ASIS INTERNATIONAL

Facilities Physical Security Measures

ASIS GDL FPSM-2009

GUIDELINE

ASIS INTERNATIONAL
Advancing Security Worldwide®

ASIS GDL FPSM-2009

an ASIS Guideline for Security

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.

Approved June 8, 2009

ASIS International

Abstract

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.

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS International standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else. ASIS does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

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, application, or reliance on this document. ASIS disclaims and makes no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person's or entity's particular purposes or needs. ASIS does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing 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 circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes standards to be used as guidelines that third parties may or may not choose to adopt, modify or reject. Any certification or other statement of compliance with any information in this document shall not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

ISBN 978-1-887056-95-3

FOREWORD

The information contained in this Foreword is not part of this ASIS International Guideline and has not been processed in accordance with ASIS' requirements for a Guideline. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Guideline.

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.

The work of preparing ASIS Standards and Guidelines is carried out through the ASIS International Standards and Guidelines Commission and its committees. The Mission of the ASIS Standards and Guidelines Commission is *to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry.*

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818, USA.

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, Purdue Pharma L.P., Chair
Robert W. Jones, Kraft Foods, Inc.
Michael E. Knoke, CPP, Express Scripts, Inc., Vice Chair
John F. Mallon, CPP
Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Roger D. Warwick, CPP, Pyramid International

At the time it approved this document, FPSM Guidelines Committee, which is responsible for the development of this Guideline, had the following members:

Committee Members

Committee Chairman: Geoffrey T. Craighead, CPP, Securitas Security Services USA, Inc.

Commission Liaison: Robert W. Jones, Kraft Foods, Inc.

Committee Secretariat: Sue Carioti, ASIS International

Sean A. Ahrens, CPP, Schirmer Engineering an Aon Global company
Randy I. Atlas, Ph.D., AIA, CPP, Counter Terror Design, Inc.
Daniel E. Bierman, CPP, PSP, Whitman Requardt & Associates
Elliot A. Boxerbaum, CPP, Security/Risk Management Consultants, Inc.
Ross D. Bulla, CPP, PSP, The Treadstone Group, Inc.
Nick Catrantzos, CPP, Metropolitan Water District of Southern California
Thomas Connolly, Red Hawk, a UTC Fire & Security Co.
Frederick J. Coppell, CPP, SAIC/DTRA/CXC
Joseph A. DiDona, The Reader's Digest Association, Inc.
Jack F. Dowling, CPP, PSP, JD Security Consultants, LLC
David R. Duda, PE, CPP, PSP, Newcomb & Boyd
Mary Lynn Garcia, CPP, Sandia National Laboratories
Ronald L. Martin, CPP, US Dept. of Health & Human Services
William J. Moore, PSP, Jacobs Global Buildings Group-North America
Patrick M. Murphy, CPP, PSP, Marriott International, Inc.
Robert L. Pearson, PE, The Protectorate Corporation
Thomas J. Rohr Sr., CPP, Carestream Health, Inc.
Steve Surfaro, Axis Communications
Paul P. Yung, Ph.D., Deloitte Touche Tohmatsu

Revision History

Baseline document.

Guideline Designation

This guideline is designated as ASIS GDL FPSM-2009.

Keywords

Access Control, Alarm System, Asset, Barrier, Camera, Crime Prevention Through Environmental Design (CPTED), Facility, Intrusion Detection, Lighting, Lock, Perimeter Protection, Physical Security, Physical Security Measure, Policy, Procedure, Security Manager, Risk Management, Security Officer, Site Hardening, Video Surveillance.

TABLE OF CONTENTS

TABLE OF FIGURES

an ASIS Guideline for Security –

Facilities Physical Security Measures Guideline

1. SCOPE, SUMMARY, AND PURPOSE

1.1 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.

1.2 Summary

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

1. Crime Prevention Through Environmental Design (CPTED),
2. Physical Barriers and Site Hardening,
3. Physical Entry and Access Control,
4. Security Lighting,
5. Intrusion Detection Systems,
6. Video Surveillance,
7. Security Personnel, and
8. Security Policies and Procedures.

In addition, the emerging field of security convergence is addressed.

1.3 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 an 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 to a level acceptable by the organization.

2. TERMS AND DEFINITIONS

2.1 access control: The control of persons, vehicles, and materials through the implementation of security measures for a protected area.

2.2 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.

2.3 asset: Any tangible or intangible value (people, property, information) to the organization.

2.4 barrier: A natural or man-made obstacle to the movement/direction of persons, animals, vehicles, or materials.

2.5 building envelope: The separation between the interior and the exterior environments of a building. It serves as the outer shell to protect the indoor environment as well as to facilitate its climate control. Building envelope design is a specialized area of architectural and engineering practice that draws from all areas of building science and indoor climate control.

2.6 camera: Device for capturing visual images, whether still or moving; in security, part of a video surveillance.

2.7 CCT rating: *Corrected Color Temperature (CCT)* is a measure of the warmth or coolness of a light. It is measured in degrees Kelvin which is the Centigrade (Celsius) absolute temperature scale where 0°K is approximately 272°C.

2.8 closed-circuit television (CCTV): See video surveillance.

2.9 contract security service: A business that provides security services, typically the services of security officers, to another entity for compensation.

