NFPA® 730

Guide for Premises Security

2008 Edition

NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA DOCUMENTS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA DOCUMENTS

NFPA codes, standards, recommended practices, and guides, of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in its codes and standards.

The NFPA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on this document. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making this document available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA 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.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does the NFPA list, certify, test or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Documents

Users of NFPA codes, standards, recommended practices, and guides should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments. An official NFPA document at any point in time consists of the current edition of the document together with any Tentative Interim Amendments and any Errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of Tentative Interim Amendments or corrected through the issuance of Errata, consult appropriate NFPA publications such as the National Fire Codes® Subscription Service, visit the NFPA website at www.nfpa.org, or contact the NFPA at the address listed below.

Interpretations of NFPA Documents

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing Committee Projects shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights asserted in connection with any items which are mentioned in or are the subject of NFPA codes, standards, recommended practices, and guides, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on these documents. Users of these documents are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

NFPA adheres to applicable policies of the American National Standards Institute with respect to patents. For further information contact the NFPA at the address listed below.

Law and Regulations

Users of these documents should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

For Further Information

All questions or other communications relating to NFPA codes, standards, recommended practices, and guides and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA documents during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101.

For more information about NFPA, visit the NFPA website at www.nfpa.org.

NFPA® 730

Guide for

Premises Security

2008 Edition

This edition of NFPA 730, *Guide for Premises Security*, was prepared by the Technical Committee on Premises Security. It was issued by the Standards Council on December 11, 2007, with an effective date of December 31, 2007, and supersedes all previous editions.

This edition of NFPA 730 was approved as an American National Standard on December 31, 2007.

Origin and Development of NFPA 730

The genesis of NFPA 730 was a request in 1994 to develop a burglary/security document. The project did not materialize until 2000, when the Standards Council appointed a committee to develop a premises security document. The committee responded by developing two documents, NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, and NFPA 730, *Guide for Premises Security*.

The 2006 edition of NFPA 730 updated references and made other minor modifications. The chapter on Industrial Facilities was modified to include key control measures, security operations, infrastructure protection, and a new section on water treatment facilities.

The 2008 edition of NFPA 730 has been updated to add new requirements for industrial security. Specifically, new material has been added for the protection of water treatment facilities. Other changes reflect corrections, updated references, and clarifications.

Technical Committee on Premises Security

Wayne D. Moore, *Chair*
Hughes Associates, Inc., RI [SE]

John C. Fannin III, *Secretary*
SafePlace Corporation, DE [SE]
Rep. Delaware Department of Safety and Homeland Security

Allan M. Apo, Insurance Services Office, Inc., NJ [I]
Randall I. Atlas, Atlas Safety & Security Design, Inc., FL [IM]
George Bish, Advanced Technologies, NC [IM]
Rep. National Burglar & Fire Alarm Association
Josh D. Brown, The Fauquier Bank, VA [U]
Rep. Virginia Crime Prevention Association/National Crime Prevention Council
Chadwick Callaghan, Marriott International, DC [U]
Rep. American Society for Industrial Security
Louis Chavez, Underwriters Laboratories Inc., IL [RT]
Thomas L. Chronister, Oxnard Police Department, CA [E]
David S. Collins, The Preview Group, Inc., OH [SE]
Rep. American Institute of Architects
Michael D. DeVore, State Farm Insurance Company, IL [U]
Rep. NFPA Industrial Fire Protection Section
Louis T. Fiore, L. T. Fiore, Inc., NJ [IM]
Rep. Professional Alarm Services Organizations of North America
Bruce Fraser, Tyco/SimplexGrinnell, MA [M]
Lauris V. Freidenfelds, The RJA Group, Inc., IL [SE]
Clark B. Goodlett, CH2MHILL, OR [SE]
Charles Hahl, The Protection Engineering Group, PC, VA [SE]
George E. Johnston, Loma Linda University, CA [U]
Rep. NFPA Health Care Section
Stewart Kidd, Loss Prevention Consultancy, Ltd., United Kingdom [SE]
Charles B. King III, US Department of Homeland Security, VA [E]
Jerry D. Loghry, EMC Insurance Companies, IA [I]
John M. Lombardi, Commercial Instruments & Alarm Systems, Inc., NY [IM]
Rep. Central Station Alarm Association
James Murphy, Vector Security Inc., PA [IM]
Isaac I. Papier, Honeywell, Inc., IL [M]
Rep. National Electrical Manufacturers Association
Rick D. Sheets, Brink's Home Security, TX [IM]
James P. Simpson, National Joint Apprentice & Training Committee, MN [L]
Rep. International Brotherhood of Electrical Workers
Tom G. Smith, Cox Systems Technology, OK [IM]
Rep. National Electrical Contractors Association
Bill H. Strother, Weingarten Realty Management Co., TX [U]
Rep. International Council of Shopping Centers
Michael Tierney, Builders Hardware Manufacturers Association, CT [M]
Raymond Walker, Town of Windsor, CT [E]

Alternates

Shane M. Clary, Bay Alarm Company, CA [IM]
(Alt. to J. M. Lombardi)
Scot Colby, Bayou Security Systems, Inc., LA [IM]
(Alt. to G. Bish)
David A. Dagenais, Wentworth-Douglass Hospital, NH [U]
(Alt. to G. E. Johnston)
Larry R. Dischert, Tyco/ADT Security Services, Inc., NJ [M]
(Alt. to B. Fraser)
Mark M. Hankewycz, The Protection Engineering Group, PC, VA [SE]
(Alt. to C. Hahl)
Robert G. Harrington, Pyramid Management Group, Inc., NY [U]
(Alt. to B. H. Strother)
Patrick D. Harris, Virginia Crime Prevention Association, VA [U]
(Alt. to J. D. Brown)
Thomas R. Janicak, Ceco Door Products, TN [M]
(Alt. to M. Tierney)
Richard A. Mahnke, The RJA Group, Inc., IL [SE]
(Alt. to L. V. Freidenfelds)
Patrick M. Murphy, Marriott International, Inc., DC [U]
(Alt. to C. Callaghan)
Steven A. Schmit, Underwriters Laboratories Inc., IL [RT]
(Alt. to L. Chavez)
James W. Tosh, Puget Sound Electrical JATC, WA [L]
(Alt. to J. P. Simpson)
William F. Wayman, Jr., Hughes Associates, Inc., MD [SE]
(Alt. to W. D. Moore)

Richard P. Bielen, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents on the overall security program for the protection of premises, people, property, and information specific to a particular occupancy. The Committee shall have responsibility for the installation of premises security systems.

Contents

NFPA 730

Guide for

Premises Security

2008 Edition

IMPORTANT NOTE: This NFPA document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notices and Disclaimers Concerning NFPA Documents." They can also be obtained on request from NFPA or viewed at www.nfpa.org/disclaimers.

NOTICE: An asterisk (*) following the number or letter designating a paragraph indicates that explanatory material on the paragraph can be found in Annex A.

Changes other than editorial are indicated by a vertical rule beside the paragraph, table, or figure in which the change occurred. These rules are included as an aid to the user in identifying changes from the previous edition. Where one or more complete paragraphs have been deleted, the deletion is indicated by a bullet (•) between the paragraphs that remain.

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in advisory sections of this document are given in Chapter 2 and those for extracts in the informational sections are given in Annex C. Editorial changes to extracted material consist of revising references to an appropriate division in this document or the inclusion of the document number with the division number when the reference is to the original document. Requests for interpretations or revisions of extracted text should be sent to the technical committee responsible for the source document.

Information on referenced publications can be found in Chapter 2 and Annex C.

Chapter 1 Administration

1.1 Scope.

1.1.1 This guide describes construction, protection, occupancy features, and practices intended to reduce security vulnerabilities to life and property.

1.1.2 This guide is not intended to supersede government statutes or regulations.

1.2 Purpose. The purpose of this guide is to provide criteria for the selection of a security program to reduce security vulnerabilities.

1.2.1 The guide addresses other considerations that are essential for protection of occupants, in recognition of the fact that security is more than a matter of having a security system.

1.2.2 The guide also addresses protective features and systems, building services, operating features, maintenance activities, and other provisions, in recognition of the fact that achieving an acceptable degree of safety depends on additional safeguards to protect people and property exposed to security vulnerabilities.

1.3 Application. This guide applies to both new and existing buildings, structures, and premises and provides guidance for designing a security system for buildings or structures occupied or used in accordance with the individual facility chapters outlined in Chapters 11 through 22.

1.4 Equivalency. Nothing in this guide is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety over those suggested by this guide.

1.5 Units and Formulas.

1.5.1 SI Units. Metric units of measurement in this guide are in accordance with the modernized metric system known as the International System of Units (SI).

1.5.2 Primary and Equivalent Values. If a value for a measurement as given in this guide is followed by an equivalent value in other units, the first stated value should be regarded as primary. A given equivalent value might be approximate.

1.5.3 Conversion Procedure. SI units have been converted by multiplying the quantity by the conversion factor and then rounding the result to the appropriate number of significant digits.

1.6 Title. NFPA 730, *Guide for Premises Security,* should be known as the "Premises Security Guide," is cited as such, and is referred to herein as "this guide" or "the guide."

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this guide and should be considered part of the recommendations of this document.

2.2 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 70®, National Electrical Code®, 2008 edition.

NFPA 72®, National Fire Alarm Code®, 2007 edition.

NFPA 80, *Standard for Fire Doors and Other Opening Protectives,* 2007 edition.

NFPA *101®, Life Safety Code®,* 2006 edition.

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* 2008 edition.

2.3 Other Publications.

2.3.1 ASTM Publications. ASTM International, 100 Barr Harbor Drive, West Conshohocken, PA 19428-2959.

ASTM F 567, *Standard Practice for the Installation of Chain-Link Fence,* 2000.

ASTM F 1090, *Standard Classification for Bank and Mercantile Vault Construction,* 1992.

ASTM F 1233, *Standard Test Method for Security Glazing Materials and Systems,* 1995.

ASTM F 1247, *Standard Specification for Intrusion Resistant Generic Vault Structures,* 1996.

2.3.2 BHMA Publications. Builders Hardware Manufacturers Association, 355 Lexington Avenue, 15th floor, New York, NY 10017.

ANSI/BHMA A156.1, *Butts and Hinges,* 2000.

ANSI/BHMA A156.2, *American National Standard for Bored and Preassembled Locks and Latches,* 1996.

ANSI/BHMA A156.4, *Door Controls — Closers,* 2000.

ANSI/BHMA A156.5, *Auxiliary Locks and Associated Products,* 2001.

ANSI/BHMA A156.12, *Interconnected Locks and Latches,* 1999.

ANSI/BHMA A156.13, *Mortise Locks and Latches Series 1000,* 2002.

ANSI/BHMA A156.16, *Auxiliary Hardware,* 2002.

ANSI/BHMA A156.17, *Self-Closing Hinges and Pivots,* 2004.

ANSI/BHMA A156.23, *Electromagnetic Locks,* 2004.

ANSI/BHMA A156.24, *Delayed Egress Locking Systems,* 2003.

ANSI/BHMA A156.25, *Electrified Locking Devices,* 2002.

ANSI/BHMA A156.26, *Continuous Hinges,* 2000.

ANSI/BHMA A156.28, *Recommended Practice for Keying Systems,* 2000.

ANSI/BHMA A156.30, *High Security Cylinders,* 2003.

ANSI/BHMA A156.31, *Electric Strikes and Frame Mounted Actuators,* 2001.

2.3.3 IESNA Publications. Illuminating Engineering Society of North America, 120 Wall Street, Floor 17, New York, NY 10005.

Lighting Handbook, 9th edition, 2000.

RP-20, *Lighting for Parking Facilities,* 1998.

2.3.4 SDI Publications. Steel Door Institute, managed by Wherry Associates, 30200 Detroit Road, Cleveland, OH 44145-1967.

ANSI/SDI A250.4, *Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors and Hardware Reinforcing,* 2001.

ANSI/SDI A250.8, *Recommended Specifications for Standard Steel Door Frames,* 2003.

2.3.5 UL Publications. Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

ANSI/UL 294, *Standard for Access Control System Units*, 1999, revised 2005.

ANSI/UL 305, *Standard for Panic Hardware*, 1997, revised 2004.

ANSI/UL 437, *Standard for Key Locks*, 2000, revised 2004.

ANSI/UL 608, *Standard for Burglary Resistant Vault Doors and Modular Panels*, 2004.

UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*, 2001.

ANSI/UL 687, *Standard for Burglary-Resistant Safes*, 2005.

ANSI/UL 752, *Standard for Bullet-Resisting Equipment*, 2005, revised 2006.

ANSI/UL 768, *Standard for Combination Locks*, 2006.

ANSI/UL 972, *Standard for Burglary Resisting Glazing Material*, 2002.

ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*, 2000, revised 2004.

UL 2058, *High Security Electronic Locks*, 2005.

ANSI/UL 3044, *Standard for Surveillance Closed Circuit Television Equipment*, 1999.

UL Burglary Protection Equipment Directory, http://database.ul.com/cgi-bin/XYV/template/LISEXT/1FRAME/index.htm

UL Security Equipment Directory, http://database.ul.com/cgi-bin/XYV/template/LISEXT/1FRAME/index.htm

2.3.6 U.S. Army Corps of Engineers Publications. U.S. Army Corps of Engineers, 10 South Harvard Street, Baltimore, MD 21201.

S/N 0-635-034/1069. "Physical Security." U.S. Army Field Manual 19-30, March 1979.

2.3.7 U.S. Department of Education. 400 Maryland Avenue, S.W. ROB-3, Room 3045, Washington, D.C. 20202–5344.

Final Regulations, November 1, 1999.

2.3.8 U.S. Government Publications. U.S. Government Printing Office, Washington, DC 20402.

S/N 027-000-01362-7, U.S. Department of Justice. *Vulnerability Assessment of Federal Facilities*, 1995.

20 U.S. Code 1092, "Higher Education Resources and Student Assistance."

2.3.9 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2003.

2.4 References for Extracts in Advisory Sections.

NFPA 72®, National Fire Alarm Code®, 2007 edition.
NFPA 99, *Standard for Health Care Facilities,* 2005 edition.
NFPA 5000®, Building Construction and Safety Code®, 2006 edition.

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter apply to the terms used in this guide. Where terms are not defined in this chapter or within another chapter, they should be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary,* 11th edition, is the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1* Approved. Acceptable to the authority having jurisdiction.

3.2.2* Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Guide. A document that is advisory or informative in nature and that contains only nonmandatory provisions. A guide may contain mandatory statements such as when a guide can be used, but the document as a whole is not suitable for adoption into law.

3.2.4 Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction

and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

3.2.5* Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

3.2.6 Shall. Indicates a mandatory requirement.

3.2.7 Should. Indicates a recommendation or that which is advised but not required.

3.3 General Definitions.

3.3.1* Access Control. The monitoring or control of traffic through portals of a protected area by identifying the requestor and approving entrance or exit.

3.3.2* Accessible Opening. An opening in a protected perimeter.

3.3.3 Alarm.

3.3.3.1* *False Alarm.* Notification of an alarm condition when no evidence of the event that the alarm signal was designed to report is found.

3.3.3.2* *Holdup Alarm.* An alarm that originates from a point where holdup protection is required, such as a bank teller window or store cash register.

3.3.3.3* *Local Alarm.* An alarm that annunciates at the protected premises.

3.3.4* Annunciator. A unit containing one or more indicator lamps, alphanumeric displays, computer monitor, or other equivalent means on which each indication provides status information about a circuit, condition, system, or location.

3.3.5 Area.

3.3.5.1* *Controlled Area.* A room, office, building, or facility to which access is monitored, limited, or controlled.

3.3.5.2 *Protected Area.* A protected premises or an area within a protected premises that is provided with means to prevent an unwanted event.

3.3.5.3* *Restricted Area.* A room, office, building, or facility to which access is strictly and tightly controlled.

3.3.6 Bar Lock. See 3.3.33.1.

3.3.7* Capacitance Sensor. A sensor that detects a change in capacitance when a person touches or comes in close proximity to an object.

3.3.8 Change Key. See 3.3.29.1.

3.3.9 Confidential Information. See 3.3.27.1.

3.3.10 Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [*72*, 2007]

3.3.11 Controlled Area. See 3.3.5.1.

3.3.12 Deterrent. Any physical or psychological device or method that discourages action.

3.3.13 Device.

3.3.13.1* *Duress Alarm Device.* An initiating device intended to enable a person at a protected premises to indicate a hostile situation.

3.3.13.2 *Signaling Device.* A device that indicates an alarm, emergency, or abnormal condition by means of audible, visual, or both methods, including sirens, bells, horns, and strobes.

3.3.14 Duress Alarm Device. See 3.3.13.1.

3.3.15 Duress Alarm System. See 3.3.46.1

3.3.16 Electromagnetic Lock. See 3.3.33.2.

3.3.17 Expanded Metal. An open mesh formed by slitting and drawing sheet metal, made in various patterns and metal thicknesses, with either a flat or irregular surface.

3.3.18 False Alarm. See 3.3.3.1.

3.3.19* Foil. An electrically conductive ribbon used for a sensing circuit.

3.3.20 Grandmaster Key. See 3.3.29.2.

3.3.21 Health Care Facilities. Buildings or portions of buildings in which medical, dental, psychiatric, nursing, obstetrical, or surgical care is provided. Health care facilities include, but are not limited to, hospitals, nursing homes, limited care facilities, clinics, medical and dental offices, and ambulatory care centers. [*5000*, 2006]

3.3.22 Hinge Dowel. A dowel or pin that projects from a door jamb into an opening in the edge of a door at its hinge that prevents removal of the locked door even if the hinges or hinge pins are removed.

3.3.23 Holdup Alarm. See 3.3.3.2.

3.3.24 Holdup Alarm System. See 3.3.46.2

3.3.25 Human/Machine Interface (HMI). The point at which people control or monitor the condition of an electronic premises security system.

3.3.26* Identification Credential. A device or scheme containing some knowledge (personal identification number or code) or a biometric identifier.

3.3.27 Information.

3.3.27.1* *Confidential Information.* Information to which access is restricted.

3.3.27.2 *National Security Information.* Designated information that requires protection in the interest of national defense or foreign relations of the United States, that is, information classified in accordance with Executive Order 12356 and not falling within the definition of Restricted Data or Formerly Restricted Data.

3.3.28 Intrusion Detection System. See 3.3.46.3.

3.3.29 Key.

3.3.29.1 *Change Key.* A key that will operate only one lock or group of keyed-alike locks, as distinguished from a master key.

3.3.29.2 ***Grandmaster Key.*** The key that operates two or more separate groups of locks, each of which is operated by different master keys.

3.3.30 Keypad. A device that is a type of human/machine interface (HMI) with numerical or function keys that can incorporate an annunciator or signaling device.

3.3.31* Line Supervision. Automatic monitoring of circuits and other system components for the existence of defects or faults that interfere with receiving or transmitting an alarm.

3.3.32 Local Alarm. See 3.3.3.3.

3.3.33 Lock.

3.3.33.1* ***Bar Lock.*** (1) A type of rim lock in which metal bars slide out from a central point on the door and into receivers on both sides of the door frame. (2) A metal rod or tube that slides through fittings affixed to the front of a file cabinet, bent at the top and secured with a combination lock, which holds the drawers closed.

3.3.33.2* ***Electromagnetic Lock.*** A door lock that uses an electrically actuated magnetic attraction to secure the door.

3.3.34* Microwave Sensor. An active intrusion sensor that detects the movement of a person or object through a pattern of microwave energy.

3.3.35* Monitoring Station. A facility that receives signals from electronic premises security systems and has personnel in attendance at all times to respond to these signals.

3.3.35.1* ***Central Station.*** A monitoring station that is listed.

3.3.35.2* ***Proprietary Station.*** A monitoring station under the same ownership as the property(ies) being monitored.

3.3.36 National Security Information. See 3.3.27.2.

3.3.37 Perimeter Protection. A scheme of protection that uses devices to detect intrusion at points of entry into a protected area such as doors, windows, and skylights.

3.3.38 Post Orders. The written procedures from the facility management that list the duties and direct the actions of security officers.

3.3.39 Protected Area. See 3.3.5.2.

3.3.40* Reader. A device that allows an identification credential to be entered into an access control system.

3.3.41 Restricted Area. See 3.3.5.3.

3.3.42* Screens. An array of wires usually interwoven every 6 in. either horizontally or vertically on a screen or alarm screening that protects areas or openings, such as skylights and crawl spaces.

3.3.43 Signaling Device. See 3.3.13.2.

3.3.44 Supervised Lines. Interconnecting lines in an alarm system that are electrically supervised against tampering. *(See also 3.3.31, Line Supervision.)*

3.3.45 Surreptitious Entry. The unauthorized entry into a facility or security container in a manner such that evidence of the entry is not discernable under normal circumstances.

3.3.46 System.

3.3.46.1* ***Duress Alarm System.*** A system that controls duress alarm devices and operates in private or public.

3.3.46.2* ***Holdup Alarm System.*** A system or portion thereof in which the initiation of a holdup signal is either semiautomatic or manual.

3.3.46.3* ***Intrusion Detection System.*** A system designed to detect the entry or attempted entry of a person or vehicle into a protected area.

3.3.47 Top Guard. Antipersonnel device, usually of barbed or concertina wire, installed at the tops of fences and along roof edges.

3.3.48 Unauthorized Person. A person who does not have permission to enter a protected premises or is not authorized to have access to specific confidential information.

3.3.49 Vault. A windowless enclosure of heavy, reinforced construction with walls, floor, roof, and door(s) designed and constructed to delay penetration sufficiently to enable the timely arrival of response forces.

3.3.50 Zone. A defined area within a protected premises.

Chapter 4 General

4.1 Fundamental Recommendation. A security program should be based on a security vulnerability assessment as described in Chapter 5.

4.2 Classification of Facilities.

4.2.1 Facility Classification. The use of a building or structure, or portion of a building or structure, should be classified in accordance with Chapters 11 through 21. Facility classification should be subject to the ruling of the authority having jurisdiction (AHJ) where there is a question of proper classification in any individual case.

4.2.2 Educational Facilities. Educational facilities include primary and secondary schools and colleges and universities.

4.2.3 Health Care Facilities. Health care facilities are used for purposes of medical service or other treatment to four or more persons simultaneously where one of the following conditions exist:

(1) The occupants are mostly incapable of self-preservation because of age or physical or mental disability or because of security measures not under the occupants' control.
(2) The facility provides, on an outpatient basis, treatment for patients that renders the patients incapable of taking action for self-preservation under emergency conditions without the assistance of others.
(3) The facility provides, on an outpatient basis, anesthesia that renders the patients incapable of taking action for self-preservation under emergency conditions without the assistance of others.

4.2.4 One- and Two-Family Dwellings. These are residential facilities containing one or two dwelling units that are occupied primarily on a permanent basis.

4.2.5 Lodging Facilities. The term *lodging facility* is an all-inclusive designation for facilities that provide housing and generally, but not always, food, beverage, meeting facilities, retail shops, recreational facilities, and other services. Hotels, motels, motor hotels, resort hotels, inns, country clubs, and conference centers are among the varieties of lodging facilities; which term is applied is based primarily on differences in layout and design.

4.2.6 Apartment Buildings. Apartment buildings generally are defined as buildings containing three or more dwelling units, each with independent cooking and bathroom facilities. They can also be referred to as apartment houses and garden apartments.

4.2.7 Restaurants. Restaurants include fast food establishments, convenience stores, walk-up-style facilities, and larger assembly-type facilities with full table service, lounges, and so forth.

4.2.8 Shopping Centers. A shopping center is a group of retail and other commercial establishments that is planned, developed, and managed as a single property.

4.2.9 Retail Establishments. Retail establishments are primarily engaged in the direct sale of goods and products to consumers.

4.2.10 Office Buildings. An office building is a facility used for office, professional, or service-type transactions, including but not limited to storage of records and accounts.

4.2.11 Industrial Facilities. An industrial facility is a facility in which products are manufactured or in which processing, assembling, mixing, packaging, finishing, decorating, or repair operations are conducted.

4.2.12 Parking Facilities. A parking facility is a structure or space where the primary use is storage of vehicles.

4.2.13 Mixed Facilities. A mixed facility is a facility in which two or more classes of facility exist in the same building or structure and where such classes are intermingled so that separate safeguards are impracticable.

