

A S I S I N T E R N A T I O N A L

Facilities Physical Security Measures

ASIS GDL FPSM-2009

GUIDELINE





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.

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

Copyright © 2009 by ASIS International

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, Embark 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. Coppel, 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

1. SCOPE, SUMMARY, AND PURPOSE.....	1
1.1 SCOPE.....	1
1.2 SUMMARY	1
1.3 PURPOSE	1
2. TERMS AND DEFINITIONS	2
3. RECOMMENDED PRACTICE ADVISORY	4
3.1 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN (CPTED)	5
3.1.1 <i>Background</i>	5
3.1.2 <i>Strategies</i>	6
3.1.2.1 <i>Outer Layer</i>	9
3.1.2.2 <i>Middle Layer</i>	9
3.1.2.3 <i>Inner Layers</i>	9
3.2 PHYSICAL BARRIERS AND SITE HARDENING	10
3.2.1 <i>Physical Barriers</i>	10
3.2.1.1 <i>Fences and Walls</i>	10
3.2.1.1.1 <i>Walls</i>	11
3.2.1.1.2 <i>Chain-Link Fences</i>	11
3.2.1.1.3 <i>Expanded Metal and Welded Wire Fabric Fences</i>	12
3.2.1.1.4 <i>Ornamental Fences</i>	12
3.2.1.1.5 <i>Barbed Wire</i>	12
3.2.1.1.6 <i>Razor or Concertina Wire</i>	12
3.2.1.1.7 <i>Concrete Fences</i>	12
3.2.1.1.8 <i>Wooden Fences</i>	13
3.2.1.1.9 <i>Electric Security Fencing</i>	13
3.2.1.2 <i>Planters, Bollards, Concrete Barriers, and Steel Barricades</i>	13
3.2.1.3 <i>Premises Openings</i>	14
3.2.1.3.1 <i>Gates</i>	14
3.2.1.3.2 <i>Turnstiles</i>	14
3.2.1.3.3 <i>Doors</i>	14
3.2.1.3.4 <i>Windows</i>	15
3.2.1.3.5 <i>Other Openings</i>	16
3.2.1.4 <i>Locks</i>	16
3.2.2 <i>Site Hardening</i>	16
3.3 PHYSICAL ENTRY AND ACCESS CONTROL	17
3.3.1 <i>Access Control Barriers</i>	18
3.3.2 <i>Electronic Access Control Systems</i>	18
3.3.3 <i>Personnel Access Control</i>	19
3.3.4 <i>Locks</i>	19
3.3.4.1 <i>Mechanical Locks</i>	19
3.3.4.2 <i>Electrified Locks</i>	19
3.3.4.3 <i>Electromagnetic Locks</i>	19
3.3.4.4 <i>Credential-Operated Locks</i>	20
3.3.4.5 <i>Combination Locks</i>	20
3.3.4.6 <i>Biometric Locks</i>	20
3.3.4.7 <i>Rapid Entry Systems</i>	20
3.3.4.8 <i>Key System</i>	20
3.3.5 <i>Contraband Detection</i>	21
3.3.6 <i>Vehicle Access Control</i>	21
3.3.7 <i>Procedures and Controls</i>	21

3.4 SECURITY LIGHTING	22
3.4.1 Applications.....	23
3.4.2 Intensity.....	23
3.4.3 Equipment	24
3.5 INTRUSION DETECTION SYSTEMS	25
3.5.1 Intrusion Detection System Devices.....	26
3.5.2 Alarm Transmission, Monitoring, and Notification	27
3.5.3 Installation, Maintenance, and Repair	27
3.6 VIDEO SURVEILLANCE.....	28
3.6.1 Functional Requirements.....	28
3.6.1.1 Camera Functional Requirements	29
3.6.1.2 Monitoring Functional Requirements.....	29
3.6.1.3 Recording Functional Requirements.....	30
3.6.2 Cameras.....	30
3.6.2.1 Lighting.....	30
3.6.2.2 Lens Selection	31
3.6.2.3 Camera Types	31
3.6.2.4 Power and Enclosures.....	31
3.6.3 Transport Medium.....	32
3.6.4 Command Center.....	32
3.6.5 Recording.....	32
3.6.6 Maintenance	33
3.7 SECURITY PERSONNEL	33
3.7.1 Security Managers.....	33
3.7.2 Security Officers.....	34
3.7.2.1 Organization.....	34
3.7.2.2 Responsibilities	35
3.7.2.3 Preemployment Screening.....	35
3.7.2.4 Training	36
3.7.2.5 Equipment	36
3.7.3 Other Employees	37
3.8 SECURITY POLICIES AND PROCEDURES	37
3.8.1 Policies.....	38
3.8.1.1 Subjects to Address.....	38
3.8.2 Procedures.....	39
3.8.2.1 Subjects to Address.....	39
3.9 SECURITY CONVERGENCE	40
A BIBLIOGRAPHY.....	41

TABLE OF FIGURES

FIGURE 1: LAYERS OF SECURITY	8
------------------------------------	---

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.

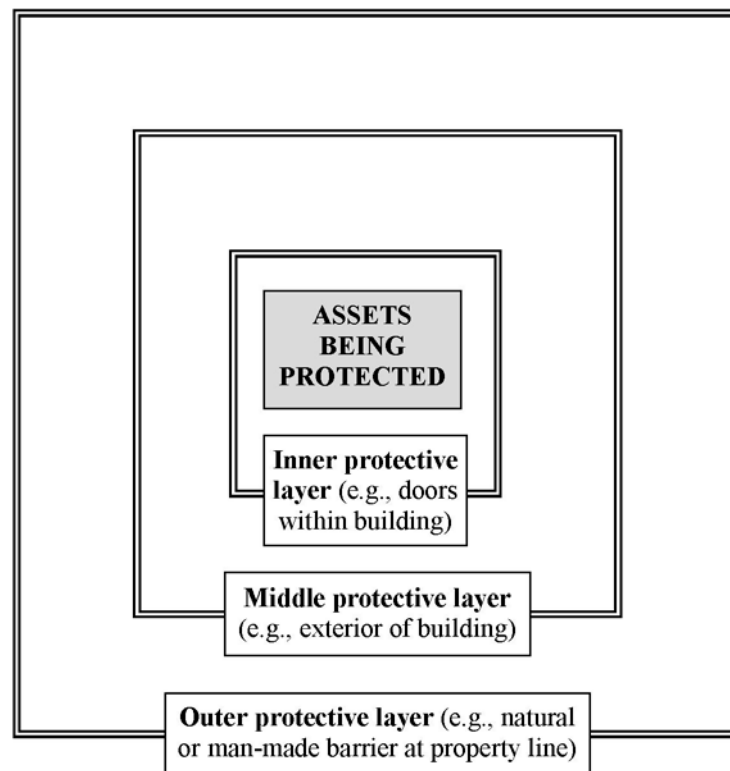


Figure 1: Layers of Security

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.