2.10 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.

2.11 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.

2.12 denial: Frustration of an adversary's attempt to engage in behavior that would constitute a security incident (see *security incident*).

2.13 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).

2.14 event: A noteworthy happening; typically, a security incident (see *security incident*), alarm, medical emergency, or similar occurrence.

2.15 facility: One or more buildings or structures that are related by function and location, and form an operating entity.

2.16 lighting: Degree of illumination; also, equipment, used indoors and outdoors, for increasing illumination (usually measured in lux or foot-candle units).

2.17 intrusion detection system: A system that uses a sensor(s) to detect an impending or actual security breach and to initiate an alarm or notification of the event.

2.18 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.

2.19 perimeter protection: Safeguarding of a boundary or limit.

2.20 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*).

2.21 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*).

2.22 policy: A general statement of a principle according to which an organization performs business functions.

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

2.24 private security officer: An individual, in uniform or plain clothes, employed by an organization to protect assets (see *assets*). Also known as a "guard".

2.25 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*).

2.26 progressive collapse: Occurs when the failure of a primary structural element results in the failure of adjoining structural elements, which in turn causes further structural failure. The resulting damage progresses to other parts of the structure, resulting in a partial or total collapse of the building.

2.27 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.

2.28 proprietary security organization: Typically, a department within a company that provides security services for that company.

2.29 protection-in-depth: The strategy of forming layers of protection for an asset (see *assets*).

2.30 risk: The likelihood of loss resulting from a threat, security incident, or event.

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

2.32 risk management: A business discipline consisting of three major functions: loss prevention, loss control, and loss indemnification.

2.33 security incident: An occurrence or action likely to impact assets.

2.34 security manager: An employee or contractor with management-level responsibility for the security program of an organization or facility.

2.35 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.

2.36 security officer: An individual, in uniform or plain clothes, employed to protect assets.

2.37 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.

2.38 security vulnerability: An exploitable security weakness.

2.39 site hardening: Implementation of enhancement measures to make a site more difficult to penetrate.

2.40 stand-off distance/set-back: The distance between the asset and the threat, typically regarding an explosive threat.

2.41 surveillance: Observation of a location, activity, or person.

2.42 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*.

2.43 threat: An action or event that could result in a loss; an indication that such an action or event might take place.

2.44 throughput: The average rate of flow of people or vehicles through an access point.

2.45 token: An electronically encoded device (i.e., a card, key-fob, etc.) that contains information capable of being read by electronic devices placed within or at the entry and exit points of a protected facility.

2.46 uninterruptible power supply (UPS): A system that provides continuous power to an alternating current (AC) line within prescribed tolerances; protects against over-voltage conditions, loss of primary power, and intermittent brownouts. Usually utilized in conjunction with an emergency generator.

2.47 video surveillance: A surveillance system in which a signal is transmitted to monitors/recording, and control equipment. Includes closed-circuit television (CCTV) and network-based video systems.

3. RECOMMENDED PRACTICE ADVISORY

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

- 3.1 Crime Prevention Through Environmental Design (CPTED)
- 3.2 Physical Barriers and Site Hardening
- 3.3 Physical Entry and Access Control
- 3.4 Security Lighting
- 3.5 Intrusion Detection Systems
- 3.6 Video Surveillance
- 3.7 Security Personnel
- 3.8 Security Policies and Procedures
- 3.9 Security Convergence

A bibliography is provided at the end of this document.

3.1 Crime Prevention Through Environmental Design (CPTED)

3.1.1 Background

Crime Prevention Through Environmental Design (CPTED)—see 2.10—proposes that proper design and effective use of the built environment can lead to a reduction in the opportunity, fear, and incidence of predatory stranger-to-stranger type crime, as well as result in an improvement of the quality of life (how and where we live, work, and play).[1] To provide maximum control, an environment is divided into smaller, more clearly defined areas or zones, or what is known as *defensible space* (Newman, 1972). Crime prevention design solutions should be integrated into the design and 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.

[1] The current definition is used by the National Crime Prevention Institute (NCPI) University of Louisville, and enhanced by Randall I. Atlas Ph.D., AIA, CPP, in the book *21st Century CPTED* (2008).

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;
- Redesigning space or using it differently to encourage desirable behaviors and discourage illegitimate activities; and
- Reducing the conflicts between incompatible building users and building uses, with the goal of eliminating "no persons land" that no one takes ownership of.

3.1.2 Strategies

In general, there are three primary controls that can be implemented that will supplement or support the strategies mentioned above. As Figure 1 on page 8 suggests, these controls overlap or complement 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:

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, video surveillance, and electronic access control (including biometrics and electronic visitor management systems). Mechanical measures must not be solely relied upon to create a secure environment, but rather be used in context with people and design strategies. While mechanical measures not only provide physical protection, criminals are discouraged from targeting areas where these measures are in place.
2. *Organizational measures*: Focus on policies and activities that encourage observation, reporting and—where appropriate—intervention. This would include education for individuals and groups of strategies they can take to protect themselves and the space they occupy. It would also entail routine patrol and enforcement by security, law enforcement, or others. Routine activity theory suggests that a suitable guardian will prevent criminal activity from occurring. Criminals will generally avoid targets or victims when police, security, door staff, neighbors, or others are in a position to observe and react.
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 space will naturally have less opportunity for criminal activity when it is effectively used. Poor layout reduces the ability of intended users to apply appropriate measures to reduce crime, and also leads to circumvention of mechanical measures.