4.3 System Design and Installation. Any security system, building service equipment, feature of protection, or safeguard provided for security should be designed, installed, and approved in accordance with applicable NFPA codes and standards, the manufacturer's specifications, applicable UL standards, the AHJ, and nationally recognized industry standards and practices.

4.4 Maintenance. Whenever or wherever any device, equipment, system, condition, arrangement, level of protection, or any other feature is recommended by this guide, such device, equipment, system, condition, arrangement, level of protection, or other feature should thereafter be maintained unless the guide exempts such maintenance.

Chapter 5 Security Vulnerability Assessment

5.1 General.

5.1.1* Security planning should begin with a security vulnerability assessment (SVA), which is a systematic and methodical process for the following:

(1) Examining ways an adversary might exploit an organization's security vulnerabilities to produce an undesired outcome
(2) Developing countermeasures to address adversarial events

5.1.2 An SVA is a technique for assessing the current status of an organization's threat exposures, security features, and preparedness and can be used in developing and strengthening both security and safety layers of protection.

5.2 Application. An SVA usually involves a seven-step process.

5.2.1 Step 1: Formation of Team. The process should begin with the formation of a team of personnel from all organizational areas. Commonly, the individual responsible for an organization's security serves as team leader.

5.2.2 Step 2: Organization/Facility Characterization. Step 2 involves a characterization of an organization and the facilities to be protected. It includes identification of assets (i.e., people, property, information, and products); physical features and operations; laws, regulations, and corporate policies; social and political environment and internal activity (i.e., community resources, crime statistics, internal activities, and loss experience); and "current layers of protection," including both site security features and safety measures.

5.2.3 Step 3: Threat Assessment. The next step is conducting a threat assessment. The process includes a classification of critical assets, identification of potential targets, consequence analysis (effect of loss, including potential off-site consequences), and the definition of potential threats (by identifying potential adversaries and what is known about them).

5.2.4 Step 4: Threat Vulnerability Analysis. The next step is conducting a threat vulnerability analysis that identifies actual and potential threat scenarios and estimates a relative security risk level. The relative security risk level is a function of determining the severity of the consequences of an adversarial event, the potential for such an attack, and the likelihood of adversary success in carrying out the anticipated event or activity.

5.2.5* Step 5: Definition of Specific Security Countermeasures. In this step, specific security countermeasures are defined. All information from the preceding steps, including characterization, threat assessment, and vulnerability analysis, is considered. An effective countermeasure is one that drives improvements in mitigating the defined threats and results in a reduction in the security risk level.

5.2.6 Step 6: Assessment of Risk Reduction. Taking into account the countermeasures defined in Step 5, this step reassesses the relative security risk levels developed in Step 4 and considers additional security risk reduction measures (security countermeasures) where appropriate.

5.2.7 Step 7: Documentation of Findings and Tracking of Implementation. Findings and recommendations are documented in a report and the implementation of accepted recommendations is tracked.

Chapter 6 Exterior Security Devices and Systems

6.1 General. This chapter covers the application of exterior security devices and systems.

6.2 Application. Exterior security devices and systems can be used in providing perimeter protection to a facility.

6.3 Exterior Security Devices and Systems.

6.3.1 Exterior security devices and systems include fences and other physical barriers, protective lighting, ironwork (e.g., bars and grills), glazing materials, passive barriers, and electronic security devices. Depending on their construction, walls, floors, roofs, doors, and windows can also be considered exterior security devices and systems. Compliance with applicable fire and building code requirements in any occupancy should be taken into consideration when any physical barriers are utilized or installed.

6.3.2 Perimeter protection defines the physical limits of a property, which can be the exterior boundaries of a premises or the walls, floor(s), and ceiling(s) of a building.

6.4 Physical Barriers. Physical barriers can be of two general types — natural and structural. Natural barriers include mountains, cliffs, canyons, rivers, or other terrain that is difficult to traverse. Structural barriers are man-made devices, such as fences, walls, floors, and roofs. Fences are the most common perimeter barrier. Chain-link fencing is the most popular type of fence in use today — it is simple to install, relatively inexpensive, and low in maintenance costs.

6.4.1 Application of Chain-Link Fencing. Chain-link fencing can be used in almost any application where there is a need for defining the physical boundaries of a facility or for a perimeter barrier that serves a security function. It is available in a variety of heights and materials and is installed to various specifications. To be most effective, a chain-link fence should be designed and installed to nationally recognized standards. The standards for the manufacture, design, and installation of chain-link fencing are published by the American Society for Testing and Materials (ASTM). ASTM F 567 provides materials specifications, design requirements, and installation procedures for chain-link fencing.

6.4.2 Design of Chain-Link Fencing. A chain-link fence consists of posts, braces, rails or tension wires, fabric, the fence top, and entrances. All materials used in the construction of the fence should be zinc-coated, aluminum-coated, or polyvinyl chloride–coated to afford protection from the elements. Subsection 6.4.3 describes important factors to be considered in the construction, design, and installation of a chain-link fence, based on ASTM F 567 requirements.

6.4.3 The Fence Line. The fence line should be as straight as possible to provide for ease of observation. Clear zones should be provided on both sides of the fence to provide an unobstructed view. If practical, the fence should be located no closer than 50 ft (15.2 m) to buildings or outside storage areas and 20 ft (6.1 m) to other areas, such as parking areas, that could afford concealment for an intruder. Utility poles in close proximity to the fence should be provided with a security collar, a device that prevents climbing the pole to a height greater than that of the fence.

6.4.3.1 Signs. "No Trespassing" or "Private Property" signs should be securely attached to the fence fabric. These signs should be placed at various points along the fence line to avoid accidental or inadvertent trespass by an intruder.

6.4.3.2 Height. Chain-link fences are available in heights ranging from 4 ft (1.2 m) for residential application to 12 ft (3.7 m) or more for use in prison facilities. In industrial or commercial security applications, the minimum recommended height for a chain-link fence is 8 ft (2.4 m), including 7 ft (2.1 m) of fabric (the chain-link material) and a top guard (discussed in 6.4.3.7) of approximately 1 ft (0.3 m). However, some fence manufacturers recommend that the fence height be 9 ft (2.7 m), at which height the top of the fence is out of standing reach of most intruders.

6.4.3.3 Posts. The posts for a chain-link fence include terminal (end, corner, and gate) posts and line posts. For a fence with 7 ft (2.1 m) high fabric, the posts should be set in concrete at a minimum depth of 36 in. (0.9 m) and the surface of the concrete crowned to shed water. The posts should be set an additional 3 in. (76 mm) deeper for each 1 ft (0.3 m) increase in the height of the fence. The diameter of the hole for a terminal post should be at least 12 in. (30.5 cm) and 9 in. (22.9 cm) for a line post. Other installation methods are acceptable if they provide equivalent or superior strength to that developed using concrete footings. Line posts should be spaced equidistant at intervals not exceeding 10 ft (3.0 m), measured from center to center between terminal posts. End posts should be set within 2 in. (5.1 cm) of building walls.

6.4.3.4 Bracing. Terminal posts should be braced to each adjacent line post. Diagonal braces should be securely fastened to the terminal post and the line post or to their footings, so that the angle between the brace and the ground at the line post is no more than 50 degrees. When a top rail (discussed in 6.4.3.5.1) is used, the brace is attached at the halfway point of the terminal post; when the top rail is omitted, the brace is attached at the two-thirds point above grade. For horizontal bracing, the braces are securely fastened with truss rods at mid-height of the adjacent line posts and the terminal post.

6.4.3.5 Rails and Tension Wires.

6.4.3.5.1 A top rail or top tension wire should be provided as support for the fence fabric. The top rail should be supported at each line post, so that a continuous brace from end to end of each stretch of fence is formed, and should be securely fastened to each terminal post. The top rail, usually in 18 ft (5.5 m) lengths, is joined with connectors that allow for expansion and contraction. On fences 12 ft (3.7 m) and more in height, a center rail is necessary.

6.4.3.5.2 A top rail improves the appearance of the fence but also provides a handhold for someone attempting to climb over the fence. For this reason, it is usually recommended that the top rail be omitted and replaced with a top tension wire. The top tension wire should be stretched taut, free of sag, from end to end of each stretch of fence, at a height within 1 ft (0.3 m) of the top of the fabric, and be securely attached to the terminal posts. A bottom tension wire that is within the bottom 6 in. (15.2 cm) of the fabric should also be provided. Some fences have a bottom rail in place of the bottom tension wire.

6.4.3.6 Fabric. The fabric for a chain-link fence should be steel wire, No. 9 gauge or heavier. The wire is interwoven in a diamond shaped pattern to form a continuous mesh without knots or ties except in the form of twisting or knuckling of the ends of the wire to form the selvage of the fabric. The mesh openings should not be larger than 2 in. (5.1 cm) per side.

6.4.3.6.1 "Twisting" describes the type of selvage obtained by twisting adjacent pairs of wire ends together in a closed helix of three full twists and cutting the wire ends at an angle to provide sharp points. The wire ends beyond the twist should be at least ¼ in. (6 mm) long. "Knuckling" describes the type of selvage obtained by interlocking adjacent pairs of wire ends and then bending the wire ends back into a closed loop.

6.4.3.6.2 In a commercial or industrial security application, the fabric should have twisted selvage at the top; for safety reasons, it is usually recommended that the bottom selvage be knuckled. On fences less than 6 ft (1.8 m) in height and in residential applications, both the top and bottom selvages should be knuckled, also for safety reasons.

6.4.3.6.3 The fabric should be stretched taut and securely fastened to the posts at 15 in. (38.1 cm) intervals. The top edge of the fabric should be fastened to the top rail or top tension wire at intervals not exceeding 2 ft (0.6 m) and the

bottom edge of the wire to the bottom rail or bottom tension wire at intervals not exceeding 2 ft (0.6 m).

6.4.3.6.4 The bottom of the fabric should extend to within 2 in. (5.1 cm) of hard ground or paving. On soft ground, the fabric should extend below the surface of the soil, or U-shaped stakes, approximately 2 ft (0.6 m) in length, can be driven into the ground to secure the fabric. Culverts, troughs, or other openings that are larger than 96 $in.^2$ (0.06 m^2) in area should be protected by fencing or iron grills to prevent unauthorized entry while allowing for proper drainage.

6.4.3.7 The Top Guard. The top of the fence, including all entrances, should be provided with a top guard, or overhang, to deter attempts at climbing the fence. A top guard consists of three strands of No. 12 gauge barbed wire that are securely fastened to metal supporting arms, usually 18 in. (45.7 cm) in length, attached to the fence posts either vertically or at an angle of approximately 45 degrees.

6.4.3.7.1 When the top guard is angled, the arms, or outriggers, should be of sufficient strength to withstand a weight of 250 lb (113.4 kg) applied at the outer strand of barbed wire. The top strand of barbed wire should be at a height 1 ft (0.3 m) vertically above the top of the fabric, with the other wires spaced uniformly along the arm.

6.4.3.7.2 The top guard can be installed facing either inward or outward from the fence line. It is usually recommended that the top guard face outward, since it is believed that this configuration makes it more difficult for an intruder to climb over the fence from the outside. If the fence is on the property line of the facility, however, the top guard should be installed facing inward; otherwise, it will extend over the property of the adjoining neighbor or over public streets or highways. Some fences have a double overhang, in the shape of a "V", making it more difficult to climb the fence from either side.

6.4.3.7.3 Barbed wire made of spring steel can be formed into concertina coils and used in place of the top guard for protecting the top of the fence. Because of the coiled configuration, concertina does not require supporting arms and is usually attached to the top of the fence with wire ties and clamps.

6.4.3.7.4 Another material used to protect the top of a chain-link fence is barbed tape, also referred to as razor ribbon. Barbed tape is manufactured of stainless steel, 0.025 in. (0.64 mm) thick and 1 in. (2.54 cm) or 1¼ in. (3.2 cm) wide, with needle-sharp barbs that are spaced on 4 in. (10.2 cm) centers. Barbed tape should be securely fastened to the top of the fence and to a top wire that is stretched taut between vertical extensions on the line and terminal posts. Manufacturers of barbed tape recommend that the material be used on fences having a minimum height of 7 ft (2.1 m) so as to avoid the possibility of contact with pedestrian traffic. Barbed tape should never be used at heights below 7 ft (2.1 m).

6.4.4 Entrances. The number of entrances should be kept to a minimum, consistent with safe and efficient operation of the facility. Entrances can be designed for vehicular traffic or for pedestrians and are usually closed by a gate or turnstile.

6.4.4.1 Gates can be single- and double-swing for walkways, multifold for wide entrances, double-swing and overhead single- and double-sliding for driveways, cantilever single- and double-sliding for driveways where an overhead track would be in the way, or vertical-lift for special purposes such as loading docks. Any of these gates can be motor operated.

6.4.4.2 The frames for gates should be constructed of tubular members that have been welded together at the corners or assembled with fittings and should be provided with truss rods or braces, as required, to prevent sagging or twisting. The fabric should be the same as that used for the fence and should be fastened to the gate frame at 15 in. (38.1 cm) intervals. The gate should be mounted so that it cannot be lifted off its hinges. The bottom of the gate should be within 2 in. (5.1 cm) of the ground.

6.4.4.3 Turnstiles are utilized in fences for the control of pedestrian traffic and are available in two heights. Waist-height turnstiles are about 3 ft (0.9 m) high and usually are used to count the number of personnel going through an access point; they do not provide any degree of security unless constantly attended. Full-height turnstiles, which are usually about 7 ft (2.1 m) high, completely surround individuals as they pass through. Full-height turnstiles do function as security barriers, since they can be locked to prevent access or automated through the use of an access control system.

6.4.4.4 When entrances are not staffed, they can be securely locked, illuminated during the hours of darkness, and periodically inspected. Semi-active entrances, such as railroad siding gates, or gates used only during peak traffic flow periods, can be kept locked except when actually in use.

6.4.5 Locks.

6.4.5.1 Locks are essential parts of fences and the protection they provide. Gates are usually locked by means of a padlock. Padlocks can be operated by keys or combinations, with key-operated padlocks the preferred type. The padlock should have a shrouded shackle, to resist sawing and bolt cutters, and should lock on both sides of the shackle (heel-and-toe locking). The padlock should be installed so that it cannot be easily attacked from the street side with a hammer.

6.4.5.2 If a chain and padlock are used to secure the gate, the chain, as a minimum, should be case-hardened. If possible, the chain should be installed so that the lock is on the inside of the gate when the gate is closed. The keys to the padlocks should be strictly controlled.

6.4.6 Lighting. Lighting should be provided along the fence line and at all entrances to enhance visibility and deter intrusion.

6.4.6.1 Table 6.4.6.1 provides minimum lighting levels that can be used for fences.

Table 6.4.6.1 Recommended Minimum Illumination Levels for Fencing

Location	Minimum Illumination* (footcandles)
Perimeter of outer area	0.15
Perimeter of restricted area	0.4
Vehicular entrances	1.0
Pedestrian entrances	2.0
Entrances (inactive)	0.1

*On horizontal plane at ground level.
Source: U.S. Army Corps of Engineers, Field Manual 19-30.

6.4.6.2 Information on recommended lighting levels for fences, including entrances, is also provided in the IESNA *Lighting Handbook*.

6.4.7 Maintenance.

6.4.7.1 The area on either side of the fence should be kept clear of trees, shrubbery, and tall grass that could afford concealment for an intruder. Items that might assist an intruder in climbing over the fence, such as boxes, containers, vehicles, and equipment, should be located away from the fence.

6.4.7.2 To be most effective, the fence should be well maintained. Breaks or damage to the fence should be repaired promptly. The fence should be inspected on a regular basis to check for any cuts or openings that can be camouflaged.

6.5 Protective Lighting. Protective lighting is a valuable and inexpensive deterrent to crime. It improves visibility for checking badges and people at entrances, inspecting vehicles, preventing illegal entry, and detecting intruders both outside and inside buildings and grounds.

6.5.1 Lighting Terms.

6.5.1.1 *Luminous flux* refers to the gross amount of light generated by a source, irrespective of the intensity of the light in a given direction. The unit of luminous flux is the *lumen* (lm).

6.5.1.2 *Luminous intensity* is the luminous flux per unit solid angle in the direction in which the flux is emitted. The unit of luminous intensity is the *candela* (cd). At one time, candela was called candle or candlepower.

6.5.1.3 *Illuminance* is the density of incident luminous flux on a surface. Illuminance is the standard measure for lighting levels and is measured in *footcandles* (fc) (1 lm/ft^2) or *lux* (lx) (1 lm/m^2).

6.5.1.4 Luminance. This relates to the luminous intensity of a surface in a given direction per unit area of that surface as viewed from that direction and is often incorrectly referred to as "brightness." The unit of luminance is the candela per square meter (cd/m^2) [candela per square foot (cd/ft^2)].

6.5.2 Principles of Protective Lighting. Protective lighting should attempt to accomplish the objectives in 6.5.2.1 through 6.5.2.9.

6.5.2.1 Illumination of all exterior areas in a facility, including pedestrian and vehicular entrances, the perimeter fence line, sensitive areas or structures within the perimeter, and parking areas, should be provided in accordance with the recommendations of Table 6.5.2.1.

6.5.2.1.1 Information on recommended lighting levels for outdoor protective lighting is also provided in the IESNA *Lighting Handbook*.

6.5.2.2 Intruders should be discouraged or deterred from attempts at entry by making detection certain. Proper illumination can lead a potential intruder to believe detection is inevitable.

6.5.2.3 A glare that handicaps guards and annoys passing traffic and occupants of adjacent properties should be avoided.

6.5.2.4 The glare should be directed at intruders, where appropriate, as a means of handicapping them.

6.5.2.5 Guard posts and video surveillance cameras should be in low-light locations to render their positions harder for intruders to pinpoint.

Table 6.5.2.1 Recommended Minimum Intensities for Outdoor Protective Lighting

Location	Minimum Intensities* (footcandles)
Perimeter of outer area	0.15
Perimeter of restricted area	0.4
Vehicular entrances	1.0
Pedestrian entrances	2.0
Sensitive inner areas	0.15
Sensitive inner structures	1.0
Entrances (inactive)	0.1
Open yards	0.2
Docks and piers	1.0

*On horizontal plane at ground level.
Source: U.S. Army Corps of Engineers, Field Manual 19-30.

6.5.2.6 Redundancy should be provided so that a single lamp outage does not result in a dark spot vulnerable to intrusion.

6.5.2.7 Complete reliability should be provided such that, in the event of a power failure, standby illumination is available.

6.5.2.8 Protective lighting should be resistant to vandalism and sabotage. Fixtures should be installed high, out of reach of potential intruders, and be of the vandal-resistant type.

6.5.2.9 Protective lighting should be covered under a maintenance agreement such that repairs are made in a timely fashion.

6.5.3 Types of Light Sources. Electric lamps are the principal source of light in common use. They convert electrical energy into light or radiant energy and are classified into three categories: incandescent, fluorescent, and high-intensity discharge.

6.5.3.1 Incandescent Lamps.

6.5.3.1.1 In an incandescent lamp, current is run through a wire or filament that heats up and glows (incandesces), giving off light. The filament, usually of tungsten, is enclosed in a glass tube that contains a specialized atmosphere, usually of argon and nitrogen, that prevents oxidation of the filament at elevated temperatures. Compared to other light sources, incandescent lamps have a low initial cost, a relatively short life (500 hours to 4000 hours), and low efficiency in lumens per watt (17 LPW to 22 LPW) of electrical energy; however, they give a generally pleasant color rendition, are easy to dim, and are readily controlled.

6.5.3.1.2 Included in the category of incandescent lamps is the tungsten halogen (or quartz iodide) lamp. Tungsten halogen lamps improve the rate of depreciation of the light output of a standard incandescent lamp, called lamp lumen depreciation, by enclosing the tungsten filament in a quartz tube containing a halogen gas. This design deters tungsten particles from depositing on the bulb wall, as is common with incandescent lamps and which causes blackening of the bulb. The design helps these particles re-deposit on the filament, increasing lamp life. Efficiency and color rendition of tungsten halogen and standard incandescent lamps are approximately the same.

6.5.3.2 Fluorescent Lamps. The fluorescent lamp produces light when an electrical discharge generates ultraviolet energy that activates fluorescent powders on the walls of a glass tube. A choice of phosphors used in the fluorescent lamp allows for the manufacture of lamps with different color characteristics.

To operate, a fluorescent lamp requires auxiliary equipment, called a ballast, that acts as a current-limiting device and provides the voltage necessary to ensure ignition of the arc. Fluorescent lamps provide good color rendition, high lamp efficiency (67 LPW to 100 LPW), and long life (9,000 hours to 17,000 hours). They are temperature sensitive, with low ambient temperatures decreasing their effectiveness. Fluorescent lamps cannot project light over long distances and so are not desirable as floodlights.

6.5.3.3 High-Intensity Discharge (HID) Lamps. HID lamps include mercury vapor, metal halide, and high-pressure sodium.

6.5.3.3.1 Mercury Vapor Lamps. These were the first of the HID lamps to be developed; light is produced by the passage of an electric current through mercury vapor. These lamps are constructed of an inner quartz arc tubing containing an electrode at both ends. The tube contains a starting electrode that starts the mercury vapor oxidation process necessary for ignition. The entire assembly is covered by an outer glass shell. Like fluorescent lamps, a ballast is necessary to limit the current and provide the required voltage. Mercury vapor lamps have the lowest efficacies of the HID family, rapid lumen depreciation, and a low color-rendering index. Because of these characteristics, other HID sources have replaced mercury vapor lamps in many applications.

6.5.3.3.2 Metal Halide Lamps. These are similar in design and operation to mercury vapor lamps; however, they use metal halides in addition to the mercury to produce better color rendition. Metal halide lamps have an efficiency (80 LPW to 115 LPW) approximately 50 percent higher than mercury vapor lamps but have a much shorter lamp life (6000 hours). They are used where efficiency, color, and light control are most important.

6.5.3.3.3 High-Pressure Sodium (HPS) Lamps. HPS lamps were introduced in 1965. They have rapidly gained acceptance for the exterior lighting of parking areas, roadways, and building exteriors because of their high efficiency. Operating on the same principles as mercury vapor and metal halide lamps, HPS lamps contain xenon as a starting gas to initiate the arc that vaporizes a sodium-mercury amalgam; however, they differ in construction and physical appearance. HPS lamps have a high lumen efficiency (80 LPW to 140 LPW), relatively good color rendition, long lamp life (24,000 hours), and an excellent lumen depreciation factor that averages about 90 percent throughout its rated life. HPS lamps are used where efficiency is most important.

6.5.3.3.4 Low-Pressure Sodium (LPS) Lamps. Although LPS lamps are similar to fluorescent systems (because they are low-pressure systems), they are commonly included in the HID family. LPS lamps are the most efficacious light sources, but they produce the poorest quality light of all the lamp types. Being a monochromatic light source, an LPS lamp makes all colors appear black, white, or shades of gray. LPS lamps are available in wattages ranging from 18 to 180. LPS lamp use generally has been limited to outdoor applications such as security or street lighting. However, because the color rendition is so poor, many municipalities do not allow them for roadway lighting. Because LPS lamps are "extended" (like fluorescent lamps), they are less effective in directing and controlling a light beam, compared with "point sources," like high-pressure sodium and metal halide. Therefore, lower mounting heights provide better results with LPS lamps.

6.5.4 Warm-Up and Restrike Times. Table 6.5.4 provides information on the time required for lighting sources to achieve full illumination. Initial warm-up is the time in minutes from initial starting to full light output at room temperature. Restrike time is the cooling time required before the lamp will restart. During the initial warm-up and restrike periods, a lamp will not operate at full output, which can be an important consideration in some security applications. The ranges given are a function of lamp wattage, with higher wattages requiring longer warm-up and restrike times.

Table 6.5.4 Time Required to Reach Full Illumination for Various Lighting Sources

Lighting Source	Initial Warm-Up (minutes)	Restrike Time (minutes)
Incandescent	0	0
Tungsten halogen	0	0
Fluorescent	0	0
Mercury (clear)	5–7	3–6
Mercury (phosphor)	5–7	5–7
Metal halide	3–5	10–15
High-pressure sodium	3–4	1
Low-pressure sodium	7–9	1–3

6.5.5 Types of Luminaires. A luminaire is a complete lighting unit consisting of a lamp or lamps together with the parts designed to distribute the light, to position and protect the lamps, and to connect the lamps to the power supply. A wide range of luminaires is available for protective lighting. Of these, four general types are most often used in a protective lighting system: floodlights, street lights, Fresnel lens units, and search lights. The type best suited to a particular application is based on the patterns of light distribution desired and the convenience of servicing, since the cost of maintenance affects the overall suitability of a protective lighting system.

