
- workplace access control management
- prohibited items and substances
- staff security awareness education
- escorting staff and visitors

Property

- safeguarding employer property
- acceptable personal use of employer assets
- limitations on who can direct security staff
- investigations
- property control, marking, and disposal
- key control and accountability
- incoming goods and materials
- vehicle access control
- occupational safety and health
- environment (light pollution, etc.)

Information

- disclosure of proprietary information
- information handling, including marking, storage, transmission, disposal, and destruction
- declassification schedule, process, or expiration of protection

### **11.8.2 Procedures**

Procedures change more often than policies to meet the changing demands and conditions that the overall organization or security department faces. Procedures can therefore be changed without the high-level, time-consuming executive review process used for policy approval. For example, a security policy may define access control as a corporate objective. The procedure for implementing access control may at first be as simple as relying on personal recognition, then progress to a card access control system, and then later call for the use of biometric technology. The policy would remain the same, but the procedure for carrying it out would be subject to change.

Promulgating security procedures clarifies responsibility for particular security concerns , demonstrates to employees that security rules were thoughtfully developed, and aids in the uniform enforcement of security rules.

***Subjects to Address***

Organizations may opt to develop procedures that address people, property, and information. Each procedure should ultimately connect to a policy. The following are some subjects that may be appropriate:

People

- responding to a threat of workplace violence
- activating the crisis management team after an executive kidnapping
- facility- or operation-specific checklist for evacuating an area in the event of an emergency
- employee badging, including varying levels of access permission
- identifying and managing suspicious packages
- protection of employees working alone
- visitor management

Property

- marking of facility property
- securing of valuable property
- removal of property from the facility
- key issuance and management
- security officer duties (post orders)
- security incident reporting

Information

- marking, storage, transmission, disposal, and destruction of confidential documents
- management of confidential meetings
- technical surveillance countermeasures (anti-eavesdropping)

## Bibliography

- American Society for Testing and Materials. (2008). *Standard practice for installation of chain-link fence*. (F567-00). Available: <http://www.astm.org> [2008, March 15].
- ASIS International. (2004). *Private security officer selection and training guideline*. ASIS GDL PSO 11 2004. Alexandria, VA: ASIS International.
- ASIS International. (2004). *Protection of assets manual*. Alexandria, VA: ASIS International.
- ASIS International. (2008). ASIS International glossary of security terms, [Online]. Available: <http://www.asisonline.org/library/glossary/index.xml> [2008, October 9].
- Atlas, R. (1991, March). "The other side of CPTED." *Security Management*.
- Atlas, R. (2008). *21<sup>st</sup> Century Security and CPTED: Designing for Critical Infrastructure Protection and Crime Prevention*. New York, NY: Taylor and Francis.
- Broder, J. F. (2006). *Risk analysis and the security survey* (3rd ed.). Burlington, MA: Butterworth-Heinemann.
- Canadian General Standards Board. (1999). *Security guards and security guard supervisors*. CAN/CGB-133.1.99. Ottawa, Canada: Canadian General Standards Board.
- Chain Link Fence Manufacturers Institute (1997 & 2008). Standard guide for metallic-coated steel chain link fence and fabric. <http://codewriters.com/asites/page.cfm?pageid=902&usr=clfma> [2008, March 15].
- Craighead, G. (2003). *High-rise security and fire life safety* (2<sup>nd</sup> ed.). Woburn, MA: Butterworth-Heinemann.
- Crowe, T. D. (1991). *Crime prevention through environmental design: Applications of architectural design and space management concepts*. Woburn, MA: Butterworth-Heinemann.
- Cunningham, W. C., Strauchs, J. S., and Van Meter, C. W. (1990). *Private security trends 1970–2000: The Hallcrest report II*. Boston, MA: Butterworth-Heinemann.
- Department of the Army. (2001). *Physical security training manual*. FM 3-19.30. Washington, DC: Department of the Army.
- Fay, J. J. (1993 & 2008). *Encyclopedia of security management* (1<sup>st</sup> and 2<sup>nd</sup> eds.). Burlington, MA: Butterworth-Heinemann.

- Federal Emergency Management Agency (FEMA). (2003). *Reference manual to mitigate potential terrorist attacks against buildings*. Washington, DC: Federal Emergency Management Agency.
- Fennelly, L. J. (Ed.). (2004). *Handbook of loss prevention and crime prevention* (4th ed.). Burlington, MA: Elsevier Butterworth-Heinemann.
- Fischer, R. J., & Green, G. (1998). *Introduction to security* (7th ed.). Boston, MA: Butterworth-Heinemann.
- Garcia, M. L. (2001). *The design and evaluation of physical protections systems*. Burlington, MA: Butterworth-Heinemann.
- Garcia, M. L. (2005). *Vulnerability assessment of physical protection systems*. Burlington, MA: Butterworth-Heinemann.
- Gigliotti, R., & Jason, R. (2004). Physical barriers. In L. J. Fennelly (Ed.), *Handbook of loss prevention and crime prevention* (4th ed.), p. 156. Burlington, MA: Butterworth-Heinemann.
- Illuminating Engineering Society of North America. (2003.) *Guideline for security lighting for people, property, and public spaces*. G-1-03. New York, NY: Illuminating Engineering Society of North America.
- Jeffrey, C. R. (1971). *Crime prevention through environmental design*. Thousand Oaks, CA: Sage Publications.
- Newman, O. (1972) *Defensible Space Crime Prevention Through Urban Design*. New York, NY: Macmillan Publishing Company.
- Purpura, P. *Security and loss prevention: An introduction* (4th ed.). Burlington, MA: Butterworth-Heinemann.
- Sennewald, C. A. (2003). *Effective security management* (4th ed.). Boston, MA: Butterworth-Heinemann.
- Wilson, J. Q., & Kelling, G. (1982, March). Broken windows. *Atlantic Monthly*.