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 the following strategies to make a site less desirable for illegitimate activity to develop or occur:

- *Natural access control*: Employing physical and symbolic barriers to discourage or prevent access or direct movement to specific access points. Doors, fences, and other physical obstacles serve to prevent opportunities for criminal access. Symbolic barriers—such as signage—directs people to a particular route, and draws attention to those crossing the threshold.

  For example, to deter intruders from entering lower-story windows—in addition to locking devices, a choice can be made between electronic or administrative controls. The decision should rest on the calculated/assumed risks associated with the particular facility.

- *Natural surveillance*: Increasing visibility, both interior-to-exterior and exterior-to–interior, to increase witness potential, foster a sense of exposure to the criminal element, and give advance visibility to areas people are entering. This increases the feeling of safety to legitimate users of a space and increases the risk of detection to criminals. Neighborhoods with poor natural surveillance provide criminals with opportunities to observe, plan, and commit criminal activity.

  For instance, a loading dock area enclosed by a high concrete wall provides a concealment opportunity for engaging in break and entry, vandalism, or assault. Conversely, the use of chain-link fencing that allows for an unobstructed view of the area by workers, law enforcement, or the general public 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 does not. 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. This marks the territory of individual buildings and discourages trespassers from cutting through 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 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 also 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 figure below illustrates a simple layered security.

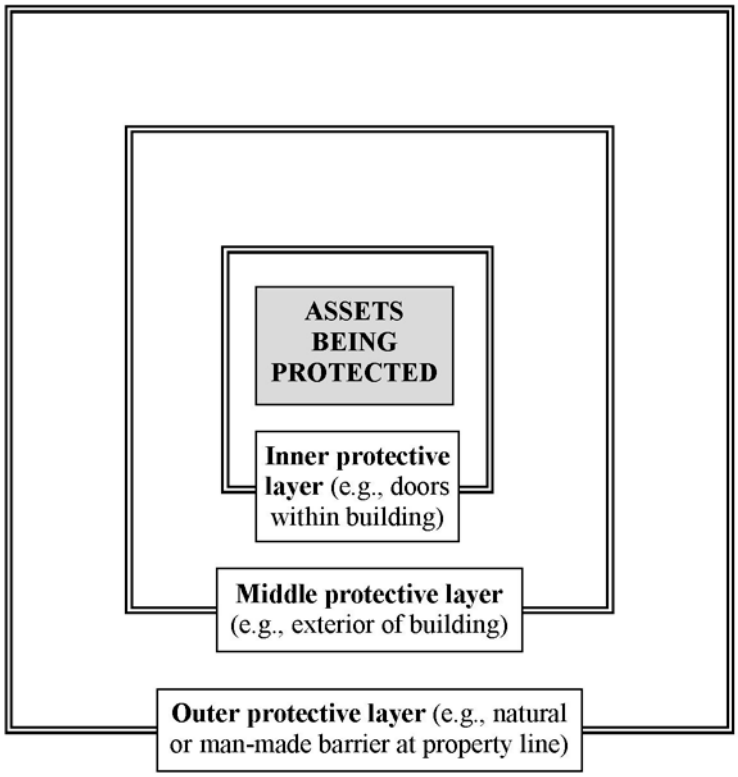

Figure 1: Layers of Security

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.

3.1.2.1 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, detect, delay[2], and respond (or defend) against 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 being noticed.

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

Some buildings have underground and/or attached parking structures. These should be considered part of the perimeter when taking into consideration the outer layer of a property.

3.1.2.2 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.

Openings under a structure, like manholes and sewers, are also vulnerable to penetration. Floors and ceilings, including raised and dropped, must be protected as well, particularly in a multi-story building where an intruder may be able to enter from different levels. Walls and openings (such as air intake vents) on the sides of buildings should also be examined for vulnerability to penetration. Intrusion detection at the building perimeter increases the effectiveness of security or police response.

3.1.2.3 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 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, video surveillance to monitor access, and safes and vaults to house the asset itself.

[2] For most organizations, denial is not a reasonable option as it is resource intensive.

3.2 Physical Barriers and Site Hardening

3.2.1 Physical Barriers

Barriers may be natural or structural (man-made). *Natural barriers* are intended to deter or impede entry, they 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.

Wherever possible and practical, a clear zone should separate a perimeter barrier from structures inside the protected area. The width of the *clear zone* will depend upon the threat that is being protected against. An exception can be made 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 barriers should explicitly define territorial boundaries. 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. Barriers should also not facilitate observation of the facility or its occupants. 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 into predictable patterns. This presents opportunities to detect abnormal and potentially illegitimate activities. A threat basis design strategy should be used when selecting physical barriers, and the barriers designed to address the specific threats.

3.2.1.1 Fences and Walls

The most common perimeter barriers are *fencing* and *walls*. A fence or wall defines an area, may stop a casual trespasser, and tells people they are at a protected property line. However, fences and walls 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 or wall 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 video surveillance system.
- 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.