6.5.5.1 Floodlight Luminaires.

6.5.5.1.1 Application. Floodlights are designed to form the light into a beam so that it can be projected to distant points or to illuminate definite areas. Floodlights are used for the illumination of boundaries, fences, and buildings and for local emphasis of vital areas or buildings.

6.5.5.1.2 Reflectorized Lamps. Floodlights with reflectorized lamps, which are lamps with a reflecting coating applied directly to part of the bulb surface, are applicable for lighting small areas and irregular spaces, such as around building setbacks, stockpiles of materials, and tanks, and for boundary lighting where the light must be confined to the immediate fence area.

6.5.5.1.3 Floodlight Specifications. Floodlights are specified in wattage and beam spread. Beam spreads, expressed in degrees, define the angle included within a beam. The greater the distance from the floodlight to the area to be protected, the narrower is the beam spread desired. Since the illumination at the edge of a floodlight beam is significantly less than that at the center (about one-tenth), the beams of individual floodlights must be overlapped to obtain the desired illumination.

6.5.5.1.4 Classification. Outdoor floodlights are classified according to beam spread by the National Electrical Manufacturers' Association (NEMA) as Types 1 through 7; they are also referred to by the terms *narrow*, *medium*, and *wide*. They are available for use with different types and sizes of lamps, both

incandescent and HID, and can be either open or closed, the latter being equipped with a glass cover to exclude rain, dust, and other airborne contaminants.

6.5.5.2 Street Light Luminaires.

6.5.5.2.1 Classification. Street lights are rated by the size of the lamp the fixture accommodates and the characteristics of the light distribution. They are classified as Types I thru V. The distribution of the light can be symmetrical or asymmetrical.

6.5.5.2.2 Symmetrical Distribution. Street light luminaires with symmetrical distributions find application in lighting large areas where the luminaires can be located centrally with respect to the area to be lighted. They can also be used at entrances and exits and for special boundary conditions.

6.5.5.2.3 Asymmetrical Distribution. Street light luminaires with asymmetrical distribution direct light by reflection, refraction, or both into the area to be lighted. They find application where the location and position of the lighting unit are restricted with respect to the area to be lighted. An example of asymmetrical distribution is the illumination of boundaries where the fixture is located inside the property and the light is delivered largely outside the fence. Another example is a roadway where the fixture must be placed outside the limits of the roadway but the effective light is that reaching the road surface.

6.5.5.3 Fresnel Lens Luminaires. Fresnel lens units used in protective lighting systems deliver a fan-shaped beam of light approximately 180 degrees in the horizontal and 15 degrees to 30 degrees in the vertical. They are intended to protect a property by directing the light outward to illuminate the approaches and inflict glare on the would-be intruder, while affording a guard comparative concealment in darkness. The use of Fresnel lens units is usually limited to facilities where the resulting glare will not be objectionable, such as commercial and industrial facilities that do not border on residential areas.

6.5.5.4 Search Light Luminaires. Search lights usually are incandescent, since incandescent lamps reach full brilliance immediately and permit very concentrated beam distributions. Search lights are generally used to supplement the fixed lighting at a location. The mountings for search lights are usually of the pedestal type, since these place the controls in the hands of guards. Portable, battery-powered search lights are also available. Search lights are generally rated by the diameter of the reflector, which can range from 12 in. (30.5 cm) to 24 in. (61 cm), and the wattage of the lamp, which can range from 250 watts to 3000 watts.

6.6 Walls, Roofs, and Accessible Openings.

6.6.1 Walls. In most commercial burglaries, the point of attack is a door, window, or other accessible opening. If those openings are secure, a burglar might try to penetrate exterior walls, especially if high-value items are inside the structure. Wood frame and masonry or concrete are the basic materials used in most commercial wall construction.

6.6.1.1 Wood frame walls are relatively inexpensive, easy to build, and durable and provide good insulation against noise, weather, and heat loss. However, they do not provide much penetration resistance. A determined intruder can usually break through an ordinary frame structure in just a few minutes, making a frame wall insufficient protection for high-value property, unless coupled with an intrusion detection system or other physical safeguards.

6.6.1.2 Masonry and concrete walls are more expensive than frame walls and are used in commercial structures because of their durability, resistance to fire, and insulation against weather, noise, and heat loss. They usually consist of either poured concrete or concrete block and can have a layer of brick face.

6.6.1.3 Poured concrete walls are relatively difficult to penetrate. Concrete block walls that have not been filled with concrete or reinforced with steel can be as vulnerable to attack as wood frame walls. Ultimately, any masonry wall can be penetrated by a determined attack.

6.6.2 Roofs.

6.6.2.1 Sloping roofs (of whatever style) are unattractive to intruders because anyone on a sloping roof is usually visible from ground level. The slope itself poses a risk of falling, and the necessary tools must be held in place while not being used. However, sloping roofs should be analyzed with respect to ventilating ducts, skylights, and other possible access points.

6.6.2.2 The flat roofs most often found on commercial buildings can be very attractive to intruders. Because the walls on many commercial buildings extend a few feet above the roof line, they can provide excellent concealment for any intruder attempting to penetrate the roof. Large, sophisticated tools can be used for an extended period of time, and a considerable amount of noise can be made if the building is unoccupied. Given such favorable conditions, flat roofs, except ones made of reinforced concrete, can be attractive attack points for burglars.

6.6.2.3 Penetration of the roof itself is seldom required, because the typical flat commercial roof offers numerous skylights, ventilation openings, elevator access doors, trap doors, and other maintenance access ways that are more convenient points of entry. Such access points can and should be strengthened to the point that they are as resistant to penetration as the roof itself. Intrusion detection systems should also be considered in these areas.

6.6.3 Accessible Openings. As noted in 6.1, doors and windows are the preferred entry points for burglars. As such, all doors and windows and other openings that are accessible should be protected.

6.6.3.1 Most doors and windows are considered accessible. Roofs are often overlooked, but openings such as vents, skylights, and maintenance access ways should also be considered accessible openings.

6.6.3.2 A burglar can attempt to go through the door or window, such as by breaking out a panel, or to pry open the door or window. These types of attacks can be prevented through the use of security devices such as locks and ironwork.

6.6.3.3 Some consideration should be given to the construction of the walls that support the doors or windows since they impact the security provided by doors and windows. Concrete and masonry walls provide rigid support for door frames when the frames are properly mounted. Wood frame construction, on the other hand, is usually flexible enough to allow a burglar to spread the door frame even when it is solidly fastened to the structure.

6.6.3.4 Windows are a particularly difficult problem in building security. Their primary functions are to provide light, to allow ventilation (if they can be opened), and to serve as a barrier to the elements. They are not ordinarily intended to serve as a security barrier, and improving their security using

ironwork and burglary-resistant glazing materials is normally difficult without affecting their primary function or creating a life safety hazard.

6.7 Ironwork. Ironwork, such as crossbars, gates, and screens, are used on doors and windows to protect against unauthorized intrusion.

6.7.1 Crossbars.

6.7.1.1 Crossbars, or braces of steel, are horizontal bars used on secondary exterior doors and shutters (of wood and/or metal) in mercantile establishments. They provide additional rigidity to the door or shutter to limit their potential for being smashed or rammed open. Crossbars afford good security if they fit tightly in their brackets and have padlocks or other means to prevent their easy removal.

6.7.1.2 A steel crossbar should have cross sectional dimensions of at least 1¾ in. × ½ in. (4.4 cm × 1.3 cm). The bracket should be of comparable strength as the bar and should be securely bolted to the door or wall. To prevent the bar from being sawed through or lifted out of the bracket from the outside, the space between the door and frame or between double doors should be covered with an overlapping metal plate.

6.7.2 Flat or Round Iron Bars.

6.7.2.1 Iron bars (the term *iron* is used here in the vernacular) are used to protect windows, transoms, skylights, and vents. Round bars should be at least ¾ in. (1.9 cm) diameter, while flat bars are usually 1½ in. × ⅜ in. (3.8 cm × 1 cm). Round bars can be mortised in masonry, fashioned in a frame, or designed with horizontal crossbars for added strength and support. Vertical bars should be spaced not more than 5 in. (12.7 cm) apart and horizontal bars 24 in. (61 cm) or less.

6.7.2.2 Bars should be secured to the window frame with heavy lag bolts that have been welded over or with bolts and nuts that have been peened, to prevent their easy removal. For a hinged installation, provision must be made to prevent removal of the hinge pins or attack on the lock.

6.7.2.3 It is always preferred that ironwork be installed on the inside of the premises, behind the door or window. Exterior installations are susceptible to being pried, pulled off, or otherwise attacked. With inside installations, however, the intruder would have to break the glass or cut through the door, thereby making noise, before getting to the substantial security, the ironwork.

6.7.2.4 Iron gates are used as security devices on entrances to stores and mercantile occupancies. Round bars should be at least 1½ in. (3.8 cm) diameter, while flat bars should be at least 1½ in. × ⅜ in. (3.8 cm × 1 cm); vertical bars should be spaced not more than 5 in. (12.7 cm) apart. The lock used to secure the gate should be of the deadbolt type, with a minimum bolt throw of 1 in. (2.5 cm) and protected so that it cannot be reached from outside the gate. The gate frame should be securely anchored within the opening to prevent the frame from being pried off, and the gate should be provided with an overlapping metal trim along its edge to cover the gap between the gate and frame. If the hinge pin is removable, then provision should be made to secure it.

6.7.3 No. 18 Gauge Sheet Steel Panel.

6.7.3.1 Exterior wood doors, especially hollow-core and wood panel doors, are vulnerable to entry attempts to cut or chop a hole through the door to gain access to the lock or the premises. These doors can be reinforced by the installation of a No. 18 gauge or thicker sheet steel panel.

6.7.3.2 The panel should be attached to the inside surface of the door, covering its length and width, with screws on maximum 6 in. (15.2 cm) centers. Since the panel will add extra weight to the door, it is likely that the hinges will have to be replaced, or a third hinge added, to accept the additional weight. In addition, it makes little sense to upgrade the security of the door without reinforcing the door frame. Sheet steel panels can also be used to line wood shutters on accessible windows.

6.7.4 No. 8 Gauge Wire Mesh Screening.

6.7.4.1 To protect glass panel doors, where it can be possible to break the glass and reach in to unlock the door, or as an alternative to iron bars for protecting windows, transoms, and skylights, No. 8 gauge wire mesh screening in a frame can be used. Screens should be bolted in place when installed on the outside or attached with thumbscrews or a padlock on inside installations where their removal during business hours is desirable. It is always preferred that screens be installed on the inside of the opening. Large screens [more than 15 ft^2 (1.39 m^2)] should have stiffener bars welded along their centers.

6.7.4.2 Basket-type screens are available that permit the opening of windows for ventilation purposes. Screens can also be hinged and padlocked, with the padlock installed on the inside of the screen to limit its vulnerability to attack.

6.7.5 Sliding or Roll-Up Grilles. Sliding or roll-up grilles of steel, aluminum, or polycarbonate plastic are found in shopping malls, arcades, and building lobbies, where they can be used to protect just one store or a series of stores. They are preferred to folding gates, both in appearance (since they are designed to retract out of sight) and in ease of use (since they can be motor driven). Sliding grilles should be provided with a locking device at the top and bottom, while roll-up grilles should be locked in each side guide. In general, they can be manually, chain, or motor operated.

6.8 Glazing Materials. Glazing materials are products that combine the capability of transmitting light, thus providing for surveillance, with the physical ability to absorb high-energy impact while still providing structural integrity. Glazing materials can be burglary resistant or bullet resisting.

6.8.1 Burglary-Resistant Glazing Materials. UL 972 provides performance testing requirements for burglary-resisting glazing materials. These materials are intended for use indoors and outdoors, principally as a substitute for plate (or float) glass show windows and showcase panels. They are designed to resist the hit-and-run (smash-and-grab) type of burglary.

6.8.1.1 UL-Listed Burglary-Resisting Glazing Materials. The three types of materials presently listed by UL for use as burglary-resisting glazing materials are laminated glass, acrylic, and polycarbonate. Glazing materials that meet the UL requirements are listed under the category "Burglary-Resisting Glazing Material (CVYU)" in the UL Security Equipment Directory.

6.8.1.1.1 Laminated Glass. This material consists of two sections of ⅛ in. thick (3.2 mm) glass bonded to an interlayer of 0.060 in. (1.5 mm) or thicker polyvinyl butyryl (PVB). The material is assembled under heat and pressure, causing the glass to bond to the PVB layer. The total thickness of the

material is approximately 9⁄32 in. (7.1 mm) and is designed to fit the nominal ¼ in. (6.4 mm) frame of a show window.

6.8.1.1.2 Acrylic. This material is a plastic sheet of monolithic construction. Acrylic sheets are made by casting or extruding polymerized acrylic ester monomers. It is available in a ⅞ in. (22.2 mm) thickness.

6.8.1.1.3 Polycarbonate. This material is also a plastic sheet of monolithic construction made by the extrusion or injection molding of polycarbonate resin. It is of ⅛ in. (3.2 mm) thickness, making it suitable for use in standard size window frames. Polycarbonate has 300 times the impact resistance of plate glass and 20 to 30 times the impact strength of acrylic.

6.8.1.2 Application of UL-Listed Burglary-Resisting Glazing Materials.

6.8.1.2.1 Burglary-resisting glazing materials find application in storefronts, as replacements for plate glass show windows, and in display cases. Of the three materials that meet the UL requirements for listing as a burglary-resisting glazing material, the polycarbonates exhibit the highest impact resistance while laminated glass has the least. An impact of sufficient magnitude to cause laminated glass to shatter (the pieces of glass tending to adhere to the PVB interlayer) would probably be resisted by the acrylics, while polycarbonate would be able to withstand an impact of much greater magnitude.

6.8.1.2.2 Laminated glass and acrylic are equal optically (both exhibit high clarity) and have good weathering characteristics; polycarbonate is less clear and becomes more opaque as it ages. The plastics weigh 50 percent to 60 percent less than glass but provide significantly less resistance to scratching.

6.8.1.2.3 Acrylic costs less than laminated glass (although more than plate glass), but it cannot be used in standard window frames because of its thickness. Polycarbonate costs more than laminated glass; however, when replacement costs are factored in, the difference in costs between the two materials can balance out.

6.8.1.2.4 A drawback to the use of laminated glass is that it usually can be cut only at the factory and so must be ordered cut to size. This somewhat limits its application as a replacement glazing material. The plastics, however, can be cut at the job site with conventional power sawing equipment and can also be drilled, routed, filed, or cemented. This ease of fabrication allows for greater flexibility in their installation.

6.8.1.2.5 In addition to serving as a replacement glazing material for show windows, a plastic panel can also be installed directly behind existing glass to form a second line of defense. For show windows, the polycarbonate sheet is suspended by a hinge at the top, and the bottom is secured to angle irons. This hinged design facilitates cleaning of the glazing surfaces.

6.8.1.2.6 On doors with glass lites or doors adjacent to glazed panels, there is the concern of an intruder breaking the glass and reaching in to unlock the door. To protect against this type of attack, a double cylinder lock (e.g., a lock that requires a key to lock and unlock the door from either side) can be used; however, this application can be in conflict with life safety requirements. An alternative is to use a conventional single-cylinder deadbolt and to either replace the glass with burglary-resisting glazing material or install a polycarbonate sheet behind the glass lite. When used to provide backup protection to a glass lite, the polycarbonate sheet is attached to the door with wood screws and countersunk washers. To allow for the expansion and contraction of the polycarbonate, the holes drilled in the polycarbonate sheet must be of a slightly larger diameter than that of the wood screw. This technique can be applied basically to any type of window.

6.8.1.2.7 The plastics are not as hard or abrasive resistant as glass. In areas subject to heavy pedestrian traffic, such as the show windows of a jewelry store, laminated glass is preferred to plastics because of its better scratch resistance. Alternatively, plastic glazing can be used behind the glass to provide secondary protection. Plastics are available with special coatings that significantly increase their scratch resistance, but this improvement still does not equal the scratch resistance of glass.

6.8.1.2.8 A potential problem with plastics is associated with their mounting in standard window sashes or window frames. The plastics are subject to greater dimensional change than glass due to thermal expansion and contraction. This fact, combined with their high flexural strength, could allow a determined intruder being able to push the plastic panel out of the window frame before the material itself breaks. Thus, allowances should be made in the installation of plastic glazing materials to account for this concern. Ideally, a frame with deeper rabbetted dimensions is preferred.

6.8.1.2.9 Both acrylic and polycarbonate are combustible, requiring that the same fire precautions be observed in their handling and storage as for other combustible materials. One particular concern arises where acrylics are used as a replacement for glass in doors and windows subject to vandalism. Lighter fluid or other flammable liquids can be used to ignite the plastic. Whereas polycarbonate will self-extinguish once the source of ignition is removed, acrylic will continue to burn and will emit toxic fumes. The burning acrylic could spread the fire to other combustibles in the building.

6.8.1.2.10 Other materials that find use in resisting forced entry but that are not UL listed are called *composites*. Also referred to as *glass-clad polycarbonates*, composites usually consist of a polycarbonate sheet bonded to a glass laminate or sandwiched between two laminations of glass and PVB. They are available in ⅜ in. (9.5 mm) and greater thicknesses. The composites are scratch resistant and fire resistant, have good weathering characteristics, and exhibit high impact resistance. However, they cannot be fabricated on the job site, and have to be ordered pre-cut, which adds to their cost.

6.8.2 Bullet-Resisting Glazing Materials. UL 752 provides test criteria for glazing materials used to form bullet-resisting barriers that are designed to protect against robbery and holdups. The standard also includes test criteria for the devices and fixtures used in bullet-resisting enclosures. ASTM F 1233 provides test criteria to evaluate the level of resistance of security glazing materials and systems to forced entry due to ballistic impact.

6.8.2.1 UL-Listed Bullet-Resisting Glazing Materials.

6.8.2.1.1 Types of Glazing. Bullet-resisting glazing material can be a laminated assembly of glass and plastic, a combination of glass and plastic or of plastics bonded together, or monolithic plastic. Four types of bullet-resisting glazing materials are presently listed by UL: laminated glass (also referred to as BR glass), acrylic, polycarbonate, and composites of glass and plastic. Glazing materials that meet the UL requirements are listed under the category "Bullet-Resisting Material" (COGT) and bear the UL Listing Mark.

6.8.2.1.1.1 Laminated Glass. This material consists of various layers of glass bonded together with interlayers of PVB plastic

and sealed under heat and pressure. BR glass is available in thicknesses from 1 3/16 in. (30.2 mm) upward to provide protection at all ballistic levels.

6.8.2.1.1.2 Acrylics. These materials are usually monolithic in structure and available in thicknesses ranging from 1¼ in. to 1¾ in. (31.8 mm to 44.5 mm). They provide protection only at the handgun levels and not in the high-power rifle category.

6.8.2.1.1.3 Polycarbonates. Usually of laminated construction, polycarbonates consist of multiple polycarbonate sheets bonded to an interlayer of PVB. They are available in thicknesses ranging from ¾ in. to 1¾ in. (19.1 mm to 44.5 mm). They provide protection only at the handgun levels.

6.8.2.1.1.4 Composites. These usually consist of chemically strengthened glass and polycarbonate sheets that are bonded together with a vinyl-based interlayer to produce a relatively thin, lightweight material. They are sometimes referred to as glass-clad polycarbonates and are available in thicknesses ranging from 0.9 in. (22.9 mm) to more than 2 in. (50.8 mm), providing protection in all the ballistic categories. Other types of composites use combinations of laminated glass, polycarbonate, and/or acrylic separated by an air gap.

6.8.2.1.2 Ratings. UL has established eight ratings for bullet-resisting glazing materials — Levels 1 through 8 — based on the ability of the material to resist penetration from medium-, high-, and super-power small arms, high-power hunting and sporting rifles, submachine guns, assault rifles, and shotguns.

6.8.2.2 Application of UL-Listed Materials. Barriers of bullet-resisting glazing material, also referred to as bandit barriers, are intended to protect personnel from armed robbery attack and to provide them with sufficient time to take appropriate countermeasures. Although these barriers are normally associated with banks, they can be used in any business at risk of armed robbery or attack.

6.8.2.2.1 Laminated Glass. Of the four types of listed bullet-resisting glazing materials, laminated glass is the heaviest. However, it has better scratch resistance and weatherability than the other three, is noncombustible, and is resistant to flame and chemical attack. It does tend to spall more than the other materials in multiple-shot situations and is vulnerable to smashing under sustained, heavy-impact attack.

6.8.2.2.2 Plastics. The main advantages to the use of plastics are that they are lighter in weight, tend to spall less, and afford greater resistance to heavy impact than glass. Also, they can usually be fabricated at the job site. However, the plastics are vulnerable to scratching and, in general, are not as weather resistant as glass — two factors that can affect their cost effectiveness. Plastics are susceptible to flame and chemical attack, and, being combustible, they increase the fire load in a building.

6.8.2.2.3 Composites. The composites provide a higher degree of attack resistance, greater bullet-resisting capabilities, and less spalling than conventional laminated glass. Their primary disadvantage is their cost; they are more expensive than either laminated glass or acrylic.

6.8.2.3 ASTM Testing. ASTM F 1233 provides a basis for the comparative evaluation of ballistic, forced entry, and containment resistance of security glazing materials and systems. It is not intended to establish or confirm the ability of the glazing material to absolutely prevent forcible entries or forced exits. Such materials may be suitable for use in high-risk facilities, such as police stations, guard posts, courtrooms, and detention facilities.

6.8.2.3.1 The test method is used to determine the resistance of the glazing material or system to forced entry by ballistic attack only or by ballistic attack followed by, and in combination with, physical attack.

6.8.2.3.2 ASTM ballistic tests are performed on 12 in. × 12 in. (305 mm × 305 mm) or 29.75 in. × 29.75 in. (760 mm × 760 mm) test samples at a distance of 25 ft (7.5 m) from the weapon. Spall is detected by perforation of an aluminum foil sheet mounted 6 in. (152 mm) behind the sample. The specifications for the test weapons are provided in Table 3 of ASTM F 1233. Three rounds are fired at the specimen at 120 degree intervals around an 8 in. (20.3 cm) diameter circle and at 0 degree angle of obliquity.

6.8.2.3.3 Five primary ballistic levels – submachine gun, handgun (.44 magnum), handgun (.38 super), rifle, and rifle (AP) – are established based on the ability of the glazing material to withstand the ballistic attack. A sixth level, shotgun, is used to further evaluate the ability of designed-through openings to resist fragmentary threats.

6.8.2.3.4 Glazing materials, depending on their applications, may be required to provide protection against a combination of ballistic and physical attack. In such cases, depending on the level of resistance to forced entry that is desired (e.g., ballistic level and physical attack level), the ASTM ballistic test should be performed followed by the physical attack test.

6.8.2.4 Bullet-Resisting Enclosures. Bullet-resisting enclosures, also referred to as bandit barriers, find application in businesses that are subject to armed robbery, such as banks, check-cashing facilities, liquor stores, ticket offices, and self-service gas stations. They also find application in municipal buildings, such as post offices and police stations, where workplace violence may be a threat to employees. Bullet-resisting enclosures are intended to enable those being protected to have sufficient time to fully assess a threat and respond with the appropriate countermeasures. While affording protection to personnel, they also protect the assets of the company and discourage attempts at armed robbery.

6.8.2.4.1 UL Listing. The devices and fixtures that are listed by UL as being bullet resisting and that are used in the construction of bullet-resisting enclosures are provided in the UL *Burglary Protection Equipment Directory* under the category "Bullet-Resisting Materials (CNEX)." These listings include bullet-resisting metals and plastics, bullet-resisting glazing materials, and bullet-resisting devices, such as deal trays, teller windows, gun ports, and tellers' fixtures.

6.8.2.4.2 Bullet-Resisting Devices. Bullet-resisting devices include deal trays, vision windows, teller windows, door and frame assemblies, package passers, and gun ports and are designed to be assembled in bullet-resisting enclosures. A bullet-resisting enclosure should be installed to a height of 7 ft (2.1 m) above the floor and with supplementary mechanical defenses above this height to protect against unauthorized access to the working quarters. In addition, doors that give access to the working quarters should be bullet resisting and have automatic locks and closers.

6.8.2.4.2.1 Deal Trays. Deal trays are installed in bullet-resisting barriers to provide a means of transferring money and other valuables between the employees' working quarters and the public space. A deal tray is designed and constructed in such a way that it will not permit a direct line of fire toward

the teller's position, or afford sufficient space for an individual to insert a small caliber handgun in such a manner as to command direct aim on the teller. UL also requires that a deal tray be designed so that a shotgun blast or ricocheted shot coming into the deal tray would be directed away from the teller.

6.8.2.4.2.2 Vision Windows. Vision windows, constructed of bullet-resisting glass or plastic, are installed in bullet-resisting enclosures to provide a secure means for viewing the public space from the protected working quarters. They are available in either fixed or movable forms. Voice communication is accomplished through the use of electronic equipment or by natural means. In the latter case, either a staggered panel arrangement with short return baffles or a baffle system within the window frame is used.

6.8.2.4.2.3 Teller Windows. Teller windows are installed at the point of public interface or transaction and consist of a vision window and a deal tray, through which currency and documents can be passed, on a counter. A teller window usually has a voice communication system.

6.8.2.4.2.4 Door and Door Frame Assemblies. Bullet-resisting doors are constructed of bullet-resisting metals and other materials and are available either as solid doors or with vision panels. Since a bullet-resisting door is considerably heavier than a conventional door, it is important that the door frame be structurally sound and properly reinforced to accept the heavier load. For this reason, the door frame also should be UL listed as bullet resisting. The lockset should be of the mortise type, with a ⅝ in. (16.0 mm) throw on the latchbolt, and it should be armored in such a way as to prevent the door from unlatching if subject to a series of shots placed in the areas of the lockset. The door should be equipped with a heavy-duty closer to ensure that the door closes fully with the latchbolt securely latched. Emergency exit and panic hardware are available for use on these doors. The authority having jurisdiction (AHJ) should be consulted for compliance with fire and building codes.

6.8.2.4.2.5 Package Passers. Package passers, also referred to as transfer devices, provide a secure means of transferring relatively large items, such as currency sacks or data processing media, that are too large for a deal tray. These devices are designed with an interlock between the passageway doors such that only one door can be open at a time, thus always keeping a bullet-resisting barrier between the public space and the working quarters.

6.8.2.4.2.6 Gun Ports. Gun ports are intended to provide personnel with a means to defend themselves against the threat of gunfire, flame, chemical, or mechanical attack. Gun ports are designed for operation from behind the bullet-resisting barrier only and are equipped with a door or shutter that closes automatically.

6.8.2.4.2.7 Tellers' Fixtures. Bullet-resisting tellers' fixtures are designed for installation in the wall of a bank building to provide a walk-up or drive-through banking facility. Although intended to protect against robbery from the exterior of the building, if they are accessible directly from the working quarters within the bank, the working quarters should be separated from the public space by a bullet-resisting enclosure. A bullet-resisting tellers' fixture is a complete assembly of bullet-resisting glass, metal, and/or plastic; safety deal trays and usually electrically operated package drawers; a voice communication system; and light fixtures.

6.9 Passive Barriers. In the typical smash-and-grab attack, burglars smash the glass door or show window of a retail store with a sledge hammer or similar tool, grab as much merchandise as can be carried, often while the alarm siren is blaring, and are gone before the police arrive. This type of attack is also called a "3-minute burglary" because the burglars can usually enter the premises and be gone in less than 3 minutes. Protection against the smash-and-grab attack involves installing roll-down grilles or ferry gates across the front of the store or replacing the glass with burglary-resisting glazing material. A modern variation on the 3-minute burglary is the "crash-and-grab" attack. In this scenario, the burglars back a pickup truck or other vehicle through the show window of the store, grab merchandise, and, again, are gone before the police arrive. While there are no statistics available on the frequency of crash-and-grab attacks, sporting goods stores with their high-value golf clubs have been frequent targets. In addition, there have been reports of as many as 100 burglaries of convenience stores and drug stores where ATM machines were located. In such attacks, the burglars made off with the ATM machine by loading it onto the truck. The traditional security measures — grilles and gates — will not prevent the crash-and-grab attack. If the store has a grille or gate, the burglars have only to tie it to the truck, pull it off its mountings, and then back the truck through the front of the store. An alarm system only limits the time the burglars feel they can safely stay on the premises before the police arrive. Burglary-resisting glazing material will not withstand the forces generated by a moving vehicle. The security measure that is most effective against the crash-and-grab attack is that used to protect against terrorist truck bomb attacks: passive barriers.

6.9.1 Concrete Planters. Concrete planters and bollards (discussed in 6.9.2) are being used to protect the White House and other federal government buildings in Washington, D.C.

6.9.1.1 In testing performed by the U.S. Army Corps of Engineers, a concrete planter, designed as shown in Figure 6.9.1.1, was capable of stopping a 15,000 lb (6804 kg) vehicle traveling at 50 mph (22.4 m/s). This planter should also stop a 4500 lb (2041.2 kg) vehicle traveling at 30 mph (13.4 m/s), which is approximately the weight of a pickup truck and the likely speed it could attain in a short distance. (Specific information on the design of a planter to stop such a vehicle was not provided in the U.S. Army Field Manual 19–30).

6.9.1.2 If local building or street codes permit their use, and the sidewalk in front of the store is wide enough, a decorative concrete planter placed between the pedestrian walkway and the curb can be used. If more than one planter is required to provide coverage for the front of the store, they should be spaced a maximum of 4 ft (1.22 m) apart.

6.9.2 Bollards. For narrower sidewalks or as an alternative to planters, bollards can be used. Bollards are 6 ft (1.83 m) to 7 ft (2.13 m) cylinders of steel, usually filled with concrete, and partially buried, leaving a 3 ft to 4 ft (0.91 m to 1.22 m) section above ground.

6.9.2.1 In testing performed by the U.S. Army Corps of Engineers, concrete-filled steel bollards *(see Figure 6.9.2.1)* spaced 4 ft (1.22 m) apart, at a height of 3 ft (0.91 m) above grade, and buried in concrete to a depth of 4 ft (1.22 m), stopped a 4500 lb (2,041 kg) vehicle traveling at 30 mph (13.4 m/s). The concrete portion of the bollard had a diameter of 8 in. (20 cm) and the steel pipe was ½ in. (1.3 cm) thick.

6.9.2.2 When the bollards were reinforced with a 12 in. (0.31 m) "C" channel *(see Figure 6.9.2.2)*, the design was capable of stopping a 15,000 lb (6,804 kg) vehicle traveling at 50 mph (22.4 m/s).

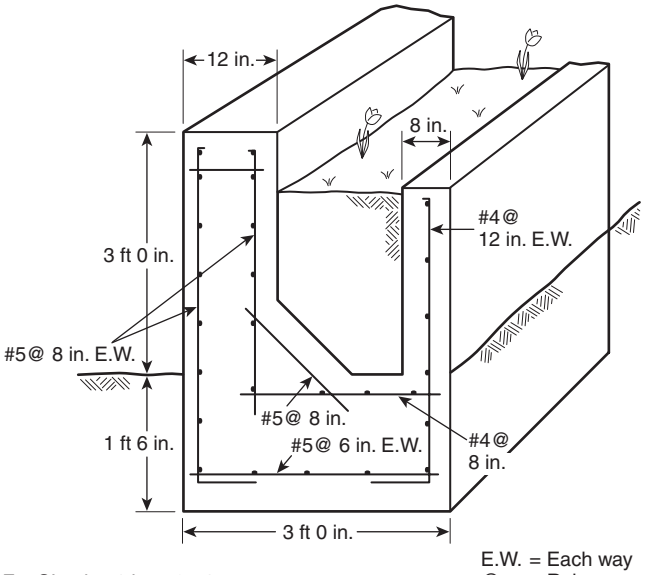

FIGURE 6.9.1.1 Concrete Planter. *(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*

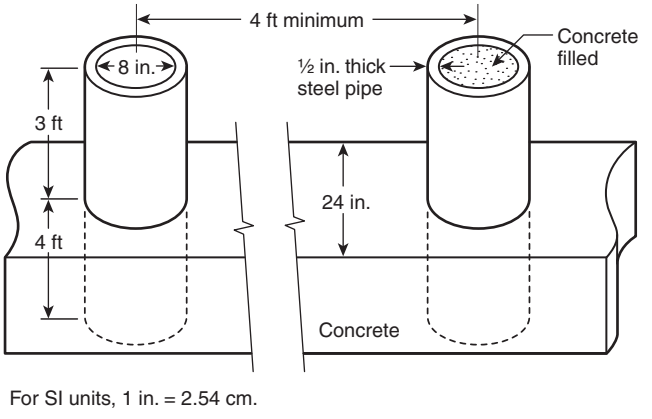

FIGURE 6.9.2.1 Concrete-Filled Bollard. *(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*

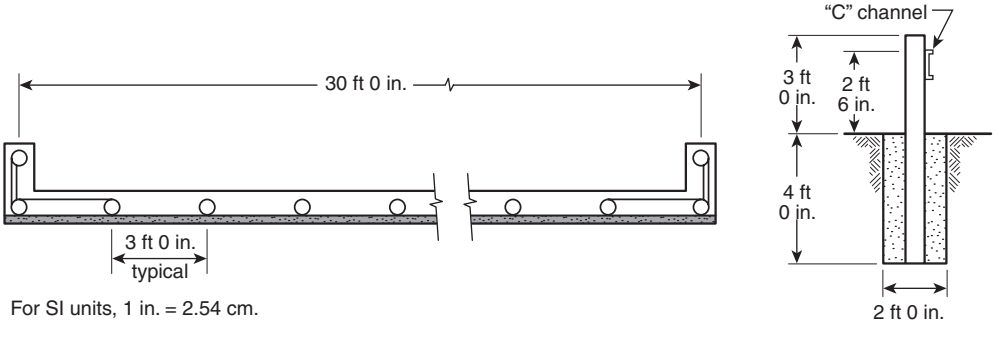

FIGURE 6.9.2.2 Concrete-Filled Steel Bollard with 12 in. "C" Channel. *(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*

6.9.3 Jersey Barriers. Designed for use on highways as a means of preventing head-on collisions between vehicles, Jersey barriers are also effective in protecting against crash-and-grab attacks. Testing performed by the U.S. Army Corps of Engineers found that a Jersey barrier, designed and anchored to a concrete slab *(see Figure 6.9.3)*, was capable of stopping a 4000 lb (1814 kg) vehicle traveling at 50 mph (22.4 m/s). Jersey barriers can be used in place of planters and bollards where aesthetics are not of concern.

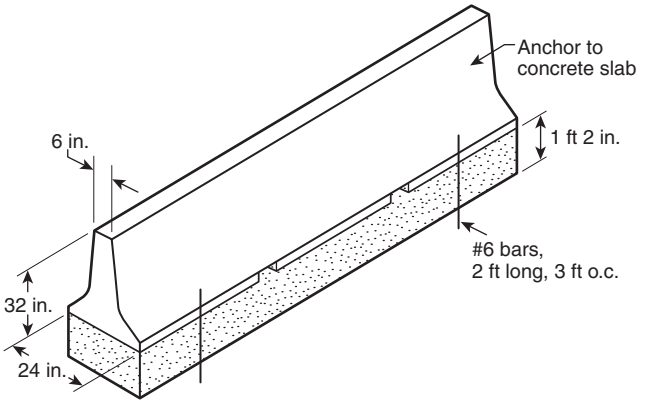

FIGURE 6.9.3 Jersey Barrier. *(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*

6.10 Electronic Perimeter Protection. Electronic perimeter security is applied to a facility to provide a means to detect unauthorized entry onto the property. When the protection is applied at the property line or to outside areas of a facility, it is referred to as *exterior perimeter protection.*

6.10.1 General.

6.10.1.1 Exterior perimeter protection can be applied to fenced areas (such as yards or loading docks where stocks or materials are stored), to a fence itself, or at the boundary lines where the perimeter is not fenced.

6.10.1.2 Exterior perimeter protection is best applied where the area to be protected is bordered by a fence or other physical barrier, such as a brick or concrete wall. The devices used to provide fence protection, referred to as *fence-mounted sensors*, include electronic vibration detectors and shock sensors. The devices used at unfenced boundary lines, referred to as *buried sensors*, include seismic detectors, pressure detectors, and leaky coaxial cables. The devices used to provide protection to fenced areas, referred to as *volumetric detectors*, include microwave sensors and photoelectric beams.

6.10.2 Fence-Mounted Sensors. Fence-mounted sensors, in general, are intended for installation on chain-link fencing and are designed to detect either the presence of intruders as they approach or touch the fence or the mechanical vibrations caused by intruders climbing over, cutting through, or crawling under the fence. Since these devices are mounted directly to the fence, to reduce the potential for false alarms, it is important that the fence be installed according to ASTM F 567. Fence signs should be securely mounted so that they do not rattle, and large bushes and tree limbs that grow along the fence line should be trimmed so that they do not rub against the fence. The primary advantage to the use of fence-mounted sensors is that installation is simplified, since the installer can follow the contour of the fence and the topography of the area. The major disadvantage to their use is that the intruder must come in contact with the fence to be detected.

6.10.2.1 Electronic Vibration Detectors. These devices detect movement of the fence through a set of point transducers that produce an analog signal. An electronic signal processor extracts alarm information from the signal. State-of-the-art equipment provides processors that can analyze the signal to eliminate false alarms caused by animals, environmental disturbances (such as wind, rain, and lightning), or vibrations from nearby activities (such as a passing truck).

6.10.2.2 Shock Sensors. Shock sensors respond to the shock waves created by an impact against the fence. In principle, the shock momentarily displaces a small metal object in the device, interrupting an electrical circuit and generating electrical impulses. A signal processor looks for a pattern of pulses generated over a period of time before signaling an alarm.

6.10.3 Buried Sensors. Buried sensors are usually installed at unfenced boundary lines and provide a narrow, sensitive band, or detection zone, along the ground above the buried sensors to detect intruders crossing the zone. They can work alone or, in high-risk application, be combined with other outdoor perimeter protection devices to provide a secondary means of detection.

6.10.3.1 Seismic Systems. These systems use passive geophone sensors to detect seismic or acoustic disturbances in the ground and measure these disturbances against a preset value. Systems can consist of a single geophone, called *point sensing*, or a series of geophones around the perimeter. Seismic systems are usually not affected by temperature or weather, but they are susceptible to false alarms if installed in areas subject to heavy ground disturbances, such as from vehicular traffic or low-flying aircraft.

6.10.3.2 Pressure Systems. Pressure systems use two liquid-filled hoses buried about 6 in. (152 mm) deep and 5 ft (1.52 m) apart. Each pair of hoses, usually up to 325 ft (99 m) in length, is connected to a pressure-sensing unit or transducer. When an intruder or vehicle passes over the hoses, the liquid hydraulically transmits the ground pressure variations to the transducers, which convert them to electrical impulses.

6.10.3.3 Leaky Coaxial Cables. These cables are ordinary coaxial cables with apertures in them to allow radio frequency energy to leak out. Two cables, one acting as a transmitter and the other as a receiver, are buried in the ground parallel to each other and produce an electromagnetic field. When an intruder enters the detection zone, the electromagnetic field is changed and an alarm is triggered. An advantage to the use of this system is that the electromagnetic field is radiated above and below ground, providing protection against tunnelers.

6.10.4 Volumetric Detectors. Volumetric intrusion detectors are usually applied to fenced areas that are level, such as yards or loading docks where stocks or materials are stored, and generate a narrow, invisible beam (or zone) of electromagnetic energy. The detectors are installed in an overlapping configuration around the perimeter of the facility adjacent to the fence. When an intruder attempts to run, walk, or crawl through this zone, the energy pattern is interrupted, resulting in an alarm condition. Volumetric detectors can also be used with other exterior perimeter protection devices to provide backup protection.

6.10.4.1 Types. Volumetric detectors are either of the microwave or infrared energy type. The energy barrier is formed by a transmitter that sends a signal, a beam of either microwave or infrared energy, to a receiver that is located in the line of sight of the transmitter. The receiver monitors the signal for changes characteristic of an intruder penetrating the beam.

6.10.4.1.1 Outdoor Microwave Systems. These systems are either monostatic, in which case the transmitter and receiver are in the same housing and a mirror is used to reflect back the signal, or bistatic, in which the transmitter and receiver are separate units. Under ideal operating conditions, microwave detectors can usually cover a zone approximately 6 ft to 32 ft (1.8 m to 9.8 m) wide by 5 ft to 13 ft (1.5 m to 4 m) high over ranges up to 650 ft (198 m).

6.10.4.1.2 Infrared Systems. In active infrared systems, the transmitter sends out a beam of pulsed infrared energy to the receiver, and the receiver detects any break in the beam. To create a "fence" of protection, a multiple-beam arrangement, with transmitters and receivers stacked one over the other, can be used. Some units, called transceivers, have the transmitter and receiver in one unit and use a reflector to bounce back the beam. Long-range outdoor infrared units are available. A curtain of protection can be provided using large-diameter optics. Their use is limited by climatic conditions, since they can be affected by heavy fog, rain, dust, or snow.

6.10.4.2 Installation. Both microwave and infrared detectors should be installed with a clear line of sight between the transmitter and receiver and with the detection zone closely paralleling the ground surface. They should not be used in hilly or uneven terrain, since gullies and dips in the terrain would create voids in the detection zone that could enable an intruder to crawl under the beam without being detected. Also, obstructions, such as lampposts, between the transmitter and receiver could block the energy, making detection unreliable. Since these devices are designed to detect movement, all trees, bushes, and tall grass between the transmitter and receiver must be removed, so that movement of vegetation by the wind does not cause false alarms. Multiple-beam configuration is specifically designed to minimize false alarms.

Chapter 7 Physical Security Devices

7.1 General. This chapter includes descriptions and usage guidance for various types of common physical security devices, including builders' hardware, locks, doors, windows, safes, vaults, and strong rooms.

7.2* Locking Hardware. Locks are designed to provide various levels of deterrence or delay entry and are an integral part of an overall security system. Egress and fire resistance provisions relating to doors and hardware in NFPA *101*, *Life Safety Code*; *NFPA 72*, *National Fire Alarm Code*; and NFPA 80, *Standard for Fire Doors and Other Opening Protectives*, should be maintained. Individual products should be listed to the following standards as applicable:

(1) *ANSI/BHMA A156 Series performance standards include security tests and are shown in the applicable sections.
(2) UL 1034 for burglary-resistant electronic locking mechanisms
(3) UL 437 for key locks
(4) UL 768 for combination locks
(5) UL 294 for access control system units
(6) UL 2058 for high security electronic locks
(7) UL 305 for controlled exit panic devices

7.2.1 Types of Locks. Locks can be divided into three general classes:

(1) Those that operate on purely mechanical principles
(2) Those that are electromechanical and combine electrical energy with mechanical operations
(3) Those that are electronic

7.2.2 Keys. Keys and locks are often the first and only level of physical security control for many organizational assets. Consequently, key control or the lack of it can mean the difference between a relatively secure activity and extraordinary loss. Almost all organizations utilize some type of key access in everyday operations. Each day offers an opportunity for key mismanagement or unauthorized duplication, which can lead to mild annoyances, such as the replacement and cost for lost keys, or to more serious losses, such as theft or personal injury. A good key control system maintains a strict accountability for keys and limit both key duplication and distribution. Refer to ANSI/BHMA A156.28. Keys should meet ANSI/BHMA A156.5, Cylinder Section, and ANSI/BHMA A156.30 in the appropriate grade for the application.

7.2.2.1 Types of Keys and Cylinders. Proprietary keyways or patented cylinder and key mechanisms are available with controlled distribution to prevent unauthorized key duplication. When they are combined with any of the various locking hardware described in 7.2.3 through 7.2.20, consideration should be given to the need for a patented high security or patented key control cylinder on keyed functions. Operating or "change" keys are keys that are used to open locks. Duplicate keys are copies of operating keys and are usually stored for use in an emergency or to replace a lost key. Duplicate keys must be kept to a minimum and must be protected to avoid proliferation and loss of accountability. Master keys are designed to open all locks of a particular series. Key systems can have one grandmaster key for the overall system and several sub master keys for each subsystem. Master keys can be used as a convenience, for example, carrying one key instead of numerous keys, but their use increases susceptibility to picking and duplication and must be carefully controlled. Construction keys open removable core lock cylinders installed on the doors during construction of a facility. These cores are replaced at the end of construction with cores subject to the facility's key system. Control keys are used to remove and replace these cores. Control keys are used only in interchangeable core cylinder systems.

7.2.2.2 Key Accountability Procedures. The integrity of a key system is important to safeguarding property and controlling access. Lost or stolen keys and keyblanks can compromise the security of a key system. The security officer should ensure that responsible individuals maintain control over the facility's key system by storing, issuing, and accounting for all keys under the facility's control. Issuance of keys must be kept to a minimum. Keys should be issued only to persons who have an official need. Accurate accountability records must be kept and should contain the information listed in 7.2.2.2.1 and 7.2.2.2.2. PC-based software, key storage cabinets, and computer-controlled key retention and distribution systems are available to facilitate the management of a master key system and help to ensure its long-term integrity.

7.2.2.2.1 Procedures should include the following:

(1) When a key to a designated controlled or restricted area is lost, the locks to the area should be changed.
(2) Access lists for persons authorized to draw master keys should be maintained.
(3) The key storage container/cabinet should be kept locked with a pick- and drill-resistant, patented high security cylinder that is not keyed to the facility master key system.
(4) The container/cabinet should be checked periodically in accordance with the security plan.
(5) All keys should be inventoried at least annually.
(6) Requests for issuance of new, duplicate, or replacement keys should be made in writing and approved or monitored by the security officer.
(7) Keys not issued or no longer needed should be destroyed or stored in a locked container.
(8) Protection of keys should be a priority at all times.
(9) Identifying key tags with user or facility names on rings is not recommended; if keys are lost, it is an open invitation for misuse.
(10) Keys should not be left on desks, in unlocked drawers, or where they can be easily taken and copied.
(11) Employees should be reminded to keep official keys on their person or securely locked in a desk or cabinet and that they are not to lend them to individuals not specifically authorized.
(12) Employees should promptly return official keys checked out on a temporary basis.
(13) Lost keys should be immediately reported to the appropriate official, and locks should be rekeyed immediately and new keys issued when keys are lost or stolen.
(14) Keys should not identify the specific premises or access doors that they open.

7.2.2.2.2 Records should include the following:

(1) Number assigned to each key and lock
(2) Location of each lock (room number)
(3) Person to whom keys have been issued
(4) Date of issuance
(5) Recipient's signature for keys issued

7.2.3 Electronic Cylinders. Electronic cylinders are useful in applications where there is a high user turnover and a need to collect access data and to limit access to particular periods. They are often used in conjunction with card readers, biometrics, and so

on. Electronic cylinders should meet the requirements of ANSI/BHMA A156.30 in the appropriate grade for the application.

7.2.4 Flush Bolts. Flush bolts are used in pairs of door openings requiring only one leaf for normal use or to meet an exiting requirement where the occasional use of a larger opening is required. Flush bolts are small deadbolts that go into the floor and ceiling and typically keep the second door in a pair of doors closed. Flush bolts are frequently used on pairs of doors in conjunction with a lock or exit device on the active leaf. Flush bolts can be either manual or automatic. Automatic (not manual) flush bolts are used on the inactive leaf of a fire-rated door in a pair of doors. Automatic bolts use the closing action of the active leaf to activate the latching. Periodic inspection for warped, weakened, or otherwise misaligned doors should be conducted to ensure activation of top and bottom bolts. This inspection should include a check to ensure that there are no obstructions or foreign objects in frame or floor strikes. In non-fire-rated applications, manual flush bolts secure the second door in a pair. Key-lockable flush bolts are surface applied and can be used to prevent the inactive leaf of a pair from being opened.

7.2.5 Coordinators. A pair of doors often requires a coordinator. These devices mount on the top jamb and hold one door open until the other door closes, which allows the door to latch shut properly. Without a coordinator, doors can be easily and inadvertently left propped open.

7.2.6 Built-In Locks. When a security container or vault door is used to safeguard confidential information, it should be listed and equipped with a lock designed to prevent the user from leaving the container in the "closed but unlocked" condition.

7.2.7 Combination Locks. A manipulation-resistant combination lock provides a high degree of protection. It is used primarily for safeguarding classified or sensitive material. Its technical design prevents the opening lever from coming in contact with the tumblers until the combination has been dialed. These locks are available with mechanical or electronic dials.