3.2.1.1.1 Walls

Walls can be made of materials such as brick, stone, concrete block, or glass brick. Some walls, particularly concrete ones, are strengthened with steel bars. Walls should be sufficiently high to discourage people from climbing over them, and can be topped with materials to prevent scaling of the wall.

3.2.1.1.2 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), 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,[3] 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*. Barbed wires vary in gauge, coating weight, number of barbs, and spacing of barbs. If chain link or expanded metal fences are intended to discourage human trespassing, barbed wire should be installed atop the fence on an outward facing top guard at a 45 degree angle. *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.

[3] ASTM International provides two very useful standards; ASTM F1553-06, *Guide for Specifying Chain Link Fence*, and ASTM F2611-06, *Standard Guide for Design and Construction of Chain Link*. The Chain Link Fence Manufacturers Institute also has published useful specifications for fencing.

- *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.
- *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.

3.2.1.1.3 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: 1) standard or regular; 2) grating; 3) flattened; and 4) architectural or decorative.

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

3.2.1.1.4 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).

3.2.1.1.5 Barbed Wire

Barbed wire varies in gauge, coating weight, number of barbs, and spacing of barbs. If 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.

3.2.1.1.6 Razor or Concertina Wire

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

3.2.1.1.7 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, razor wire, or metal spikes – can make concrete fences more effective barriers. It should be noted, however, that concrete fences can enhance concealment.

3.2.1.1.8 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 wire, or metal spikes. When utilizing a wooden fence to delay entry, the vertical picket sections must be no wider than 1-3/4 inches and the horizontal sections should be 50 inches apart, located on the protected side of the building.

3.2.1.1.9 Electric Security Fencing

Electric security fences consist of a close wire grid supported by posts fitted with insulators. These fences can be simple 5 wire systems for wall top security, or multi-zoned systems with up to 50 wires for high security sites. Most industrial applications are 8 ft (2.4m) high with 20 wires and are fitted to the inside of the chain link perimeter fence.

Electric security fences come in two forms: 1) the all live wire "deterrent" fence that relies on the human fear of electric shock; or more commonly 2) the "monitored" fence, where in addition to the fear factor, the fence will detect cutting or climbing of the wires and trigger an alarm. Monitored fences are usually integrated with intruder alarm or access control systems and—increasingly—with surveillance cameras.

These fences are non-lethal but unpleasant for the offender who chooses to make contact. They do not use electrical current; instead electrical energy in the form of a "pulse" is discharged on to the wire about 45 times per minute. There are international safety standards for both the manufacture of the energizer monitor units as well as for building the fence structures.

3.2.1.2 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 (sometimes anchored to the ground)—can be effective vehicle barriers. Planters may be available in crash-rated configurations that meet the Department of Defense (DOD) K-ratings K4, K8, and K12. A K4-rated barrier is designed to stop a 15,000 pound vehicle traveling at 30 mph; a K8-rated barrier is designed to stop a 15,000 pound vehicle traveling at 40 mph; and a K12-rated barrier is designed to stop a 15,000 pound vehicle traveling at 50 mph.

Bollards are waist-high cylindrical posts—usually made of steel or concrete—that are anchored to the ground. They may be fixed position, removable posts for emergency access, or can be raised or lowered as needed. Bollards are available in crash-rated configurations meeting the Department of Defense (DOD) K-ratings; K4, K8, and K12.

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. Various concrete barriers are available in crash-rated configurations meeting the Department of Defense (DOD) K-ratings; K4, K8, and K12.

Standard *highway metal guard rails* may also be used as vehicle barriers, though they generally will not stop a vehicle impacting the guard rails in a perpendicular fashion. Steel barrier systems are available in crash-rated configurations meeting the Department of Defense (DOD) K-ratings; K4, K8. and K12.

There are also *operable barrier systems*, capable of being raised or lowered, that can serve to block vehicle entry and exits until authority has been granted for the vehicle to pass. These come in the form of operable bollards, operable wedges, and heavy reinforced operable gates. These are also available in crash-rated configurations meeting the Department of Defense (DOD) K-ratings; K4, K8, and K12.

3.2.1.3 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.

3.2.1.3.1 Gates

The number of pedestrian and vehicular gates should be kept to the minimum, consistent with efficient operation and safety. Local building codes must be taken into consideration when designing gates. 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.

3.2.1.3.2 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, and 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.

3.2.1.3.3 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, hand-carried tools, and some explosives (Gigliotti & Jason,

2004, p. 148). 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 can be weaker or stronger than its frame and the surface into which it is set. Hinges can be defeated. Measures can be taken to strengthen the doors by adding steel plate for reinforcement, anchoring frames, adding kick plates, using set screws in hinges or spot welding hinges. 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. As with any large opening, vehicular doors create a vulnerability of unrestricted pedestrian access.

3.2.1.3.4 Windows

The following are some different types of window glass:

- *Annealed* or *plate glass* has been manufactured to control residual stresses such that it can be subjected to fabrication. Regular plate, float, sheet, rolled, and some patterned surface glasses are examples of annealed glass. Annealed glass breaks into large shards that can cause serious injury, and building codes may restrict its use in places where there is a high risk of breakage and injury, such as door panels and fire exits.[4]
- *Tempered glass* is treated to resist breakage. Building codes require tempered glass for safety reasons because when the glass breaks, it fragments into small pieces rather than shards.
- *Wired glass* provides resistance against large objects, but may still shatter. It is often required for certain windows by fire codes (used to maintain fire ratings in fire-rated doors), which is the primary purpose of most wired glass.
- *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 installed in a frame, and the frame secured to the structure. 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* or *burglar-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 protect the window opening from being used as an access point.