7.2.8 Combination Padlocks. Combination padlocks are used primarily on a bar-lock filing cabinet. They are not rated for resistance to physical attack and are not recommended for outdoor use. The procedures for changing combinations, protecting combinations, and recording combinations established in 7.2.2.2 should also be followed for combination padlocks.

7.2.9 Exit Devices.

7.2.9.1 Exit devices are used where occupancy levels require unimpeded single-motion egress. Typical locations are at an opening from an area of assembly and at all latched openings in the direction of the building exit. Exit devices are also required in hazardous locations, often so designated because of gas, chemicals, or flame. Selection of an exit device should include an evaluation of the environment. Nonfire devices can be equipped with "dogging," which holds the latch(es) retracted for extended periods of time. This makes entry easier, reduces wear, and allows designers to use pulls instead of functioning trim to limit vandalism.

7.2.9.2 In areas exposed to abuse, the use of vertical rods should be limited to those locations where they are the only acceptable alternative. Additional steel covers to retard damage can protect rods. Surface vertical rods are susceptible to bending and other damage by carts. For security as well as fire code compliance, vertical rod latches must latch at top and bottom; otherwise, flexing in the door can allow criminal entry. Use of a threshold with vertical rods provides a better mounting surface for bottom strikes. Vertical rod deadbolt exit devices provide further resistance to forced entry.

7.2.9.3 Cross-corridor double egress pairs of door openings typically require vertical rods in pairs. Pairs of doors swinging in the same direction can be either vertical by vertical or vertical by mortise exit device. When fire doors are required to have an overlapping astragal, the use of a vertical by mortise system is required. The latter application also requires a coordinator. The securest approach to pairs of doors swinging in the same direction is to use a mullion and two rim or mortise devices.

7.2.9.4 Electrified exit devices are available in various functions. Electric dogging will hold the latch retracted once the power is applied, allowing push-pull operation. Electric latch retraction allows dogging the device without going to the device. Both of these applications are convenient for fire-rated exits that are not permitted to be mechanically dogged. Electric latch retraction can be combined with an access control system to provide controlled entrance even on pairs of doors that latch at the top and bottom. Electric latch retraction can be combined with an auto-operator to provide access for persons with physical impairments. Electric strikes or electric control trim can be added to exit devices to provide electric release.

7.2.10 Bored/Cylindrical Locks. These lock designs provide convenient installation along with moderate security. Different locking functions are offered to meet access needs, such as non-keyed locking (for bathrooms) and keyed entry. For enhanced resistance to forced entry, doors with these locks can have a separate deadbolt mounted on the door; however, local codes should be consulted, since the second lock requires two actions for egress. Recent product developments have greatly increased the strength and durability of these locks in order to retrofit existing installations with more secure locking solutions. These locks should meet ANSI/BHMA A156.2 and UL 437 in the appropriate grade for the application.

7.2.11 Interconnected Locks. These lock designs combine cylindrical locks and deadbolts and are used in residential occupancy where one motion is required to open the door. They include independently installed cylindrical and deadbolt locks that contain a linkage that allows instant retraction of the deadbolt with movement of the interior lever handle or knob. They combine the security and safety of a latching device with the security of a deadbolt. These locks should meet ANSI/BHMA A156.12 and UL 437 in the appropriate grade for the application.

7.2.12 Mortise Locks. These lock designs are typically used in institutional and high-rise residential applications. They can incorporate both a latch and a deadbolt in the same body. Mortise locks allow a deadbolt with latch in a path of egress because the latch and deadbolt are retracted in a single motion. Mortise locks can be designed with a low-cost failure point, shear pin, spindle, and so forth, making their application attractive for locations that are apt to receive a lot of abuse. Mortise locks should meet ANSI/BHMA A156.13 and UL 437 in the appropriate grade for the application.

7.2.13 Electromechanical Locks. Electromechanical door locks are primarily used to control entry into an area. They can be opened via key (mechanically activated) or electrically by receiving power from a power supply after the valid presentation of a code to a secure encrypted electronic credential (e.g., magnetic/stripe card, proximity card, smart card, digital keypad). They can also be remotely activated by a simple pushbutton or intercom

system. Some of the advantages of using these locks are code-compliant operation, low cost, easy installation, simple operation, and integration with access control systems. Electromechanical locks should meet ANSI/BHMA A156.25 in the appropriate grade for the application. Electrified locking devices should also meet the performance requirements as defined by the applicable ANSI/BHMA A156 series of standards for the product and grade specified by the manufacturer and be listed to UL 1034.

7.2.14 Electromagnetic Locks. These lock designs provide reasonably high levels of force resistance in high-traffic access-controlled areas. The use of electromagnetic locks must not alter the requirement for fire-rated hardware or single-motion egress. Electromagnetic locks should meet ANSI/BHMA A156.23 in the appropriate grade for the application and be listed to UL 1034 for burglary-resistant electric locks.

7.2.15 Delayed Egress Locks. Delayed egress locks were designed for use in retail applications and are valuable in many applications to provide reasonable security by operating on a delay with an alarm in nonemergency situations. They can be installed only where permitted by code and must be released instantly (without delay) by the fire alarm system in the event of emergency. They should meet ANSI/BHMA A156.24 in the appropriate grade for the application and be listed as "Special Locking Arrangements."

7.2.16 Electric Strikes. Electric strikes provide electric release via access control or pushbutton interface for use with bored/cylindrical locks, mortise locks, or exit devices. Models are available for use in both fail-safe and fail-secure situations. Fail-safe models cannot be used in high-rise stairwell applications where codes require re-entry to every fourth floor in the event of a fire, because the doors are fire-rated and the positive latching is lost in this mode. Fail-safe models can be used on non-fire-rated traffic control doors. There are many varieties of electric strikes offering varying levels of protection against forced entry. Electric strikes should be used only where the door frame or the surrounding wall structure is sufficient to prohibit access to strike components or wiring. Electric strikes should meet ANSI/BHMA A156.31 in the appropriate grade for the application and should be listed to UL 1034 for burglary-resistant electric door strikes.

7.2.17 Electrified Trim. Electrified trim can be used in place of electromechanical locks or electric strikes and can provide a high level of resistance to forced entry. Electric trim can be used with bored/cylindrical locks, mortise locks, or exit devices. They typically would provide keyed or electric entry. They can be used in either fail-safe or fail-secure configurations.

7.2.18 Deadbolts and Auxiliary Deadbolts. These products provide an added degree of security due to their longer throw and positive deadlocking. Auxiliary deadbolts are used to protect perimeter doors where not prohibited by codes requiring single-motion egress and are also used on interior doors for forced-entry resistance. The use of auxiliary deadbolts is often prohibited in conjunction with another lock when in a path of egress, because that would require two separate motions and could be confusing to a person during an emergency. Double-cylinder auxiliary deadbolts provide a high level of security, particularly when there are glass panels in the vicinity of the lock, but local codes should be checked for allowable applications. Deadbolt exit locks and deadbolt exit devices provide a higher degree of resistance to forced entry and can be used on doors requiring single-motion egress. The only deadbolts permitted on fire-rated exit doors are those that are self-relocking. Mortise locksets that contain both a latch and a deadbolt can contain single-motion release for use on doors in the path of egress and fire-rated doors. Multipoint deadbolt locks are available in a wide variety of functions and types (surface-mounted, mortise, exit device) and provide the highest level of resistance to forced-entry attempts. Auxiliary deadbolts should meet ANSI/BHMA A156.5, "Deadbolt Section," and UL 437, "Door Locks," in the appropriate grade for the application.

7.2.19 Hinges. Hinges or pivots are required for all swinging doors. Hinges other than continuous hinges should be installed at intervals of every 30 in. (76.2 cm). Nonremovable pins (NRP) should be used on hinges accessible from the outside (outswinging doors). Various types of security studs are available to prevent attack. They should meet ANSI/BHMA A156.1 or ANSI/BHMA A156.26 in the appropriate grade for the application.

7.2.20 Door Closers and Spring Hinges. These devices automatically close the door after opening ensuring latching or locking. They are essential for security due to the fact the door cannot latch if it is not closed. Many door closers include a "hold open" feature, which allows a door to be held in the open position without using a dangerous and inconsistent device such as rock, brick, or wedge to keep the door open. They should meet ANSI/BHMA A156.4 or ANSI/BHMA A156.17, "Spring Hinges," in the appropriate grade for the application.

7.3 Doors.

7.3.1 A door is a vulnerable point of the security of any building. The best door is of little value if there are exposed removable hinge pins, breakable vision panels, or other physical weaknesses that would allow entry. A secure door is made of metal or solid wood. Steel doors produced to ANSI/SDI A250.8 and tested to ANSI/SDI A250.4 and wood doors are tested for security. Door strength and reinforcement should be compatible with the locks used.

7.3.2 Nonexit doors should be installed so the hinges are on the inside to preclude removal of the screws and pins or the use of chisels or cutting devices. Exit door exterior hinges should be protected by welded, flanged, or otherwise secured pins, or hinge dowels should be used to preclude the door's removal.

7.3.3 An operable or glazed transom should be protected by permanently sealing it, locking it from the inside with a sturdy sliding bolt lock or other similar device, or equipping it with bars or grills.

7.3.4 The security measures outlined in this section are designed specifically to increase the resistance of doors to illegal entry. All doors should be secured with a locking mechanism. Consideration should be given to the structure of the opening and the surrounding wall, so that the ability to provide a secure locking device is not compromised.

7.3.5 Exterior doors should be of a solid-core design or steel construction with hinges on the interior of the door (in residential applications and where permitted by codes) and a keyed lock with a strike bolt into a solid frame. Frames should be fastened to the wall studs with long screws to ensure the door's stability. Strike plates should also be firmly fastened to the frame to avoid being ripped out.

7.3.6 Other security measures that should be considered for doors are described in 7.3.6.1 through 7.3.6.9.

7.3.6.1 Assuming exterior doors are of solid construction, they should be equipped with a good deadbolt with at least a 1 in. (25.4 mm) throw lock as described in 7.2.18.

7.3.6.2 Exterior doors must fit tightly in the frame with no more than ⅛ in. (3.2 mm) clearance between the door and frame. If the gap is too large, replace the door or install a sturdy metal strip or latch guard to the door edge to cover the gap. Deadbolts or locks with deadlocking latches help prevent entry by manipulation of the bolts through the gap.

7.3.6.3 The hinged side on outward swinging doors should be protected by using nonremovable hinge pins or hinges that incorporate security studs. Where practical, projecting pins that fit snugly into sockets in the door jamb when the door is closed should be installed in the hinged edge of the door. This will prevent attempts to open the door on the hinged side by removal of the hinge pin or by cutting off the hinge knuckle.

7.3.6.4 If an exterior door has a glass panel within 40 in. (101.6 cm) of the lock, the glass should be replaced with UL-listed burglary-resisting glazing material, such as polycarbonate glazing. Alternatively, a piece of polycarbonate can be attached to the inside of the door behind the glass to provide backup protection, or the glass panel can be protected with a metal security screen. This will prevent a burglar from breaking the glass and reaching in to unlock the door.

7.3.6.5 Glass panels or inserts along with side panels should be addressed when determining the appropriate locking mechanism. Glass panels can easily be broken by intruders. Consider covering the glass with a break-resistant panel, burglary-resistant glazing, or decorative grill.

7.3.6.6 The rollers on sliding glass patio doors should be installed and adjusted so that a burglar cannot lift the doors out of their tracks and remove them. The rollers can be adjusted so that the door cannot be pushed up enough to lift it off the track. Alternatively, a projecting screw placed in the track above the door or a nail inserted through the inside frame and partway through the metal door frame will prevent the door from being lifted out of the track. The same techniques can be applied to sliding windows. Secure stationary doors with locks and long screws to prevent removal.

7.3.6.7 Since the lock catch on sliding glass patio doors can usually be easily pried out of the soft aluminum door frame, a wooden dowel or a patio door bar should be placed in the track of a sliding patio glass door. This will positively block the travel of the sliding portion of the door even if the lock is broken.

7.3.6.8 Secure exterior doors to basements (particularly "doggie doors") on the interior with a slide bolt or on the exterior with a heavy-duty padlock that has a hardened steel hasp.

7.3.6.9 For doors without glazed panels, a wide-angle door viewer installed into the door allows occupant to view the exterior before opening the door. Door viewers meeting ANSI/BHMAA156.16 are available in three viewing angles to suit the application: Grade 1, 185 degrees; Grade 2, 145 degrees; and Grade 3, 115 degrees.

7.3.7 Specialty doors include those described in 7.3.7.1 through 7.3.7.4.

7.3.7.1 Coiling doors should be protected with slide bolts on the bottom bar unless they are controlled or locked by electric power.

7.3.7.2 An iron keeper for securing the hand chain or an iron pin for the shaft on the crank should be provided.

7.3.7.3 Solid overhead, swinging, sliding, or folding doors should be protected with a cylinder lock or padlock. A metal slide bar, bolt, or crossbar should be provided on the inside.

7.3.7.4 Metal accordion grate or grill-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

7.4 Windows.

7.4.1 Windows are another vulnerable point for gaining illegal access to a building. The window frame must be securely fastened to the building so that it cannot be pried loose. As with glass panels in a door, window glass can be broken or cut so the intruder can reach inside and release the lock.

7.4.2 Windows should be secured on the inside with a window lock, locking bolt, slide bar, or crossbar with a padlock. Under no circumstances should any window lock or bars that are installed deviate from building and fire code requirements for emergency egress.

7.4.3 Bars should be steel of at least ½ in. (12.7 mm) in least dimension and spaced 6 in. (152.4 mm) apart on center. If a grille is used, the material should be at least No. 9 gauge 2 in. (50.8 mm) square mesh. Bars and grills must be securely fastened to the window frame so they cannot be pried loose.

7.4.4 Outside hinges on windows should have nonremovable pins. The hinge pins should be welded, flanged, or otherwise secured so they cannot be removed.

7.5 Security Vaults. A vault is a completely enclosed space with a high degree of protection against forced entry. Vaults are commonly used for storing cash, information, and valuable property. The protection provided by the vault walls, ceiling, floor, and door(s) should be equivalent. For an enhanced level of protection, vaults should be used in combination with intrusion detection systems.

7.5.1 Classification of Vault Walls. The ANSI/UL classification system for burglary-resistant modular vault panels is based on the length of time the vault will resist the efforts of skilled technicians, using tools and torches, to make a significant penetration. The four classifications are: Class M, ¼ hour; Class 1, ½ hour; Class 2, 1 hour; Class 3, 2 hours. The classifications indicate that a vault, constructed with a UL-listed door and modular panels, will resist attempts at entry, using the tools and techniques specified in the standard, for attack times varying from 15 minutes to 2 hours. Entry is defined as opening the door or making a 96 in.^{2} (619.4 cm^2) opening entirely through the door or door frame, the modular panel, or a seam joining two or more modular panels. The smallest dimension of the opening must be at least 6 in. (15.2 cm).

7.5.2 Alternative Vault Wall Constructions. The UL 608 standard for burglary-resistant vaults is performance based and allows for alternative construction materials. Over the years, many types of vault construction have been used, with the type chosen for a particular situation determined by the construction and load capacity of the building. For example, in a high-rise building designed for a maximum floor live load of 100 lb/ft^2 (450 kg/m^2), a conventional vault with reinforced concrete walls would not be chosen, unless extensive structural reinforcement of the building was possible.

7.5.3 Construction Materials. The materials used in constructing vault walls include reinforced concrete, steel lining, reinforced concrete blocks, or a combination of these materials.

7.5.3.1 Reinforced Concrete.

7.5.3.1.1 The majority of vaults built in the past had walls made of reinforced concrete. Vault walls of this type are usually referred to as generic vault walls. Such walls are very heavy, limiting their use to locations that can accept heavy floor loads, such as a basement or a ground floor that has been structurally reinforced. Where floor loading is not a concern, such as in basement or grade locations, reinforced concrete can be used for the vault walls, floor, and ceiling. Protection equivalent to a UL-listed modular vault panel can be obtained using reinforced concrete.

7.5.3.1.2 ASTM F 1090 provides the following equivalencies for reinforced concrete to UL-listed vault doors and modular panels *(see Table 7.5.3.1.2)*:

(1) A 9 in. (22.9 cm) thick reinforced concrete wall will provide protection equivalent to a Class M panel.
(2) A 12 in. (30.5 cm) thick wall will provide protection equivalent to a Class 1 panel.
(3) An 18 in. (45.7 cm) thick wall will provide protection equivalent to a Class 2 panel.
(4) A 27 in. (68.6 cm) thick wall will provide protection equivalent to a Class 3 panel.

7.5.3.1.3 ASTM F 1247 provides the following guidelines for the construction of reinforced concrete (generic) vaults:

(1) The concrete should have a minimum compressive strength of 4000 psi (27.6 MP_a), and the reinforcing should be one of the following types:
   (a) #5 rebars located in horizontal and vertical rows to form grids spaced 4 in. (10.2 cm) on center and parallel to the face of the wall
   (b) Grids of expanded steel bank vault mesh, weighing at least 6 lb/ft^2 (27.0 kg/m^2), and having a diamond pattern not more than 3 in. (7.6 cm) by 8 in. (20.3 cm), placed parallel to the face of the wall and spaced 4 in. (10.2 cm) on center
(2) The reinforcing should be placed in the vault walls, floor, and ceiling as follows:
   (a) For a 9 in. (22.9 cm) thick wall, 2 grids of expanded metal or rebars
   (b) For a 12 in. (30.5 cm) thick wall, 2 grids of expanded metal or 3 grids of rebars
   (c) For an 18 in. (45.7 cm) thick wall, 3 grids of expanded metal or 4 grids of rebars
   (d) For a 27 in. (68.6 cm) thick wall, 4 grids of expanded metal or 5 grids of rebars

7.5.3.2 Laminated Panels.

7.5.3.2.1 A steel/ply system consisting of two layers of No. 9 gauge low-alloy steel sandwiching a sheet of ¾ in (1.9 cm) thick exterior grade plywood was found to afford good protection against attack by drilling, sawing, and cutting. In testing performed by a government laboratory, the laminated panel resisted, for approximately 15 minutes, attempts to make a 9 in. × 12 in. (22.9 cm × 30.5 cm) opening with an electric drill, an electrically powered reciprocating hacksaw, and an oxygen lance. (For comparison purposes, a steel plate of equal thickness was penetrated in less than 3 minutes with the oxygen lance.) An additional 5 minutes of protection was achieved by placing 90 lb (40.8 kg) gravel finish roofing paper next to the steel layers.

7.5.3.2.2 An advantage of the steel/ply system, besides its light weight, is that it can be used to retrofit the walls, floor, and ceiling of a vault lacking in burglary resistance. The sheets of steel and plywood, either fastened or bonded together, can be precut and carried to the job site for installation as a liner in an existing vault.

7.5.3.3 Steel Lining.

7.5.3.3.1 Plates of steel are used to construct vault walls because their light weight, compared to other materials, allows for their application in high-rise structures where floor loading can be a concern. Steel plate without other protective materials, however, is unacceptable for vault wall construction because it is very vulnerable to torch attack. Although it can provide protection against common hand tools, steel affords minimal protection against a torch.

7.5.3.3.2 In prior testing by UL, making a manhole-size opening with a torch in a ½ in. (1.3 cm) thick steel plate took less than 2 minutes, a 1 in. (2.5 cm) thick plate withstood attack for about 3 minutes, and a 1½ in. (3.8 cm) thick plate lasted a little less than 4 minutes.

7.5.3.4 Reinforced Concrete Block.

7.5.3.4.1 Vault walls also can be constructed of 8 in. (20.3 cm) or 12 in. (30.5 cm) thick concrete blocks filled with concrete and reinforced with steel rods. This method of vault construction has gained acceptance because it is less expensive and lighter than a reinforced concrete wall, making it suitable for use in some high-rise buildings without extensive structural reinforcing. Walls of this type are often backed by ½ in. (1.3 cm) or 1 in. (2.5 cm) steel lining to improve their security.

7.5.3.4.2 Vault walls of reinforced concrete block with steel lining (often referred to as a *jeweler's special*) provide a level of protection better than that of steel lining but not as good as

Table 7.5.3.1.2 Reinforced Concrete Equivalencies to UL-Listed Vault Doors and Modular Panels

UL Classification	Thickness of Reinforced Concrete		Reinforcement No. of Rows of #5 Rebars	No. of Grids of Expanded Metal
	in.	cm		
Class M	9	22.9	2	2
Class 1	12	30.5	3	2
Class 2	18	45.7	4	3
Class 3	27	68.6	5	4

that from a reinforced concrete wall of equal thickness. It is preferred that a listed lightweight modular panel be used in place of reinforced concrete block.

7.5.4 Vault Doors. The ANSI/ UL classification system for burglary-resistant vault doors is based on the length of time the vault will resist the efforts of skilled technicians, using tools and torches, to make a significant penetration. The four classifications are directly related to vault constructions and should meet or exceed that of the overall vault modular panels rating: Class M, ¼ hour; Class 1, ½ hour; Class 2, 1 hour; Class 3, 2 hours.

7.6 Strong Rooms.

7.6.1 Description. A strong room is an enclosed space constructed of solid building materials. Strong rooms are normally used for the storage of classified material or sensitive materials, such as firearms. Protection is normally supplemented by guards or alarm systems. Rooms that have false ceilings, walls constructed of fibrous materials, and other modular or lightweight materials cannot qualify as strong rooms.

7.6.2 Construction Standards.

7.6.2.1 Heavy-duty builder's hardware should be used in construction. All screws, nuts, bolts, hasps, clamps, bars, hinges, and pins should be securely fastened to preclude surreptitious entry and to ensure visual evidence of forced entry. Hardware accessible from outside the strong room must be peened, brazed, or spot welded to preclude removal.

7.6.2.2 Walls and ceiling should be made of plaster, gypsum board, metal, hardboard, wood, plywood, No. 9 gauge or heavier 2 in. wire mesh, or other material of sufficient strength or thickness to deter entry and/or give evidence of unauthorized entry. Insert-type panels should not be used.

7.6.2.3 Floors should be solidly constructed using concrete, ceramic tile, or wood.

7.6.2.4 Windows that open and are less than 18 ft (5.5 m) from an access point (such as the ground, another window outside the area, roof, ledge, or door) should be fitted with ½ in. (12.7 mm) horizontal bars and crossbars). In place of bars, No. 9 gauge wire mesh can be fastened by bolts extending through the wall and secured on the inside of the window board. Windows should be kept closed and made opaque by any practical method.

7.6.2.5 Where ducts, registers, sewers, and tunnels are of such size and shape (in excess of 96 $in.^2$ (619 cm^2) inches and over 6 in. (15.2 cm) in the smallest dimension) as to permit unauthorized entry, they should be equipped with man-safe barriers such as wire mesh or steel bars.

7.6.2.6 Doors should be substantially constructed of wood or metal. Where windows, panels, louvers, or similar openings are used, they should be secured with No. 18 gauge expanded metal or wire mesh securely fastened on the inside of the room.

7.7 Safes.

7.7.1 Designed Resistance. Safes are designed to be burglary-resistant or fire-resistant. Not all fire-resistant safes are burglary resistant.

7.7.2 Classification of Burglary-Resistant Safe. UL 687 classifies burglary-resistant safes according to the length of time the safe will resist various methods of expert burglary attack.

7.7.2.1 Tool-Resistant Safe — Class TL-15.

7.7.2.1.1 This represents a combination-locked steel chest, weighing at least 750 lb (340 kg) or with means for anchoring it in a larger safe, in concrete blocks, or to the premises, that is designed to offer protection for 15 minutes against entry by common hand tools, picking tools, mechanical or portable electrical tools, grinding points, carbide drills and pressure-applying devices. Entry is defined as opening the door or making a 6 $in.^2$ (38.7 cm^2) opening entirely through the door or front face.

7.7.2.1.2 The metal used in the body of the safe usually is open-hearth steel 1 in. (2.54 cm) thick with an ultimate tensile strength of 50,000 psi (345 MPa) or ½ in. (12.7 mm) thick steel with an ultimate tensile strength of 100,000 psi (690 MPa). Materials other than steel can be used if, in testing by UL, they can be shown to provide equivalent resistance to attack.

7.7.2.1.3 The door of the safe is usually of steel at least 1½ in. (3.81 cm) thick with hardened steel plate on the inside of the door to protect the locking mechanism. Composite materials (i.e., metal alloys) can be substituted for the steel if their attack resistance is equal to or better than that for steel. The safe is required to have a combination lock, complying with UL 768 of Group 2M, 1, 1R; or UL 2058.

7.7.2.1.4 The UL tests on TL-15 and deposit safes (see 7.7.2.2) are limited to the door and front face. Because pressure-applying devices and carbide drills can easily penetrate the body of these safes, they should be clad in concrete to improve their burglary resistance. Their use should be limited to low-risk situations where inventory values are kept to a minimum.

7.7.2.2 Tool-Resistant Safe — Deposit Safes. This safe is similar in design to the TL-15 safe, except that it is provided with a mechanism for making money deposits. Because the safe is designed to receive envelope and deposit bags, UL performs fishing and trapping tests to determine its resistance to these methods of attack. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 2M, 1, 1R; or UL 2058, Type 1.

7.7.2.3 Tool-Resistant Safe — Class TL-30. The body and door of this safe are very similar in design to those of the TL-15 safe, with the exception that the hardened steel plate, used to protect the lock mechanism, usually extends over the entire face of the door. This safe is required to resist entry, defined as opening the door or making a 6 $in.^2$ (38.7 cm^2) opening entirely through the door or front face, for 30 minutes using the same tools specified for the TL-15 safe and abrasive cutting wheels and power saws. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 2M, 1, 1R; or UL 2058, Type 1. The same limitations in the use of the TL-15 safe apply to this safe, since the safe's body is vulnerable to attack. Encasing the safe in reinforced concrete improves its performance.

7.7.2.4 Tool-Resistant Safe — Class TL-15x6. This upgraded version of the "door only" TL-15 safe provides equivalent protection on all six sides, thus the "x6" nomenclature. The body and door of these safes usually are built of composite materials that can resist attack from common hand tools, abrasive cutting wheels, and power saws. Entry is defined as opening the door or making a 6 $in.^2$ (38.7 cm^2) opening entirely through the door or body of the safe, compared to through just the door and front face for the TL-15 and TL-30 safes. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 2M, 1, 1R; or UL 2058, Type 1.

7.7.2.5 Tool-Resistant Safe — Class TL-30x6. Like the TL-15x6 safe, this is an upgraded version of the "door-only" TL-30

safe. This safe provides a moderate degree of burglary protection on all six sides. Entry is defined as opening the door or making a 6 in.^{2} (38.7 cm^2) opening entirely through the door or body of the safe. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 2M, 1, 1R; or UL 2058, Type 1.

7.7.2.6 Torch- and Tool-Resistant Safe — Class TRTL-30.

7.7.2.6.1 This represents a combination-locked safe weighing at least 750 lb (340 kg) and having a body constructed of solid open-hearth steel at least 1 in. (2.54 cm) thick with a tensile strength of 50,000 psi (345 MPa). The body of the safe is required to be encased in reinforced concrete at least 3 in. (7.62 cm) thick with a minimum compressive strength of 4,000 psi (27.6 MPa). Materials other than solid metal encased in concrete can be used if they can be shown to provide equivalent resistance to attack.

7.7.2.6.2 The UL tests on this safe are restricted to the door and front face; no tests are performed on the body of the safe. The door and front face are required to resist attack using the same tools as for the TL-30 safes and an oxyacetylene torch. The protection to torch attack is achieved through the use of copper or an alloy material in the door and front face, which helps dissipate the heat of the torch. This is the lowest rated UL safe that resists attack using an oxyacetylene torch.

7.7.2.6.3 Entry into this safe is defined as opening the door or making a 2 in.^{2} (12.9 cm^2) opening (compared to a 6 in.^{2} (38.7 cm^2) opening for tool-resistant safes), entirely through the door or front face. This size opening is designed to resist a "fishing-type" burglary attack, in which a small hole is drilled in the safe and an attempt is made to "fish" out the valuables. The safe is required to have a combination lock complying with UL 768 of Group 1 or 1R; or UL 2058, Type 1.

7.7.2.6.4 The limitation in the protection afforded by this safe is that the steel walls of the safe are vulnerable to torch attack once the concrete cladding is removed. The safes with composite materials in the body provide better protection. The TRTL-30 safe provides only moderate burglary protection because of the lack of testing on the body of the safe.

7.7.2.7 Torch- and Tool-Resistant Safe — Class TRTL-15x6.

7.7.2.7.1 This is the lowest rated safe that provides six-sided protection from tool and torch attack. This safe provides better protection in the walls than safes with the TRTL-30 label. Besides the tools permitted for testing the TRTL-30 safes, UL also allows the use of impact tools (such as an impact hammer, which is very effective in penetrating concrete). Entry into this safe is defined as opening the door or making a 2 in.^{2} (12.9 cm^2) opening entirely through the door or body. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 1 or 1R; or UL 2058, Type 1.

7.7.2.7.2 Safes with this label are intended for the medium-risk situation. The door and body of the safe are usually constructed of super-hard composites that resist both tool and torch attack. These safes usually are manufactured with an inner and an outer steel shell, between which the composite material is poured and allowed to harden. The lock and boltwork are quite sophisticated, with hard-alloy plates protecting not only the lock itself, but the boltwork as well. The bolts are usually of a hardened steel alloy to resist torch and tool attacks.

7.7.2.8 Torch- and Tool-Resistant Safe — Class TRTL-30x6. Safes with this label are intended for high-risk situations with substantial inventory levels. The construction of this safe is similar to that of the TRTL-15x6, except that it is required to provide twice the protection in terms of length of time. The tools used in the test are the same as those used on the TRTL-15x6, as is the definition of "entry." The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 1 or 1R; or UL 2058, Type 1.

7.7.2.9 Torch- and Tool-Resistant Safe — Class TRTL-60x6. Prior to the introduction of the TRTL-30x6 in 1980, this was the lowest rated of the UL safes that provided six-sided protection, even though UL classified it as TRTL-60. In the 1995 edition of UL 687, the classification was changed to TRTL-60x6. This means that only safes manufactured after 1995 will bear the TRTL-60x6 label; all older safes will have the TRTL-60 label.

7.7.2.9.1 The same testing requirements and tool complement that apply to the TRTL-30x6 safe apply to this safe. The safe is required to weigh at least 750 lb (340 kg) and have a combination lock complying with UL 768 of Group 1 or 1R; or UL 2058, Type 1.

7.7.2.9.2 This safe finds application in high-risk situations; however, because of its high cost, it has essentially been replaced by the TRTL-30x6 safe, which is less costly.

7.7.2.10 Torch-, Explosive-, and Tool-Resistant Safe — Class TXTL-60x6. This safe also did not have the "x6" designation until 1995, so safes manufactured prior to 1995 will have a TXTL-60 label. This safe is intended for the very highest risks and is designed to offer six-sided protection against entry from explosives, torches, and tools for 60 minutes, with the explosive charge limited to 4 oz (113 g) of nitroglycerine or its equivalent. UL requires that the safe weigh at least 1000 lb (454 kg) and have a combination lock complying with UL 768 of Group 1 or 1R; or UL 2058, Type 1.

7.7.3 Fire-Resistant Safes. There are three classes of fire-resistant safes. All three classes must pass three tests: fire endurance, explosion, and impact. During the fire endurance test, the inside temperature of a safe cannot exceed 350°F (176.7° C) at any time during the test. At the end of the test, all papers inside a safe must be entirely legible and uncharred.

7.7.3.1 Class 350-4 Hours. A safe containing papers and records is placed in a testing furnace, and the temperature is raised through a standard curve until it is 2000°F (1093°C) at the end of 4 hours.

7.7.3.2 Class 350-2 Hours. A specimen safe containing papers and records and placed in a testing furnace must withstand 2 hours of exposure to heat reaching 1850°F (1010°C).

7.7.3.3 Class 350-1 Hour. A specimen safe containing papers and records is placed in a testing furnace for a 1-hour exposure to heat reaching 1700°F (927°C).

7.8 Insulated Filing Devices. Insulated filing devices afford considerably less protection for records than the three levels of fire-resistant containers discussed in 7.7.3. The thermocouple devices to measure interior heat during the tests are located in the center of the interior compartment, and the insulated filing devices are not drop tested. Because it is possible to confuse the 350-1 Insulated Filing Device with the 350-1 Fire-Resistant Safe, the label should be carefully noted.

7.8.1 Class 350-1 Hour. A specimen filing device is placed in a testing furnace and heated to a temperature of 1700°F (927°C) for 1 hour.

7.8.2 Class 350-½ Hour (Former UL and SMNA Classification "E"). A specimen filing device is heated for ½ hour to a temperature reaching 1550°F (843°C) in a test furnace.

7.9 Combination Locks for Safes and Vaults. These types of locks are classified by UL as Group 1, Group 1R, Group 2, or Group 2M according to the degree of protection afforded against unauthorized opening.

7.9.1 Group 1. Group 1 combination locks afford a choice of at least 1,000,000 combinations and are highly resistant to expert or professional manipulation for a period of 20 man hours.

7.9.2 Group 1R. Group 1R combination locks afford a choice of at least 1,000,000 combinations and are highly resistant to expert manipulation. In addition to resisting unauthorized opening by expert manipulation, these locks are secure against radiological attack.

7.9.3 Group 2. Group 2 combination locks afford a choice of least 1,000,000 combinations and have a moderate degree of resistance to unauthorized openings.

7.9.4 Group 2M. Group 2M combination locks afford a choice of least 1,000,000 combinations and have 2 man hours of resistance to expert or professional manipulation. These combination locks are considered suitable for use on insulated safes, insulated record containers, insulated vault doors, light vault doors, and tamper-resistant doors.

7.10 Combinations Numbers.

7.10.1 Changing Combinations. Combinations to insulated and burglary-resistant containers should be changed by the responsible individual, the security officer, or a bonded contractor. Combinations should be changed when the container is placed in use, when an individual knowing the combination no longer requires access to the container, when the combination has been lost or is suspected to have been lost, at least once every 12 months, or when the container is taken out of service. Combinations to containers taken out of service must be reset to the standard factory combination of 50-25-50 prior to removal from the office space.

7.10.2 Methods. Combination locks have either hand-change or key-change capability. A number of combination locks produced by a variety of manufacturers have been approved by the General Services Administration (GSA). GSA-approved locks and nonapproved locks use slightly different operating instructions and unique keys or particular hand-change techniques for changing combinations. Often the experience necessary, as well as change keys, operating instructions, and changing procedures, are lost with the passing of time.

7.10.3 Safeguarding Combinations.

7.10.3.1 Selecting a Combination. When selecting combination numbers, avoid multiples of 5, ascending or descending numbers, simple arithmetical series, and personal data such as birth dates and Social Security numbers. Use numbers that are widely separated. This can be achieved by dividing the dial into three parts and using a number from each third as one of the high-low-high or low-high-low sequences. The same combination should not be used for more than one container in the same office. Carefully follow manufacturers' instructions in installing combination numbers.

7.10.3.2 Protecting Combinations. Combinations should be known only by those persons whose official duties require access. The written combination should be protected at the highest classification level of material in the container or be protected in a manner commensurate with the value of the protected material. Combinations should be memorized. They must not be carried in wallets, concealed on persons, or written on calendars, desk pads, and so forth. When opening any kind of combination lock, be sure that no unauthorized person can learn the combination by observing the sequence of numbers being entered or dialed. It can be necessary to position your body so as to block the dial from the view of anyone standing nearby.

7.10.3.3 Recording Combinations. Each security officer should ensure that a record of the combination to each vault, secure room, combination padlock, and security container is recorded showing the location of the container or room; the name, home address, and home telephone number of a person responsible for the container; and the names of all individuals having knowledge of the combination. Some standard forms have been designed for this purpose. A central repository, usually the most secure container, should be designated to hold the sealed SF 700 form for use during emergencies. Only appropriately authorized employees should be given access to a combination.

Chapter 8 Interior Security Systems

8.1 General. There are few facilities where access is intended to every area in the facility. Accordingly, access to some areas is necessarily controlled. For example, interior controls are necessary to protect confidential information from unauthorized disclosure, to prevent damage to the area or equipment, to prevent interference with operations, for safety purposes, or for a combination of these and other reasons.

8.1.1 Usually, interior controls are applied to specific rooms or physical spaces within a building. The senior facility manager or responsible manager should determine whether interior controls are necessary. Office area controls can include key accountability systems, locking devices, and access control systems such as sign-in registers and automated systems.

8.1.2 Determination of the extent of interior controls should take into consideration the monetary value and mission criticality of the items or areas to be protected, the vulnerability of the facility, and the cost of the controls. Normally, the cost of security controls should not exceed the value of the asset or areas to be protected.

8.2 Area Designations. The decision to designate an area as either a "Controlled Area" or a "Restricted Area" should be made in conjunction with a decision to close the property or a portion thereof to the public.

8.2.1 Controlled Area. A controlled area is defined as a room, office, building, or other form of facility to which access is monitored, limited, or controlled. Admittance to a controlled area is limited to persons who have official business within the area. Responsible managers are authorized to designate an area as a controlled area after adequate security measures are in place. Typically the following minimum areas should be designated as controlled areas:

(1) An area where confidential information or highly sensitive information is handled, processed, or stored (e.g., a mailroom)

(2) An area that houses equipment that is significantly valuable or critical to the continued operations or provision of services
(3) An area where uncontrolled access would interfere with or disrupt personnel assigned to the area in carrying out their official duties
(4) An area where equipment or operations constitute a potential safety hazard
(5) An area that is particularly sensitive as determined by the responsible manager

8.2.2 Restricted Area. A restricted area is a room, office, building, or other form of facility to which access is strictly controlled. Admittance to a restricted area is limited to personnel assigned to the area and persons who have been specifically authorized access to the area. Visitors to a restricted area must be escorted by personnel assigned to the area, and all classified information must be protected from observation, disclosure, or removal. The responsible manager is authorized to designate an area as a restricted area after adequate security measures are in place. If applicable, the following minimum areas should be designated as restricted areas:

(1) An area that houses mainframe computers or designated sensitive information systems
(2) An area that is highly critical or sensitive as determined by the responsible manager

8.3 Intrusion Detection Systems. Intrusion detection systems are intended to sound alarms or alert response personnel of an actual or attempted intrusion into an area. See NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, for installation requirements of these systems. These warning systems detect intrusion or attempts, but do not prevent them. Any intrusion detection system requires an assessment and a response capability to provide protection for an area. All systems have vulnerable points by which their functioning can be minimized or completely interrupted or circumvented.

8.4 Planning Intrusion Detection System Installations. Intrusion detection systems are used to detect intrusion. Some are intended for exterior (outdoor or unconditioned area) protection, and some are suitable only for indoor installations. The following should be considered in the planning of an intrusion detection system:

(1) Sensitivity or criticality of the operation
(2) Facility vulnerability to damage, interruption, alteration, or other harm
(3) Sensitivity or value of the information or property stored within or at the facility
(4) Location of the facility and accessibility to intruders
(5) Other forms of protection in place or available
(6) Law enforcement or responder capability

8.5 Components of an Intrusion Detection System. An intrusion detection system is composed of one or more sensors to detect the presence or actions of an intruder and a control unit that constantly monitors the sensors and can actuate signaling devices or transmit an alarm signal off premises when a sensor is activated.

8.5.1 Perimeter protection alarm systems utilize point protection sensors almost exclusively, while area protection (volumetric) sensors are used primarily in interior alarm circuits to detect an intruder within a building. Object protection provides direct security for individual items and is often the final stage of an in-depth protection system with perimeter and area protection.

8.5.2 Intrusion detection systems can be designed so that various parts of a building have separate sensor circuits, or zones. Duress or holdup alarm circuits can be added to enable employees to summon security personnel.

8.5.3 The installation of intrusion detection system components is very important, and attention should be given to NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, and the manufacturers' specifications. Individual sensors are designed to respond to specific stimuli that indicate the presence of an intruder or an attempt to gain entry into a protected area. Similarly, switch sensors must be mounted so that they detect the actual opening of a door or window, but at the same time, the manner of installation should not make them prone to nuisance tripping. Conditions that can cause nuisance tripping include vibrations from passing trucks, wind rattling doors or windows, flickering lights, electromagnetic interference from mobile radios, and thunderstorms.

8.6 Sensors. The three basic types of sensors are perimeter, volumetric, and proximity.

8.6.1 Perimeter Sensors. The most common points for perimeter sensing devices are doors, windows, vents, and skylights. These openings can be protected, with devices intended to sense their position, forcing, or breaking. If intrusion occurs through unprotected walls or ceilings, these devices can be ineffective.

8.6.1.1 Contact Switches. These devices are usually magnetic operated switches affixed to a door or window in such a way that opening the door or window beyond a specific gap breaks a magnetic field, causing the switch to trip (an alarm). High-security switches are normally balanced or biased magnetic switches.

8.6.1.2 Metallic Foil. Metallic foil window tape is a traditional method for detecting glass breakage. Strips of thin foil are affixed to a glass surface. Breaking the glass also fractures the foil, which interrupts an electronic circuit, causing an alarm. Metallic foil deteriorates with time and can require frequent maintenance.

8.6.1.3 Screens. Openings such as vents, ducts, skylights, and similar openings can be alarmed by thin wire filaments that signal an alarm if the screen is cut or broken. Often the wire filaments are placed in a frame of wooden rods and require little maintenance.

8.6.1.4 Glass Breakage (Tuned Frequency) Sensing Devices. Electronic circuits are designed to detect a specific frequency sound pattern when the glass is broken.

8.6.1.5 Glass Breakage (Inertia) Sensing Device. This device is attached to a window or frame and can detect glass breakage from single or multiple glass panels. This device requires "shock," which is generated during intrusion, to activate the alarm system, thereby opening the normally closed circuit of the protective loop on the security system. Some shock sensors require a separate analyzer to function or utilize the alarm system's protective loop voltage for power.

8.6.1.6 Lacing. Lacing can protect walls, doors, and safes against penetration. Lacing is a closely woven pattern of metallic foil or fine brittle wire on the surface of the protected area. An intruder can enter only by breaking the foil or wire. A panel over the lacing protects it from accidental damage.

8.6.2 Volumetric Sensors. Volume protection sensors are designed to detect the presence of an intruder almost anywhere

within an entire room, from floor to ceiling. A variety of volumetric devices are available. Each type of detector has inherent advantages and limitations. Therefore, a device must be selected with consideration given to specific environmental factors. A major advantage of volumetric devices is that they provide a highly sensitive and invisible means of detection in high-risk areas. The major disadvantage is that an improper application can result in frequent false alarms.

8.6.2.1 Passive Infrared Detectors. A passive infrared detector is designed to detect the difference between air temperature and mass temperature when an intruder enters its protected field of detection range. This differential activates the initiating device.

8.6.2.2 Ultrasonic Detectors. Ultrasonic motion detectors generate a high frequency of sound that is out of the normal range of human hearing. An intruder disrupting the ultrasonic wave pattern initiates the alarm. Because ultrasonic devices are prone to false alarms due to excessive air currents or ultrasonic noise from mechanical equipment, their use in buildings is discouraged.

8.6.2.3 Microwave Detectors. Microwave detectors use high-frequency radio waves to detect movement. Because microwave energy penetrates materials such as glass, and metal objects reflect them, they can detect motion outside the protection area, causing false alarms if not properly installed.

8.6.2.4 Photoelectric Devices. Photoelectric devices transmit a beam across a protected area. When an intruder interrupts this beam, the circuit is disrupted, causing an alarm. Photoelectric devices use diodes that emit an invisible infrared light and usually pulses rapidly to prevent compromise by substitution. Consideration should be given to the fact that the detection beams are narrow and can be discovered or avoided by an intruder.

8.6.3 Proximity Sensors. Proximity object protection provides direct security for individual assets.

8.6.3.1 Capacitance Sensors. A capacitance sensor is used to protect specific objects such as file cabinets, security containers, and safes. False alarms can occur if the container is carelessly touched when the device is armed.

8.6.3.2 Vibration Detectors. These seismic sensing devices use a piezoelectric crystal or microphone to detect a sound pattern, such as a hammer-like impact on a rigid surface. These devices are attached directly to safes and filing cabinets or to the walls, ceiling, and floor of vaults. False alarms can occur with these devices by external factors such as passing vehicles or falling objects.

8.7 Intrusion Detection System.

8.7.1 Characteristics. All intrusion detection systems incorporate a control unit, which might or might not be a separate component. The control unit is able to regulate the entire system, turn an intrusion detection system on and off, and transmit the alarm signal to an annunciator or monitoring station. The method for controlling the intrusion detection system is usually a key or a digital keypad located inside the premises to avoid tampering. When someone enters a protected area, the alarm is delayed briefly to allow authorized user to disarm the system without initiating an alarm. With local systems, the user is responsible for turning the alarm on and off. The central station and proprietary systems shift responsibility for verifying that the system is on or off from the user to the central station or proprietary personnel. Intrusion detection system monitoring falls into three categories: local, central station, and proprietary.

8.7.2 Local Intrusion Detection System. The local intrusion detection system has circuits within the secured areas that are directly connected to audible or visible signaling devices such as lights, bells, or sirens. The signaling devices are normally mounted on the exterior of the building, or in large buildings, at an interior location where they will be audible or visible at a reasonable distance. The signaling device should be protected from weather and tampering.

8.8 Annunciator. An annunciator is a unit containing one or more indicator lamps, alphanumeric displays, or other equivalent means on which each indication provides status information about a circuit, condition, or location.

8.9 Line Supervision. The means used to transmit the alarm signals from the protected area to the monitoring station should be protected to prevent interruption, manipulation, or defeat of the alarm signal. To ensure such integrity, the transmission means should be electronically supervised.

8.10 Intrusion Detection Systems — Extent of Protection. The amount of alarm protection installed in a system is designated as the extent of protection provided in UL 681.

8.11 Video Surveillance. A video surveillance system can detect motion or heat or be used to remotely observe a location.

8.11.1 Automatic Assessment.

8.11.1.1 Video surveillance can be used as a monitoring and detection device to trigger alarms.

8.11.1.2 A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected, such as a safe or a doorknob. When the image of an intruder or moving object enters the monitored window, the difference in contrast is detected and triggers an alarm.

8.11.2 Manual Assessment. A video surveillance system can be used to visually assess the cause of an alarm or monitor critical locations. Visual monitoring from a remote location is advantageous for locations such as gates, doors, corridors, elevators, and other areas where it is not practical or cost effective to post a guard.

8.11.2.1 Equipment. Video surveillance equipment should provide appropriate resolution equal to or greater than the manufacturer's resolution specified in a marking on the equipment or in the literature packaged with the video equipment. Video surveillance equipment should be listed for its purpose as specified in UL 3044.

8.11.2.2 Advantages.

(A) One individual can monitor several video surveillance camera locations simultaneously.

(B) The image is visual and conveys much more information than other types of alarm system components.

(C) Authorized individuals can be distinguished from unauthorized persons.

(D) The signal can be recorded by a video recorder for playback and analysis at later time. Many recorders have a time-lapse mode for quick playback of lengthy periods of tape coverage. This system is often used in conjunction with a date-time generator that

can project a continuous image of the date and time in the corner of the monitor screen.

8.11.2.3 Disadvantages. The weakness in video surveillance systems is the human/machine interface.

(A) Monitors generally do not provide an alarm to alert the observer.

(B) The attention span of persons monitoring TV images is generally short.

(C) There are often distractions at monitoring stations.

8.12 Holdup, Duress, and Ambush Alarms. The teller's holdup alarm in a bank is a common example of an emergency alarm. Based on a risk analysis, emergency alert alarms should be considered for use at medical treatment facilities, personnel counseling or interview offices, credit unions, cash-handling activities, and other high-risk areas. The type and location of the device should be selected carefully to ensure the device is readily available for surreptitious activation in an emergency. If there is a building security force, a silent alarm should annunciate at the dispatch point. If not, the alarms can be transmitted directly to a central station monitoring location or directly connected to local police.

8.12.1 Planned Response. The planned response to an emergency alert alarm must be designed to prevent endangering the occupants or creating hostage situations.

8.12.2 Holdup Switches. The actuating device should be designed to avoid accidental actuation. Double-squeeze buttons, triggers in trigger guards, and a variety of other devices can be used to deter accidental signaling.

8.12.3 Manual Switches. Manual switches provide a holdup alarm system in which the signal transmission is initiated by the person attacked manually activating the device.

8.12.4 Automatic Switches. Automatic switches provide a holdup alarm system that is automatically activated by device such as a money clip in a cash drawer.