[4] PPG Industries "Frequently Asked Questions."
< http://corporateportal.ppg.com/NA/IdeaScapes/resources/glass/lib-faq.htm > (11 March, 2009).

- *Window film (fragment retention film)* adheres to the interior surface of the glass, strengthens and holds the glass in place if broken, and can accomplish various other purposes. Window film can be designed, tested, and applied to:
    - Provide varying degrees of protection from intrusion or "smash and grab".[5] It can generally be defeated with repeated attacks.
    - Reduce injury from projectile shards of glass in case of an explosion or blast force.
    - Reduce injury form projectile penetration in case of extreme weather (i.e., hurricane or tornado).
- *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 nonetheless 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) that 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.[6]

3.2.1.3.5 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. Where such openings exceed 96 square inches[7], openings should be fortified with steel bars or grills, wire mesh, expanded metal, and fencing (and/or possibly protected with intrusion detection devices). Consideration should also be given to other objects that might be passed through an opening (contraband, weapons, etc.).

3.2.1.4 Locks

(See 3.3.4, *Locks*.)

3.2.2 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).

---

[5] Some with UL 972 anti-intrusion certification. See also British Standard BS 5544-1978.

[6] Abacus Construction Index, "About security shutters" < http://www.construction-index.com/usa-security-shutters.asp > (3 July 2008).

[7] As stated by Underwriter's Laboratories as the maximum opening size that a human cannot pass through.

- *Prevention of progressive collapse*, accomplished by structural design that prevents the loss of a primary structural member from causing the further failure of primary structural members beyond the local damage zone.
- *Redundancy of operating systems*, such as power, heating, ventilating, air-conditioning (HVAC) systems, and communications systems.

Consideration should be given to protecting HVAC systems by preventing 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, electrical power, and telecommunications. Utilities protection should include identifying critical systems rooms and closets with non-descriptive signage, where possible.

3.3 Physical Entry and Access Control

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

- Will the access control system be integrated with other systems, such as alarms, video surveillance, 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 video surveillance system?
- Will the various components of the access control system comply with all applicable building and fire codes?
- Will these systems be actively monitored by trained security personnel?

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. These systems are used to prevent the entry of unauthorized people, may control the introduction of prohibited items into a secure facility, and may control the unauthorized removal of tangible/intangible assets.

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 person's 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.

3.3.1 Access Control Barriers

Where 3.2, *Physical Barriers, and Site Hardening*, focuses on keeping unwanted parties out, this section, *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.

3.3.2 Electronic Access Control Systems

Electronic access control systems validate one or more credentials, which can be in the form of something you know, something that is inherent to you, or something you carry. Components of a full-featured system can include a credential reader, communication cabling, distributed processor, central database, software, supplementary interfaces to external systems, and applications for request-to-exit devices for applicable 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. At the other end of the spectrum are single locations with electronic pushbutton locks that have no central administration or connection, providing only minimal protection.

3.3.3 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 access through an access control portal.

3.3.4 Locks

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

3.3.4.1 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.

3.3.4.2 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.

3.3.4.3 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 safety codes, as there are specific and additional requirements with these doors that must be provided.

3.3.4.4 Credential-Operated Locks

Credential-operated locks rely on a unique card or other device 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 the information already stored in the system, and either activates the lock to permit entry or denies access.

3.3.4.5 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 is used, or a biometric feature is identified.

3.3.4.6 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.

3.3.4.7 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. Rapid entry key boxes may be monitored by the facilities alarm system to detect unauthorized opening or tampering. A key to the box should be supplied to emergency responders at the time of installation.

3.3.4.8 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.

3.3.5 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.

3.3.6 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).

3.3.7 Procedures and Controls

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

- Wearing of badges.
- Sharing of personal identification numbers (pins).
- Sharing of access cards.
- Tailgating or piggybacking.
- Challenging of unbadged persons.
- Number of access attempts allowed.
- Searching of packages, briefcases, and purses.
- Calibration of metal detectors.
- Use of explosives detectors.
- List of prohibited materials.
- Access hours and levels of access.
- Credential tampering and replacement.
- Accommodation of disabled or physically impaired persons.
- 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. A system transaction history should be maintained and available for review.

3.4 Security Lighting

Security lighting can augment other security measures such as physical barriers, intrusion detection systems, video surveillance, 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.
- Enhanced observation.

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.
- May call attention to a site that otherwise would remain hidden.

Typically, the purposes of security lighting—discouraging unauthorized entry, protecting employees and visitors on site, 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. Security lighting is also beneficial indoors.

3.4.1 Applications

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

- *Continuous*. In this application, illumination devices installed or deployed 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 turned on:
    - Automatically at random intervals;
    - Manually at random intervals;
    - When suspicious activity is detected,
    - When suspicious activity is suspected by security personnel; or
    - When suspicious activity is suspected by an intrusion detection system.
- *Controlled*. This lighting illuminates a limited space (such as a road) with little spill over 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.