8.12.5 Foot Rails. A foot rail is a type of holdup switch securely mounted on the floor and designed to minimize nuisance alarms. It permits unobtrusive operation.

8.13 Electronic Access Control Systems. As a result of increased security awareness, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. The technology used in access control systems ranges from simple push-button locks to computerized access control systems integrated with video surveillance systems. Regardless of the technology used, all access control systems have one primary objective — to screen or identify individuals prior to allowing entry. Since identification is the foundation of all access control systems, they generally require that the user be in possession of an identification credential.

8.13.1 Types of Access Control Systems. Access control systems can be of either the stand-alone type or the multiple-portal type. While each type performs essentially the same functions, stand-alone systems are limited in data storage and system features.

8.13.1.1 Stand-Alone Systems. Stand-alone systems are used to control access at a single entry point and are available either as one integral unit or as two separate components — a reader/keypad and a controller. While stand-alone systems can be networked, they generally do not require a central processing unit (CPU). Data for the entire user population are stored in the unit. The installation of a stand-alone system is simple and thus cheaper, since there is no need to run wires to connect the unit(s) to the CPU.

8.13.1.2 Multiple-Portal Systems. Multiple-portal systems are part of a large network of readers and controllers that are connected to a CPU and that can regulate activities at more than one entry point at a time. Some systems are directly under the control of the CPU, while others are programmed to receive only periodic programming updates or to upload data according to a preprogrammed schedule. Installation costs for these systems are relatively high because of the need to interconnect the units to the CPU.

8.13.2 Access Control Systems. Access control systems can range from small, relatively simple one-door affairs to highly complex, computer-operated systems capable of handling hundreds of doors and tens of thousands of individually encoded identification credentials. A basic system usually consists of a CPU, a reader at each protected door, and an identification credential assigned to each user. A printer is often included to provide a record of all activity. The CPU is the brains of the system and is programmed with data on each user. The data can include an access level, which determines which doors the user is allowed to enter, and time zones, which define the hours of the day and days of the week a user is allowed to enter a door at a particular access level.

8.13.2.1 General.

8.13.2.1.1 When the identification credential is presented to the reader, the requester's identification number is relayed to the CPU. The requester's access level and time zone are instantly checked by the computer. If the identification is valid, the door lock, which can be an electronic or electromagnetic lock or an electric strike, is released. If entry is attempted with a card that is not valid or if a card is used outside its authorized time zone or at an unauthorized door, entry is denied, and an alarm is immediately generated.

8.13.2.1.2 There are three reader types: swipe, in which the card is passed along an open slot; insertion, in which the card is pushed into the reader and withdrawn; and proximity, which requires that the card be moved within a certain distance of the reader.

8.13.2.1.3 In some card access control systems, improved security is achieved by requiring the user to present the card to a reader, as well as enter a unique passcode, a personal identification number (PIN), on a keypad. With this enhancement, the loss of a card will not compromise the system, since an unauthorized user would also need to know the PIN. The added security afforded by the card/PIN combination more than offsets the delay that results from the user having to enter a PIN.

8.13.2.2 Card Technologies. There are at least nine different card-encoding technologies available: magnetic stripe, Wiegand, proximity, barium ferrite, infrared, bar code, Hollerith, "smart" card, and optical storage. The magnetically based technologies include magnetic stripe, Wiegand, and barium ferrite. The optically based technologies are infrared, bar code, optical storage, and Hollerith. Proximity cards and some smart cards use radio signals to communicate with the reader. Surveys indicate that magnetic stripe, Weigand, and proximity technologies control over 80 percent of the market in terms of usage. Selection of a technology involves several factors: encoding security, susceptibility of the reader to environmental hazards, resistance of the

reader to vandalism, initial cost, and long-term cost, including card and reader replacement and reader maintenance costs.

8.13.2.2.1 Magnetic Stripe. This was the first card technology incorporated into access control systems and is the most commonly used today. It is the same technology that finds application in credit cards, ATM cards, debit cards, and a host of other uses. The cards are produced with a narrow strip of magnetic material fused to the back. Data are stored on the strips as a binary code in the form of narrow bars, some of which are magnetized and others not. The card is inserted or swiped through the reader and the code is read.

(A) There are two types of magnetic cards on the market today: the 300 Oersted and the 4000 Oersted, high coercivity card. The code on a 300 Oersted card can become scrambled when subjected to a magnetic field. The 4000 Oersted card is the preferred card, since the material that comprises the magnetic stripe retains data better and is almost invulnerable to magnetic fields.

(B) Although relatively inexpensive and widely used, magnetic stripe cards are one of the most insecure cards in use. The card can be encoded with readily available encoding devices and, as such, should be used only in low-security applications. For higher security applications, the card should be used in combination with a passcode.

(C) Since there is direct contact between the card and reader, both components are subject to wear. The readers are vulnerable to weather and the environment, as well as vandalism, and need regular maintenance.

8.13.2.2.2 Wiegand.

(A) The operation of the Wiegand card is based on the use of short lengths of small-diameter, ferromagnetic wires that have been subjected to a patented twisting process that imparts unique magnetic properties to the wires. When exposed to a magnetic field in a reader, a current is induced in the wires that generates a signal for the reader to pick up.

(B) The Wiegand card provides a very high degree of security, since it is factory-encoded and extremely difficult to counterfeit or alter. It is also immune to electromagnetic (EM) and radio frequency (RF) fields. The reader is completely sealed, which protects the working parts from the elements, and is capable of operating over wide temperature ranges. Weigand cards are relatively expensive when compared to other cards. They can be encoded only once, since the wires within them can be magnetized only one time.

8.13.2.2.3 Barium Ferrite. The barium ferrite card uses magnetized spots to create a code on the card that must match magnets in a reader to close a microswitch. The card has generally been used in high-volume, high-turnover applications, such as parking lots. It affords high encoding security and is relatively inexpensive to produce and encode. Older readers were of the insertion type and subject to high maintenance costs due to wear and the environment. Newer, state-of-the-art readers are of the proximity or "touch" type and use an array of electronic sensor devices installed behind a touch plate to read the magnetic spot patterns on the card.

8.13.2.2.4 Infrared.

(A) Data are stored on an infrared card by means of a bar code written between layers of plastic. The card is read by passing infrared light through it. The bar code in the card casts a shadow on the other side that is read by an array of infrared light sensors. Encoding security is high because duplication is almost impossible.

(B) Although they provide a high degree of security, infrared cards are not in widespread use for access control because of high card and maintenance costs. The optical reader comes in both swipe and insertion styles and is subject to wear and contamination from the environment, requiring regular maintenance.

8.13.2.2.5 Bar Code.

(A) The bar code card is not widely used for access control because encoding security is very low and the bar code strip can be easily damaged. Card encoding is accomplished at relatively low cost. Because the bar code card is an optical system, periodic cleaning and servicing of the reader are necessary.

(B) Bar code labels can be applied to magnetic stripe, Weigand, and other types of cards by simply affixing the label to an area of the card that does not contain information. These types of cards are called *dual technology cards*.

8.13.2.2.6 Optical Storage.

(A) Information is written to an optical storage card by etching small pits into the surface of a reflective layer of plastic using a solid-state infrared laser. The reflective layer is sandwiched between two protective layers of plastic. More than 4 MB of information can be written on the card. The data are secure from compromise, since the information on the card is usually in an encrypted format.

(B) The reader is equipped with a solid-state laser and generally a transport system that moves the card past the reader at a steady speed. Generally, the users are required to enter a passcode before inserting the card. Data are read from the card by a systematic striking of its surface with an infrared beam of light from the laser in the reader. A photo sensor reads the data from fluctuations in the reflected light. While relatively expensive compared with other card technologies, optical storage cards are reusable. The readers and transport systems are initially expensive and require regular maintenance.

8.13.2.2.7 Hollerith. The Hollerith card is the oldest technology in use. Data are written on the card by punching holes in the card. The card is read by either passage of light through the holes or by fine contact brushes that connect with an electrical contact on the other side of the card through the holes. The plastic or paper card is inexpensive, but the security is low. This optical-type card is commonly used in hotels as a replacement for key systems.

8.13.2.2.8 Proximity. Proximity identification credentials are of two types — active and passive. Both types of proximity identification credentials have a microminiature electronic tuned circuit and a switching mechanism buried within them, while active identification credentials also have a power source.

(A) Active identification credentials transmit a coded signal when they come within range of a proximity reader or when someone manually activates them. Other identification credentials transmit a signal continuously. Generally, a long-life lithium battery is used as the power source.

(B) Passive identification credentials rely on an electrostatic field generated by the proximity reader to cause them to transmit a unique coded signal that is received by the reader.

(C) Proximity technology has grown in popularity because of its convenient hands-free feature. An identification credential is

simply waved in front of a reader to transmit the code. Operating ranges are usually from 2 in. to 12 in. (5 cm to 30.5 cm). The identification credential is factory-encoded and difficult to copy or counterfeit and affords good encoding security. Since there is no contact with the reader, identification credential life is generally long, and the reader can be installed inside, behind a wall or glass partition, to afford protection from the elements and vandals. The electronic circuits in the identification credentials, however, can be damaged if handled roughly.

8.13.2.2.9 Smart Card. *Smart card* is a generic term for a single card that serves many functions. The smart card is the state of the art in access control technology. The basic card provides access control and can double as a photo ID card or debit card, as well as serving other functions.

(A) The card contains an integrated circuit in which all the information needed to identify and permit access can be stored, eliminating the necessity for a CPU. To function, a passcode must be provided before the card can be read. Some smart cards are powered by their own battery, while others rely on the reader to power them either directly by a set of external contacts or electromagnetically.

(B) Because of their relatively high cost, at present, the smart cards find limited application. Their use is expected to grow substantially, since they provide a high level of security and can serve many other applications.

8.13.3 Biometric Systems. Establishing a person's identity can be based on three methods: something known by an individual (a password), something possessed by an individual (a card or key), and something physical about an individual (a personal characteristic). Biometric access control devices, or personal characteristic verification locks, rely on the third method. Since duplication of individual physical characteristics is very rare, biometric devices, in theory, could offer the highest security possible. Biometric systems measure a unique characteristic of the person seeking access. These systems are classified as fingerprint, hand or palm geometry, handwriting, voice, and retinal verification systems. Typically, biometric readers are connected to a CPU but can also be used alone.

8.13.3.1 Fingerprint Verification Systems. Fingerprint verification systems have been around for more than a decade. These systems identify an individual by matching stored fingerprints with live prints presented on an electro-optical scanner.

(A) Two types of systems have been developed for fingerprint identification. One system stores a laser picture or hologram on the access card and compares the user's print data to those stored on the card. In the other system, the fingerprint data are indexed in a computer and called up by an access card or code issued to the user. The user places a finger onto the scanner, which optically scans it and compiles, in digital form, a list of significant features (minutiae) of the fingerprint and their locations. The minutiae, which consist of ridge endings and ridge branches, are then compared with the stored data.

(B) Fingerprint verification systems are considered to be very high in their relative resistance to counterfeiting; in more than 60 years of compiling fingerprints, the FBI has never found two sets of identical prints. However, the equipment is very costly and, according to some accounts, can be adversely affected by dirt or grime on the hands. For this reason, most fingerprint verification systems are programmed to give the user a second or third try or to request the use of another alternate finger before rejection.

8.13.3.2 Hand and Palm Geometry Verification Systems. Hand geometry units identify a user by measuring the length and curvature of the fingers of the user's hand together with the degree of translucency of the fingertips and the webbing between the fingers. These measurements are then compared to those stored in a computer. The translucency test is intended to prevent the use of a synthetic "forged" hand. Palm geometry systems optically scan a section of the palm, recording creases, skin tone, and swirls for minute computer analysis. The disadvantages to the use of these systems are that both are very expensive and can be adversely affected by dirt or grime on the hands.

8.13.3.3 Handwriting Verification Systems. Handwriting verification systems are also referred to as signature dynamics verification. These systems are based on an examination of the dynamics of writing, that is, the speed, rhythm, and peculiar flourishes a person uses rather than the signature itself. While a forger may be able to duplicate a signature, the dynamics of the signature cannot be falsified for the reason that writing is considered a ballistic motion that is done almost "reflexively," requiring very little conscious effort.

(A) Two methods are used in handwriting verification. One method uses a pen containing an accelerometer to record the dynamics of the signature and to compare them to the data stored on a computer. The other method uses a sensitive tablet that measures the pen's acceleration, pressure, and velocity as it sweeps through the signature.

(B) The greatest advantage to the use of handwriting verification systems in access control is that people are accustomed to and accept signing their names to gain certain privileges, such as cashing a check or paying with a credit card. On the other hand, fingerprint (or palm or hand geometry) verification carries an association with wrongdoing that many people find objectionable.

(C) The major drawback to the use of handwriting verification is that of inconsistencies in writing one's signature. As noted in 8.13.3.3, signature writing is a ballistic motion that requires little conscious effort. However, signing in on a verifier could result in a more conscious effort on the part of a legitimate user, resulting in inconsistencies. For this reason, handwriting verification systems use the average of three or four signature dynamics for the data stored in the computer. Inconsistencies would also come about as a result of an injury to the hand or fingers used in signing one's name.

8.13.3.4 Voice Verification Systems. Certain features of a person's speech, such as resonance, pitch, and loudness, can be used to identify the person. In voice verification systems, also known as speech recognition systems, the prospective user is enrolled by speaking certain key words or phrases into a microphone connected to a computer that translates features of the spoken words into quantitative terms for storage. To gain entry, the user speaks the same words or phrases into a microphone at the access control point for comparison with those stored on the computer. However, because the voice can vary due to the weather, a cold (illness), stress, and other factors, voice recognition systems tend to be error prone, limiting their commercial application.

8.13.3.5 Retinal Verification Systems. Retinal verification systems use the pattern of blood vessels within the retina of the eye, which is unique in everyone, as a means of identifying an individual. The user looks into an eyepiece that scans the retina with a safe low-level infrared light. The infrared light reflected back is

converted into digital data that is compared to information stored in a computer. The limitation in retinal verification systems is that retinal patterns are not stable and can be altered by injury, illness, alcohol, or drugs. There also may be resistance on the part of an individual to look into the device.

8.13.4 Video Monitoring. Among the uses of video monitoring in access control are to remotely identify visitors requesting entry, to verify the identity of employees entering a facility, and to determine who wants to get into or leave a restricted area. Additionally, video monitoring can help to determine that rules are being followed; for example, to ascertain that items such as purses and packages are not carried into or out of controlled areas.

8.13.4.1 A combination video monitoring–intercom system lets security personnel communicate with visitors requesting entry. The system allows a guard to question visitors as to the purpose of their visit and destination and, if necessary, dispatch an escort for the visitor. In this way, control is established for the movement of visitors throughout the facility.

8.13.4.2 Video monitoring can be used with a photo ID card to provide access control for employees. The system can be used at gates, turnstiles, and doors on outer perimeter access points, at main doors in lobbies and rear doors of buildings, and at limited-access areas, such as computer rooms. A photo ID–video monitoring access control system is cost effective because it allows one guard to view many locations from one central console.

8.13.4.3 Controlling the access of people into a facility is not always possible, however. In buildings that are open to the general public, such as retail stores, screening of customers may create such an inconvenience that they will go elsewhere. Nonetheless, video monitoring in such businesses can be effective in preventing crime, since the visible presence of the system may cause would-be criminals to reconsider their actions.

Chapter 9 Security Personnel

9.1 General. Security personnel can be an effective and useful component of a facility's physical security program. The effectiveness of alarm devices, physical barriers, and intrusion detectors can depend on a response by security personnel.

9.2 Determining the Need. Security services can be used for, but are not limited to, the following circumstances:

(1) The mission of the facility is particularly critical.
(2) There is a high level of sensitivity of information handled at the facility, such as national security information.
(3) An in-house response capability is needed, for example, the facility contains alarmed vaults or other sensitive operations, and off-site security personnel or police are not close enough for quick response.
(4) The facility is vulnerable to theft or damage, for example, a facility location in a high-crime area.
(5) Pedestrian or automobile traffic is heavy or congested and requires special controls.
(6) Valuable goods are stored or used in the facility.

9.3 Cost Factors.

9.3.1 As with any expenditure of funds for security, the annual costs of security services normally should not exceed the monetary value of the protected items.

9.3.2 A substantial expense for security services can be required for crowd or traffic control, for safeguarding highly classified or sensitive information, or for protecting material or functions that have high intrinsic rather than monetary value. This is especially true as applied to the safety of employees, since it is impossible to put a dollar value on human lives or peace of mind. A security post in a high-crime area can yield substantial benefits in terms of improved safety, higher employee morale, and increased productivity.

9.4 Security Duties.

9.4.1 Post Orders.

9.4.1.1 Any facility having security officers should have post orders.

9.4.1.2 Post orders should contain a list of the duties of the security officer and instructions to cover reasonably foreseeable events the security officer may encounter.

9.4.1.2.1 Post orders should list the name of the facility, the date issued, effective date, and purpose.

9.4.1.2.2 Duties of the security officer should be listed, including job classification, uniforms, carrying firearms, reporting times, watch tours, hours of coverage, and other duties to be assigned.

9.4.1.2.3 Instructions should be lawful and endeavor to protect the safety of the security officer and those they meet.

9.4.1.3 Post orders should be reviewed and updated at least annually.

9.4.1.3.1 A procedure should be established to inform security officers of changes in post orders.

9.4.1.3.2 Reviews of post orders should be conducted regularly with facility management and security officers.

9.4.2 Services. Security personnel can perform the following services:

(1) *Entrance control.* Operate and enforce a system of access control, including inspection of identification credentials and packages
(2) *Roving patrol.* Patrol routes or designated areas, such as perimeters, buildings, vaults, and public areas
(3) *Traffic control.* Direct traffic (vehicular and pedestrian), control parking, check permits, and issue citations
(4) *Key control.* Receive, issue, and account for certain keys to the building and its internal areas
(5) *Security and fire systems.* Monitor, operate, and respond to intrusion and fire alarm systems or protective devices
(6) *Utility systems.* Monitor, record data, or perform minor operations for building utility systems
(7) *Lost and found.* Receive, provide receipts for, and store found items
(8) *Reports and records.* Prepare reports on accidents, fires, thefts, and other building incidents
(9) *Response to emergencies.* In case of any emergency (e.g., fire, bomb threat, assault, or civil disturbance), respond, summon assistance, administer first aid, and assist public safety personnel
(10) *Law and order.* Maintain law and order within the area of assignment
(11) *Hazardous conditions.* Report potentially hazardous conditions and items in need of repair

9.5 Personnel Requirements. The number of full-time security posts for a facility is determined by the person responsible for site security. The decision should be based on a security vulnerability assessment as described in Chapter 5.

9.6 Security Personnel Selection.

9.6.1 Criteria. When selecting security personnel, the person responsible for site security should give strong consideration to the following factors:

(1) Federal, state, and local laws and regulations pertaining to the site
(2) Candidate's knowledge of criminal activities and proper law enforcement response procedures
(3) Candidate's judgment and emotional stability
(4) Candidate's experience and demonstrated ability to retain composure under pressure
(5) Candidate's personal history free of convictions for felonies or crimes involving dishonesty or moral turpitude

9.6.2 Armed Security Personnel. Security personnel should be armed only when there are compelling reasons.

9.6.2.1 If security personnel are armed for a deterrent effect, that is, to prevent crime or other unauthorized activity, responsible officials must weigh that advantage against such disadvantages as the danger to innocent personnel if a firearm is used by a security person; the possibility of an accidental discharge; and the possibility, no matter how remote, of irrational behavior on the part of security personnel.

9.6.2.2 If the decision is made to provide firearms to security personnel, firearms training should be provided on an ongoing basis.

9.7* Supervision. Security patrols can be supervised using spot checks by supervisors and through daily logs and activity reports. These methods are most effective when applied in conjunction with a system that ensures the patrols are actually performed. Such systems include watchclock service, electronic guard tour monitoring, and watchman systems. These systems provide a documentary record of the locations in the facility that were visited and the times at which each location was visited. Regular review of these records can help to ensure that security personnel are performing their patrols as planned.

Chapter 10 Security Planning

10.1 General. An effective asset protection program should include the development and implementation of a security plan, which should be documented, and the cooperation and support of top management. This facility security plan should address the protection of all of an organization's defined critical assets, which can include people, property, information, and products.

10.2 Security Planning.

10.2.1 Security planning should begin with a security vulnerability assessment (SVA). See Chapter 5 for detailed information regarding the development and implementation of a facility-specific SVA.

10.2.2 A security plan is a document that usually contains an organization's security-related measures and procedures, as well as information required to implement them. The objective of a security plan is to ensure that security measures and personnel respond in an integrated and effective way to mitigate the effects of an adversarial act in a manner that is appropriate for that particular organization or facility.

10.2.3 In addition to features of protection, the security plan usually includes a concise statement of purpose, identifies the intended users of the plan, designates where the master copy is maintained, identifies to whom the plan has been distributed, and contains clear instructions on the use of the security plan.

10.2.4 Specific plan components should be based primarily on the potential threats faced by the organization or facility as determined by the SVA. Nonetheless, given a potentially broad range of threats, priority should also be placed on developing plan components that accomplish the following:

(1) Address events that are most likely to occur and have the greatest potential impact on defined critical assets
(2) Allocate sufficient time and resources to plan development and implementation
(3) Identify and collect the information necessary to develop an effective plan
(4) Are specific and comprehensive

10.2.5 The objectives of the security plan should be obtainable and easily understood. The underlying assumptions of the security plan should be fully examined to make sure that they are correct and well thought out. Responsibilities and authorities of facility personnel should be clearly identified and assigned. Alternatives and options should be incorporated into the plan to make it flexible and capable of responding to changes or unexpected events. The security plan should be reviewed on a regular basis to determine the strengths and weaknesses of the plan.

10.3 Benefits of a Security Plan. A plan provides facility personnel with an effective means of assisting in the prevention and mitigation of the effects of security incidents by integrating those approaches that have proven to be effective in that environment (and others) in the past. This is especially important for new personnel.

10.3.1 When facility personnel are confronted with an incident or situation that is unforeseen, a plan can assist in directing personnel to react in a manner that is appropriate to the situation.

10.3.2 For incident responses that require coordinated actions by many facility personnel (such as evacuations), a security plan with a clear, concise, and useful set of staff activities and responsibilities helps to ensure a rapid and effective response.

10.3.3 Even if a security plan is not implemented exactly as envisioned, contingency planning (the plan and the process of developing it) has the following advantages:

(1) Facility personnel respond more rapidly and effectively than if no planning had taken place.
(2) It promotes an understanding of the issues involved in responding to a variety of threatening or dangerous situations.
(3) It ensures development of complex responses to complex situations.
(4) It provides for a complete examination of difficult and controversial issues, such as who has authority to call for an evacuation or whether ransom will be paid to kidnappers and hostage takers.
(5) It identifies information that must be gathered to respond to an emergency, such as names and up-to-date telephone or radio contact information of all facility personnel, local police stations, and embassies.

(6) It identifies preparations that must be made for an emergency response, such as obtaining communications equipment, consolidating personnel and sensitive records, or keeping funds on hand for an evacuation.
(7) It promotes a sense of ownership and buy-in to the plan among facility personnel who participate in the planning and who will be affected by the plan.
(8) It ensures a clear division of tasks and responsibilities among facility personnel, helping to avoid important things being left undone and the unnecessary duplication of effort.
(9) It produces a plan that, though perhaps not completely applicable to every situation, can serve as a baseline or starting point for a modified plan should an emergency arise.
(10) It identifies training and resource needs of facility personnel, reflecting assigned responsibilities. Personnel should be oriented to the plan and trained in the skills necessary to enable them to fulfill their assigned responsibilities.

10.4 Elements of a Security Plan.

10.4.1 The facility or organization mandate/mission should include a summary of the threat/risk assessment situation, as well as the security strategy of the facility or organization.