3.4.2 Intensity

The right level or *intensity* of lighting depends on a site's overall security requirements. Lighting intensity[8] can be measured with instruments in lux and foot-candles, but as a general rule, "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 and comply with sustainability initiatives. A video surveillance system's needs may also dictate the proper level of lighting and CCT rating (measured in degrees Kelvin).

[8] 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).

3.4.3 Equipment

General security lighting equipment falls into the following categories:

- *Streetlight*. This projects a downward circular pattern 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.
- *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.
- *High mast lighting*. This is utilized mainly in parking lots and along highways and usually varies in height from 70 to 150 feet.

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

- *Incandescent*. These lamps are the least efficient, 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, and have poor color rendition for video surveillance, 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 video surveillance system by providing accurate color rendition.
- *High-pressure sodium*. These lamps are energy efficient and have a long life span, but poor color rendition for video surveillance system. 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 and provide poor color rendition for video surveillance system.
- *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 lighting sources has specific characteristics related to color rendition, life span, and startup times. In addition, some applications call for infrared lighting, which can be invisible to the naked eye but is useful for video 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; and
- 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), although it is subject to lightning strikes.

3.5 Intrusion Detection Systems

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*. When detection occurs, intruders may be delayed or denied by activating other measures.
- *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 (nuisance and unintentional) which generate costly and repeated deployment of security or law enforcement and maintenance personnel.
- 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) and its ongoing maintenance:

- 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.

3.5.1 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*, these alarm types include but are not limited to: point-to-point, area, buried cable, etc., and rely on a consistent reception level of its transmitted or reflected energy. When the energy level changes due to reflection or deflection, an alarm is transmitted.
    - *Infrared detectors*, available in both active and passive types. *Active detectors* include the infrared beam (transmitter/receiver) variety and alarm when either a total or pre-described volumetric loss of receiving signal occurs. *Passive infrared detectors (PIRs)* absorb invisible light energy and compare the actual energy to the established background energy. When the received energy fluctuates from ambient levels, an alarm is transmitted.
    - *Dual-technology motion detectors* are selectable to employ either or both microwave and infrared technologies in a single package. When using dual technologies, disturbances in both are required before an alarm is transmitted. Selecting both technologies reduces the false alarm rate and detection sensitivity.
    - *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.
- *Temperature sensors*. These devices trigger alarms when the air or surface temperature changes occur outside of predetermined limits.

- *Capacitance devices*. Often used with various metallic products such as safes and vaults, these devices detect changes in electrical capacitance. Low voltage is applied to the protected items. If an object or person approaches or touches the protected item, the voltage (non-harmful) discharges, altering the capacitance level and causing an alarm.
- *Impact sensors*. These detect sudden changes in air pressure.
- *Glass break sensors*. These detect the impact (pressure change) that causes the glass to break, the sound frequencies of breaking glass (by either sequential acoustical analysis or mechanical energy), and finally, broken glass hitting the floor/ground.
- *Duress/Panic alarms*. Wired switches, person-down devices, wireless pushbutton transmitters, "Lack of Motion" devices, emergency notification call boxes, etc., are some of the device types which are employed to protect personnel by transmitting assistance alarms. These alarms should be of the highest priority level.

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

3.5.2 Alarm Transmission, Monitoring, and Notification

Alarm 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 transmissions, monitoring, and notification mediums/devices should be supervised to better detect occurrences of tampering or interception. Regular tests should be performed to assure accuracy and timeliness of transmitted information.

Alarm monitoring, performed either in-house (proprietary) or on a contract basis, can have the system owner notified by several methods, including telephone, e-mail, and pager. A list of all persons to be notified and their associated phone numbers (and alternate contact information) should be developed.

3.5.3 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 without proper design engineering, if the selected components are not installed properly, or are not the correct components 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.

3.6 Video Surveillance

Video surveillance can be a valuable component of a facility's security program. Video surveillance is 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; and
- Assist with incident assessment.

The main elements of a video surveillance 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 provided by the lens to an electronic signal for transmission. The camera requires mounting hardware and sometimes a housing for protection against vandalism or environmental conditions (i.e. rain, snow, etc.).
- *Transmission medium*. The medium through which the signal generated from the camera is transmitted to equipment for viewing or recording, typically over coaxial cable, twisted-pair wire, network cable, optical fiber, or radio frequency 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:
    - Analog; or
    - Digital.
- *Control equipment*. This equipment is used to control what video is viewed and where the video is stored. This equipment can also be used to change the field of view of a specific camera via Pan, Tilt, and Zoom (PTZ) functions.

3.6.1 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 video surveillance 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 are the requirements for real-time monitoring or recorded video?

3.6.1.1 Camera Functional Requirements

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

1. *Target*. This may consist of:
   - Persons (individuals or groups);
   - Packages or objects;
   - Vehicles (individual); or
   - Traffic.
2. *Activity*. This could be:
   - Assault;
   - Vandalism;
   - Trespassing;
   - Robbery; or
   - Package or vehicle left unattended.
3. *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. The first purpose would be best served by use of a fixed camera position. A fixed camera position is static - it does not move. A fixed focal or variofocal lens is used with the camera to capture a defined field of view. A significant benefit associated with using a fixed camera is that the camera is always aimed at the desired field of view, which facilitates assessment. A Pan Tilt and Zoom (PTZ) camera, unlike a fixed camera position is able to pan (move side to side) or tilt (move up and down), enabling the operator to observe/access a much larger viewing area. In addition, a motorized variofocal lens is used to expand or narrow the field of view providing enhanced viewing flexibility. A potential drawback to PTZ camera applications is that the camera is out of position, unable to capture an event as it is happening. Most PTZ camera applications are used for assessment or video patrol purposes.

3.6.1.2 Monitoring Functional Requirements

If the purpose of the video surveillance system is to generate a response to specific incidents, then a trained person should monitor the system and respond accordingly. Even a trained 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 are available that 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 video surveillance system can be integrated with a security alarm system so that, for example, a door alarm can trigger a nearby PTZ camera to pre-position, aim at and zoom in on the person walking through the door.

- *Intelligent video analytics*. Video analytics come with various capabilities; 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.

3.6.1.3 Recording Functional Requirements

If a video recording is to be useful, 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 video surveillance 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 video surveillance system, with other workplace systems, and with the environment in which it is needed. This approach results in a video surveillance 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.

3.6.2 Cameras

The following subclauses detail key considerations in camera selection.

3.6.2.1 Lighting

Video surveillance system manufacturers specify the amount of illumination needed for minimum function and for maximum performance. Image quality is also affected by excessive shadows (light to dark ratio), lens glare, and backlighting.

3.6.2.2 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 variofocal (adjustable) focal length. Variofocal 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.

3.6.2.3 Camera Types

The following are the major types of video surveillance cameras:

- *Analog*. These cameras may be black-and-white or color. Analog cameras work well in both indoor and outdoor applications. 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 camera imager to significantly amplify the available light.
- *IP (Internet protocol)*. These digital cameras are available in either black-and-white or color. An IP camera combines both a camera and computer in one standalone unit. IP cameras use the "network" rather than a dedicated point-to-point cabling medium to transport the video signal. Like their analog counterparts, IP cameras require plenty of visible light to create a useful image. These cameras are available in either standard, or megapixel resolutions.
- *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 cameras 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 a grayscale palette to represent temperatures in black and white. Color may be artificially assigned so that, for example, cold objects are shown in varying shades of blue, while hot objects are shown in varying shades of red. Since thermal cameras "see" heat, they excel in low visibility conditions due to smoke, fog, foliage, and other low visibility conditions. These types of cameras are usually restricted to high security applications.

3.6.2.4 Power and Enclosures

The availability of power can greatly affect a video surveillance 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 extreme environments.

3.6.3 Transport Medium

The video signal generated by the camera must be transmitted to equipment to be viewed and/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 it does not work for IP-based systems without a media transformer. 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, unshielded twisted pair (UTP) cable (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.

3.6.4 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 video surveillance with other systems, such as access control and intrusion detection.

3.6.5 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. Digital Video Recorders (DVRs)* are devices which act like a VCR in that they have the ability to record and playback video images. A DVR, utilizing video connectors, inputs analog

video signals from a camera and records that video signal into a digital format for storage onto an internal hard drive, CD, DVD other medium or a combination of medium. Because the data can take considerable storage space, video compression can be utilized to reduce size by tracking patterns in the data, reducing resolution, averaging colors, or other methods. Most DVRs are controlled from a front panel and feature some forms of video analytics, search capabilities, and image enhancement, as well as the ability to connect through a network or phone line for remote access.

Network Video Recorders (NVRs) are similar to DVRs in that they record the video signal into a digital format; however, they do so in a server-based setting. A NVR is an internet protocol based device that sits on a network. Because they are IP based, NVRs can be managed remotely via a LAN, WAN, GAN, or over the Internet. The units communicate with digital cameras (or analog-to-digital devices) over the network, recording to network storage devices (server hard drives). While DVR controls for review and operation are on the front panel of the unit, NVRs must be accessed by software on a remote personal computer on the same network.

Video File Servers capture digital networked IP or IP-enabled cameras via an IP switched data network. The digital images are compressed and stored on hard drives in an array format.

3.6.6 Maintenance

When a video surveillance 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.

3.7 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. Other ASIS International documents address this topic in greater detail:

- ASIS CSO.1-2008, *Chief Security Officer (CSO) Organizational Standard*
- *Chief Security Officer (CSO) Guideline*
- *Private Security Officer (PSO) Selection and Training Guideline*

3.7.1 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. A security manager, regardless of title, can either be a direct employee or contractor to the organization.

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

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

- Physical security of the organization's assets
- Development and enforcement of security policy and procedures
- Preemployment screening
- Crisis management
- Business continuity planning
- Executive protection
- Investigation of security incidents
- Employee security awareness
- Law enforcement and governmental liaison
- Information protection
- Workplace violence prevention
- Termination support
- 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.

3.7.2 Security Officers

Organizations use *security officers* to provide, supplement, or complement other controls/measures where human presence and human decision making is needed, or—in some instances—to provide regulatory compliance. Security officers may be regulated by local ordinances and state laws.

3.7.2.1 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, and its location(s). Each organization must weigh the advantages and disadvantages of the two approaches. Some organizations use both proprietary and contract officers simultaneously. This is typically referred to as a "hybrid" security program.

Proprietary security officer programs may offer more direct control of personnel selection, screening, training, and supervision. In some instances, the proprietary approach may be more expensive than the contract approach. However, budget models should be developed by individual organizations to ensure a thorough understanding of the costs associated with each approach.

Contract security officer programs can shift some of the burden for hiring, training, and supervising from the organization to the security services firm. Some contractual agreements may also shift a portion of the liability for certain actions or incidents away from the organization. Contract security officer programs may provide greater flexibility in staffing levels. However, there can be trade-offs in terms of officer knowledge of specific organizational needs, and other program elements.

The structure of hybrid security organizations could vary greatly. In some instances, proprietary security managers administer programs staffed by contract officers. In other instances, contract officers work side-by-side with proprietary officers, and in still other organizations, contract officers are assigned only specific duties or provide on-call supplemental coverage.

In determining which structure is appropriate, organizations should identify their programmatic goals (based on a needs assessment), regulatory requirements, financial and management capabilities, performance expectations, cultural, and other factors. Where contract services are considered, legal counsel should review all contractual agreements prior to being signed.

3.7.2.2 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.
- Utilizing various security measures (doors, locks, alarms, video surveillance cameras, lighting, etc.).

3.7.2.3 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).
- 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.

3.7.2.4 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.

3.7.2.5 Equipment

Security officers may use or be issued equipment which is unique to the geographic region, post, or otherwise. Such equipment may include:

- *Communications devices*: In the form of a two way radio or mobile telephone device, the officer should be fully trained on their proper use. These items should be tested regularly in order to reduce the risk of device failure during a critical or emergency situation.
- *ID Badge*: Normally provides the officer with proper identification and access to areas which are either toured regularly or where an officer may need to enter during an emergency. ID Badges should be cared for, not defaced, and kept in a secure location when not in use. Badges may also contain electronic devices such as proximity or memory chips. These electronic devices can be damaged if not properly cared for.
- *Keys*: A fundamental tool to most security officer positions. Keys should be appropriately stored, and proper training for use of the key box is essential. Keys may be of differing varieties, including mechanical and electronic types. Care should be taken to ensure that all keys are accounted for at the beginning and end of shift. Additionally, proper care should be taken so that damage to keys does not occur.
- *Weapons/Restraints*: Not only must an officer be fully trained and deemed competent to use these devices, but also must be knowledgeable in the care of such devices.
- *Vehicles*: Safe driving techniques, regular vehicle inspections, and adherence to all standard procedures is a must for all security officers. Regular training and driving observations should be a consideration by security management.

3.7.3 Other Employees

In a broad sense, every employee should be considered part of the security program. Through a security awareness program, 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.

3.8 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.

3.8.1 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.

3.8.1.1 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.

3.8.2 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.

3.8.2.1 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).
- *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.

3.9 Security Convergence

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. In doing so, this guideline takes a traditional view of physical security measures. However, it is recognized that many security systems are increasingly being equipped with network connectivity to enable them to share a facility's network infrastructure. Planning for, implementation, and management of *converged security solutions* often requires partnerships between physical security, IT security, IT, and other corporate or organizational stakeholders. As this convergent environment matures, this treatment of Facility Physical Security Measures will be revised.

A BIBLIOGRAPHY

Alliance for Enterprise Security Risk Management (AESRM). (2007). *The convergence of physical and information security in the context of enterprise risk management.* Available: < http://www.aesrm.org >.

Alliance for Enterprise Security Risk Management (AESRM). (2006). *Convergent security risks in physical security systems and IT infrastructures.* Available: < http://www.aesrm.org >.

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. (2008). *Chief security officer (CSO) organizational standard.* ASIS CSO.1-2008. Alexandria, VA: ASIS International.

ASIS International. (2004). *Chief security officer (CSO) guideline.* ASIS GDL CSO 06 2004. Alexandria, VA: ASIS International.

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). *21st century security and CPTED: Designing for critical infrastructure protection and crime prevention*. Boca Raton , FL: CRC Press.

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/CGSB-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*. Available: < http://codewriters.com/asites/page.cfm?pageid=902&usr=clfma > [2008, March 15].

Craighead, G. (2003). *High-rise security and fire life safety* (2nd 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 Commerce, NIST, Information Technology Laboratory. (2005). *Federal information processing standard 201-1, personal identity verification (PIV) of federal employees and contractors.* Available: < http://csrc.nist.gov >.

Department of Commerce, NIST, Information Technology Laboratory. (2009). *SP 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) of Federal Employees and Contractors* Available: < http://csrc.nist.gov >.

Department of the Army. (2001). *Physical security training manual.* FM 3-19.30. Washington, DC: Department of the Army.

Federal Emergency Management Agency *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426)*

Fay, J. J. (1993 & 2008). *Encyclopedia of security management* (1st and 2nd 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. 148. 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 (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.

Pearson, R. (2007). *Electronic security systems: A manager's guide to evaluating and selecting system solutions.* Burlington, MA: Elsevier 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.*

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the general public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management*, ASIS leads the way for advanced and improved security performance. For more information, visit *www.asisonline.org.*

1625 Prince Street
Alexandria, Virginia 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org