10.4.2 Procedures for movement, communication, facility management, reacting to security incidents, and reporting and analyzing incidents are part of the plan. Components of a security plan include the following:

(1) Security vulnerability assessment
(2) Description of the facility and organizational structure
(3) Security organization and operations
(4) Threat/risk assessments
(5) Employee, visitor, and vendor safety

10.4.3 Additionally, components of the security plan can include the following:

(1) Protective barriers
(2) Security and emergency lighting
(3) Alarm systems
(4) Access control (mechanical and electronic)
(5) Electronic surveillance
(6) Computer operations
(7) Communications
(8) Security staff: organization, capabilities, resources, and procedures
(9) Contingency plans: criminal attacks, terrorist attacks, accidents, natural disasters
(10) Outside resources: local, state, and federal public safety (e.g., law enforcement, fire, and emergency medical services)

10.4.4 The supporting information should include the following:

(1) A personnel roster with addresses, telephone numbers, and passport numbers
(2) A list of cooperating agencies, contact people, telephone numbers, and radio frequencies
(3) A list of important contact people (government officials, security personnel, airport and transportation authorities, utility companies, health care facilities and clinics, and so forth)
(4) Maps (regional, national, subregional, local) indicating assembly points, overland routes, air fields, border crossings, and so forth
(5) Emergency supply inventory (food, medical, documents, clothing, and so forth)

10.4.5 The components of a contingency plan are as follows:

(1) Nature of specific incident
(2) General concept of how to react to the incident, including the sequence of personnel activities
(3) Division of responsibilities and authorities among the facility personnel, including who can initiate the plan
(4) Identifying who is covered by the plan (e.g., who is to be evacuated?)
(5) Information on how to contact all personnel
(6) Resources that should be applied to the management of the incident
(7) Guidance on the emergency use of funds, disposition of project property, and personal effects
(8) List of annexes, including maps, forms, location of personnel, telephone numbers, radio frequencies, extraordinary procedures, and so forth

10.5 Planning for Terrorism.

10.5.1 Terrorism is the use of force or violence against persons or property in violation of the criminal laws of the jurisdiction for purposes of intimidation, coercion, or ransom. Terrorists often use threats to create fear among the public, to try to convince citizens that their government is powerless to prevent terrorism, and to get immediate publicity for their causes. Acts of terrorism include threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings, cyber attacks (computer-based), and the use of chemical, biological, and nuclear weapons. In addition to high-risk targets, such as military and other government facilities, airports, and high-profile landmarks, terrorists might also target large public gatherings, water and food supplies, utilities, and corporate centers. Further, they are capable of spreading fear by sending explosives or chemical and biological agents through the mail. An organization or facility should prepare for a terrorist event in much the same way it would prepare for other crisis events.

10.5.2 The U.S. Department of Homeland Security (DHS) has instituted and maintains the Homeland Security Advisory System *(see Annex B)*. The Homeland Security Advisory System was designed to provide a comprehensive means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities as well as to the American people. Annex B contains detailed information about the Homeland Security Advisory System, threat preparedness, and response.

10.6 Pre-Employment Screening. Negligent-hiring liability is a basis for recovery against employers for the wrongful or criminal actions of employees against third parties, whether those actions are performed within or outside the scope of employment. The requirements of this tort are satisfied when the offending employee is hired without an adequate background investigation and when such an investigation would have indicated the applicant was a potential risk.

10.6.1 Pre-employment screening not only is necessary for hiring the best personnel available for the success of an organization, but it can help in protecting against negligent-hiring lawsuits. The courts are increasingly upholding the negligent-hiring doctrine. They are taking the position that the employer should make every effort to ensure that the employee selection process is a reasoned and useful exercise.

10.6.2 A great deal of information is available to an employer willing to invest the time and make a reasonable effort to screen employees. Public records, for example, can tell if an applicant has been convicted of a crime, has sued a previous employer, or

has been the subject of a fraud investigation. Records can verify an applicant's identity, document self-employed business experience, and answer many other questions.

10.6.3 Employers cannot know absolutely, in advance, that a prospective employee will later cause injuries to third parties. Therefore, employers are not exposed to liability simply because they failed to check an applicant's background. It is only when such a check would have revealed information indicating the undesirability of the applicant that the failure to obtain the information can be considered negligence.

10.6.4 The amount of background investigation performed on an applicant should be proportional to the degree of risk presented by the position to be filled. For employees who have frequent contact with the public or close contact with persons due to a special relationship, the courts have stated that the employer has a duty to use reasonable care in hiring the person.

10.6.5 Employers have numerous options available to screen applicants, such as resumes and job applications, reference checks, interviews, and background checks. While some options can be time consuming and expensive, many are fairly straightforward and cost effective. However, the failure to investigate properly can have more severe consequences.

10.6.6 While courts have imposed a responsibility on employers to use due care in screening job applicants, federal and state privacy laws impose restraints on employers that have made the task more difficult and demanding. These laws determine the type of information an employer can request and prescribe how the information can be handled. An employer who does not comply with these laws can become the object of a discrimination lawsuit initiated by a job applicant. For this reason, businesses should understand the privacy rights of job applicants. These rights are provided in laws such as the Discrimination in Employment Act, Title VII of the 1964 Civil Rights Act, the Immigration Reform and Control Act, the 1973 Rehabilitation Act, the Americans with Disabilities Act (ADA), the Fair Credit Reporting Act, and the Privacy Act.

10.6.7 Employers are advised to establish a companywide policy regarding pre-employment screening practices and to be consistent in applying the policy. If, for example, the policy calls for criminal background checks on security officers, then these checks should be obtained for every applicant who is hired as a security officer. Additionally, all information obtained from the background investigation should be well documented, kept confidential, and secured in a safe place.

Chapter 11 Educational Facilities

11.1 General. Educational facilities, for the purpose of this chapter, include primary and secondary schools, colleges, and universities.

11.2 Application. This chapter addresses measures to control security vulnerabilities in educational facilities.

11.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as described in Chapter 5, should be conducted.

11.4 Primary and Secondary Schools. A security program for a primary or secondary school should address the following security vulnerabilities: vandalism, theft and embezzlement, sexual predation, assault, weapons violations, and burglary.

11.4.1 Vandalism Prevention. The impact of vandalism is felt in many areas within a school, from graffiti on walls, to breakage of windows, to malicious destruction of equipment and school property. The majority of recurring losses usually result from window and door glass breakage, at least until such time as the glass is replaced with breakage-resistant materials. However, since windows and doors serve as means of access into a school, glass breakage can serve as a prelude to more serious losses. This can include damage from fires and destroyed school property, such as plumbing and lighting fixtures, athletic and playground equipment, and vehicles.

11.4.1.1 A number of research studies on vandalism in schools have concluded that educational programs for students, designed to teach respect for property, are essential as a preventive measure. However, it is generally not enough to ask that acts of vandalism not occur; a program must be set up to limit the opportunity for vandalism.

11.4.1.2 The success of the program will depend on developing an honest assessment of the scope of the problem; creating awareness of the problem among students, teachers, parents, community leaders, the police, and school administrators and involving them in program planning; convincing potential vandals that they will benefit from the program; and improving the physical security of the school buildings. The following are the general components of a program to deter vandalism and protect school property:

(1) A comprehensive code of conduct
(2) Restrictions on loitering
(3) A system of restitution
(4) Informing the public
(5) Parent/student activities
(6) Community involvement
(7) Security surveys
(8) Evaluation as to whether the school is open for more hours than necessary, as well as which doors need to be left unlocked

11.4.1.3 Studies have indicated that schools that are lax or unfair in the area of discipline have the most serious vandalism problems. A code of conduct that clearly defines each regulation and assigns a specific penalty for each infraction should be developed. The code should be well publicized and strictly enforced.

(A) Acts of vandalism are often associated with persons being on school grounds or in school buildings without authority or permission after school has closed, as well as during hours when school is in session (i.e., students who are in the wrong place at the wrong time).

(B) Some states have statutes that make parents or guardians liable for willful damage to property caused by minors. Peer juries, in which students are selected to serve on a panel to determine the appropriate restitution for offenders, have proven to be effective in some schools.

(C) Schools are often community property supported by taxpayers, so when schools are victims of vandalism, the community pays. Publishing incidents of vandalism can wake up an apathetic community to the problem.

(D) Crime prevention programs can offer a healthy medium for parents and students to become involved in solving a problem that affects everyone.

(E) Competitive school pride programs that are initiated at the district level and that emphasize the positive aspects of care and responsibility for school property can be a real deterrent to school vandalism.

(F) All exterior openings that are accessible to intruders, including main and side doors, delivery entrances, windows, skylights, roof hatches, and openings for ventilation, should be evaluated with respect to their resistance to forced entry and adequately secured. Doors should be of solid construction and provided with high-security locking hardware. Glass panels and sidelights in exterior doors should be protected with wire mesh screens. If not in conflict with requirements of NFPA *101*, *Life Safety Code*, ground floor windows should be protected with wire mesh screening or the glazing replaced with burglary-resistant glazing materials.

(G) Strict control of keys and proper maintenance of locks are essential to good security. At the end of each day, the building should be checked to ensure that nobody has stayed behind and that all doors and windows are securely locked.

11.4.1.4 School grounds should be kept clear of rocks, bottles, and other objects that can be used as missiles. Clear antigraffiti coatings can be applied to surfaces to make them easier to clean. Exterior lighting will serve to discourage vandals. Lighting fixtures should be protected through the use of plastic lenses or metal screens over the fixtures.

11.4.1.5 Video surveillance systems can also be effective in schools as a deterrent to vandalism. Video surveillance systems can be used to monitor the hallways to determine who is there, where they are going, and what they are doing. They can be used to provide surveillance of parking areas. Video surveillance can be combined with video motion detectors to detect and record unauthorized intrusions. Monitoring and response contribute to the effectiveness of deterring vandalism.

11.4.1.6 Physical barriers, such as chain-link fencing and walls, should be sturdy and well-maintained. The entry and movement of visitors, including vendors, service personnel, and salespeople, within school buildings should be controlled and supervised. An intrusion detection system that provides for surveillance of areas through which unauthorized access can be gained is recommended, and the local police should be consulted for advice. However, an alarm system should not be a substitute for good physical security.

11.4.1.7 A designated parking area should be assigned for teachers. Surveillance of this area, whether by patrols or cameras, will serve as a deterrent to the vandalism of vehicles by students.

11.4.1.8 The use of security guards or off-duty police officers can also serve as a deterrent to crime. To be most effective, guards should patrol the facility. Video surveillance systems should not substitute for guard patrols, but they can support the efforts of guards by expanding their surveillance capabilities and providing records of events at the facility.

11.4.1.9 The use of security guards, especially armed personnel, can create liability exposures. Lawsuits involving security personnel have claimed negligent hiring, training, or supervision. Training programs for security personnel should address these exposures.

11.4.1.10 Liaison with the local police should be established and the police requested to include the school grounds in their patrols. Police patrols should be able to drive onto school grounds and around school buildings. If the school grounds are completely surrounded by a fence and locked gate, police patrols should be able to view all sides of the school building.

11.4.2 Theft and Embezzlement Prevention. Schools are at risk of theft and embezzlement losses. Such losses can range from theft of cash, to misappropriation of funds, to collusion with suppliers and vendors. The first line of defense against employee theft is to have honest employees and volunteers. This is best accomplished through a program of personnel screening. By performing in-depth checks of job histories and references, an environment of honesty can be created. A thorough screening process for all personnel, including employees and volunteers, will convey to all the commitment of the organization to having the highest level of integrity.

11.4.2.1 Consideration should be given to implementing procedures to limit the opportunity for embezzlement. Responsibilities and functions should be divided so that no one person has control over all facets of a transaction. For example, the person who makes the bank deposits should not be responsible for reconciling the bank statement, and the person who orders supplies should not be responsible for paying invoices.

11.4.2.2 School supplies and valuable equipment, such as cameras and laptop computers, should be kept in locked closets or cabinets to limit the opportunity for theft. An inventory system should be established to account for supplies and equipment. Equipment should have a permanent identifying mark or stamp that shows ownership. The model and serial number of all equipment should be recorded and stored in a secure location.

11.4.2.3 Cash should be kept in the lowest possible amount by making regular bank deposits. The times and routes of bank deposits should be varied to reduce the risk of robbery. Extra cash should be kept locked in a safe; depending on the amount of cash on hand, a burglary-resistant safe might be advisable.

11.4.2.4 Lockers should be provided for teachers and students to store personal possessions. Teachers' lockers should be in a separate room, preferably a faculty room that is always under lock and key.

11.4.2.5 Procedures should also be in place to prevent losses from check fraud. Checks received in payment of tuition or for other reasons should be stamped "For deposit only" upon receipt. Check books should not be left unattended but kept in a locked drawer or closet. Bank statements should be reviewed regularly. The authorized signers of checks should not be the same people who reconcile the accounts.

11.4.3 Burglary Prevention. Burglary is a crime of opportunity. Research into the crime indicates that burglars look for places that offer the best opportunity for success. In choosing targets, burglars look for locations that contain something worth stealing and then select those that look easy to break into. Burglars appear to be strongly influenced by the look and feel of the business they are planning to burglarize. Consequently, if the exterior of the building appears to reflect attention to security, the burglar will be more likely to look for an easier opportunity. Good locks and ironwork contribute to making a building appear secure.

11.4.3.1 The primary method of preventing burglary is to design buildings that are difficult to burglarize. The physical design of buildings, such as features that allow for increased visibility of intruders, plays an important role in deterring vandalism. Inadequate lighting and places of concealment, such as dense shrubbery, create opportunities for burglary.

11.4.3.2 Many of the methods outlined for vandalism prevention are also effective in preventing burglary. These include exterior doors of solid construction that are provided with high-security locking hardware; glass panels and sidelights in exterior doors protected with wire mesh screens; if not in conflict with life-safety code requirements, ground floor windows protected with wire mesh screening or the glazing replaced with burglary-resistant glazing materials; and roof hatches and other openings into the building, such as air vents, protected to prevent illegal entry.

11.4.3.3 An intrusion detection system also can deter a burglar. An alarm system that sends a signal to a monitoring station, which dispatches guards on receipt of the signal, is preferred. An alarm system that sounds a local bell is better than no alarm at all — at the very least, it can scare off the burglar. If a safe or security closet is used to protect property, it should also be protected by the alarm system. The alarm system should be regularly tested and properly maintained.

11.4.3.4 To limit the opportunity for burglary, classrooms in which there is a high inventory of expensive equipment, such as computer labs, should be provided with extra security. This includes providing secure doors, high-security locking devices, protection for exterior windows, and alarm system protection. During periods when the school is closed, such as summer recess, consideration should be given to placing this equipment, as well as other high-value items, in a security closet or similar structure that is protected by the alarm system.

11.4.3.5 Security guards are also effective as deterrents to burglary. To be most effective, guards should patrol the facility. If the janitorial staff is expected to provide a security function, training should be provided on the school's security procedures.

11.5 Colleges and Universities.

11.5.1 Legislation.

11.5.1.1 The federal Crime Awareness and Campus Security Act of 1990 (hereinafter referred to as the Act) was enacted. The specific statue can be found in 20 USC 1092, Higher Education Resources and Student Assistance; Subchapter IV – Student Assistance; Section 1090. See Section 1090(a) for Information Dissemination Activities and Section 1090(f) for Campus Security Policy and Campus Crime Statistics.

11.5.1.2 The Act is intended to increase the awareness of students, parents, and college and university administrators of the risk of crime on campuses and the need for the development of an effective campus security program to deal with crime. The legislation requires institutions of higher education to collect statistics on campus crime and furnish such information to current and prospective students. Colleges and universities also must publish this information, along with a description of campus security policies and programs, in an annual report. While the Act requires colleges to develop and implement campus security policies, it offers no specific guidelines on what constitutes a campus security program.

11.5.1.3 On October 7, 1998, the Higher Education Amendments of 1998 Act was signed into law. The new law expanded the disclosure of campus crime statistics and required many colleges and universities to keep a public crime log for the first time. These amendments marked the first major revisions to the Act and included amendments to formally rename it the Jeanne Cleary Disclosure of Campus Security Policy and Campus Crime Statistics Act (Jeanne Cleary Act). To comply with the new law, the Department of Education has published new standards, which became effective July 1, 2000, for reporting campus crime.

11.5.1.4 The U.S. Department of Education November 1, 1999, Final Regulations govern consumer disclosure requirements for institutions participating in the federal student financial assistance program.

11.5.2 Requirements of the Act.

11.5.2.1 To comply with the Act, colleges and universities are required to prepare an annual report containing specific information with respect to the campus security policies and campus crime statistics of that institution. Information required in the annual report includes the following:

(1) A statement of current campus policies regarding procedures and facilities for students and others to report criminal actions or other emergencies occurring on campus and policies concerning the institution's response to such reports
(2) A statement of current policies concerning security and access to campus facilities, including student residences, and security considerations used in the maintenance of campus facilities
(3) A statement of current policies concerning campus law enforcement, including the enforcement authority of security personnel and their working relationship with state and local police agencies

11.5.2.2 Policies that encourage accurate and prompt reporting of all crimes to the campus police and appropriate police agencies include the following:

(1) A description of the type and frequency of programs designed to inform students and employees about campus security procedures and practices and to encourage students and employees to be responsible for their own security and the security of others
(2) A description of the programs designed to inform students and employees about the prevention of crimes
(3) Statistics concerning the occurrences on campus during the most recent school year and during the two preceding school years for which data are available, of the following criminal offenses reported to campus security authorities or local police agencies: murder, rape, robbery, aggravated assault, burglary, and motor vehicle theft
(4) A statement of policy concerning the monitoring and recording, through local police agencies, of criminal activity at off-campus student organizations that are recognized by the institution and that are engaged in by students attending the institution, including those student organizations with off-campus housing facilities
(5) Statistics for the number of arrests for the following crimes occurring on campus: liquor law violations, drug abuse violations, and weapons possession
(6) A statement or policy regarding the possession, use, and sale of alcoholic beverages and enforcement of state underage drinking laws; a statement of policy regarding the possession, use, and sale of illegal drugs and enforcement of federal and state drug laws; and a description of any drug or alcohol abuse prevention programs

11.5.3 Amendments to the Act. The changes implemented by the Jeanne Cleary Act regarding the disclosure of campus security information, include the following:

(1) Defining terms, such as *campus*, *noncampus buildings or property*, and *public property*

(2) Excluding pastoral or professional counselors from the definition of a campus security authority
(3) Adding new categories of crimes to be reported and new policies to be disclosed
(4) Clarifying how to compile and depict crime statistics by changing the date for disclosure of the annual security report to October 1
(5) Requiring certain institutions to maintain a publicly available crime log
(6) Requiring institutions annually to submit their crime statistics to the Department of Education

11.5.4 Elements of a Campus Security Program. The goal of a campus security program is to provide students and employees with an atmosphere free from fear of personal harm or property loss. To accomplish this goal and to comply with the requirements of the Act, a campus security program should have the following components:

(1) Record-keeping system
(2) Communication system
(3) Training program
(4) Campus law enforcement
(5) Security surveys
(6) Access control system
(7) Security for campus housing
(8) Security for research facilities
(9) Security equipment

11.6 Record-Keeping System.

11.6.1 A record-keeping system should be established that tracks all criminal and violent acts on campus, in the immediate surrounding area of the campus, and at off-campus student organizations that are recognized by the institution. The Act requires that these statistics be maintained and made available to students, parents, faculty, and staff. Analysis of the statistics on a regular basis helps to determine crime trends and the effectiveness of loss prevention measures.

11.6.2 Computer programs are available that can analyze the crime data and generate useful information on trends. A system of tracking crimes with colored pins on a map of the campus grounds provides a visible profile of crime trends that can be of significant value in allocating resources for security patrols.

11.6.3 The record-keeping system should also keep track of arrests on campus for liquor law and drug abuse violations and weapons possession. This information can be obtained from local police agencies.

11.7 Communication System.

11.7.1 An important tool for communicating with the student body is the student handbook. The handbook can provide important information on safety and crime prevention tips. It can also be used to provide information on campus security procedures and policies and instructions on how to report suspicious or criminal activity on campus to the proper authorities.

11.7.2 The Act requires colleges to publish crime statistics on a yearly basis. However, to keep the campus community better informed, some colleges take a more proactive approach by publishing the statistics on a monthly basis. Campus publications, such as the student newspaper and newsletters, campus email systems, and crime prevention bulletins, can be used to provide the information.

11.7.3 Communication should also be established with local police agencies. Police familiarity with campus layout allows for timely response in the event of an emergency on campus. Local police agencies can also be a valuable resource in providing safety and crime prevention training programs for the student body.

11.8 Training.

11.8.1 The Act requires not only that students be informed of crime trends but that they be made more aware of the importance of security and be educated on how their campus security program works. The student handbook can be used to provide this information. The student newspaper and campus newsletters can be used to provide updates about the security program.

11.8.2 A crime prevention training program for students should focus on promoting campus security as a shared responsibility among students, staff, and campus law enforcement. Specifically, it should include information on how to report crimes, security for residence halls, entrances and dormitory doors, and common-sense safety and crime prevention tips.

11.9 Campus Law Enforcement.

11.9.1 At most colleges and universities, it is the public safety department that is charged with the administration of the campus security program, including managing campus security personnel. This department can also have responsibility for investigating crimes, as well as instances of employee misconduct, theft of college property, and threats against persons.

11.9.2 Campus security personnel can range from contract or proprietary security personnel, with basically civilian status, to peace officers, with greater arrest powers than civilians but not the sweeping arrest powers of the police. In some jurisdictions, campus security officers have full police authority.

11.9.3 Security personnel should have levels of education, work experience, and training in line with their level of responsibility. Security personnel should also go through a thorough background investigation and criminal history check. They should also be required to take psychological examinations and be screened for illegal drug use.

11.9.4 Training should be commensurate with job responsibilities and should meet requirements of applicable state laws. Almost all states have regulations governing screening or training of security officers.

11.9.5 A campus security department is usually staffed with at least one administrator, a number of supervisors, one or more investigators, and possibly a crime prevention specialist, and the remainder of the force is in patrol operations.

11.9.6 The crime prevention specialist is responsible for coordinating crime prevention programs, developing printed crime prevention material, giving speeches or lectures at campus crime prevention training programs, conducting security surveys, and analyzing crime statistics.

11.9.7 A major function of the security force is patrolling the campus. Security patrols should focus on the prevention of crimes and the elimination or reduction of criminal opportunities, rather than the traditional police model of reacting to crime. To that end, security officers should be schooled in the principles of crime prevention and trained in the techniques of preventive patrols.

11.10 Security Surveys.

11.10.1 The physical environment of the campus should be surveyed. The survey should attempt to determine the following:

(1) Is perimeter fencing needed to limit access from other properties?
(2) Is foliage and shrubbery kept trimmed to eliminate hiding spaces for criminals and provide for natural surveillance of the property?
(3) Do design features of buildings create hiding spaces for criminals? If so, should they be fenced off or otherwise secured?

11.10.2 The survey should also look for signs of vagrants living on or around the property and signs of vandalism or graffiti on buildings, since these can be indications of future, more serious problems.

11.10.3 Security lighting can serve as a deterrent to crime. The security lighting should illuminate walkways, building entrances, and vehicular entrances and provide minimum illumination levels in accordance with the IESNA *Lighting Handbook*. The lighting system should be inspected regularly and broken or inoperative fixtures repaired as soon as possible. Lighting surveys should be performed on a regular basis to check illumination levels.

11.11 Access Control. While a campus can be viewed as an open environment where students, guests, and staff can roam freely, an access control program should be implemented to permit authorized individuals to come and go with ease, while restricting access to unauthorized individuals. The degree of access control should be a function of the campus layout. If perimeter access control cannot be readily provided because of the size or layout of the facility, at the very least, a system should be implemented to limit access into buildings. The access control system should be designed to meet life safety and fire code regulations, as well as the Americans with Disabilities Act's requirements on accessibility for the disabled.

11.12 Key Control.

11.12.1 Prior to making any changes to a key or lock system, a study should be made to determine whether it would be cost effective to convert the system to a computer-controlled access control system, as discussed in Section 11.13. These systems offer many advantages over the conventional key and lock system.

11.12.2 A key control program should ensure that all campus keys are accounted for. If the locking system has been in place for a long time and all keys cannot be accounted for, the most effective way to gain control of the keys is to rekey the existing locks. The lock cores should be rotated when possible or changed to a new system.

11.12.3 A number of factors should be considered in selecting a new key system. The system should have restrictive key blanks that are not readily available to locksmiths, thus ensuring that keys are not easily duplicated. The key system also should be compatible with the existing campus locks so that new locks will not have to be purchased.

11.12.4 Once all the keys are accounted for, a database to track all door locks, keys, and keyholders should be established. Keys should be issued on a "need for" basis, rather than as a convenience. A computer is recommended for this record keeping. A secure key storage cabinet should be used to store duplicate keys.

11.12.5 To maintain the integrity of the key control program, policies should be established regarding who has access to rooms, who has authority to grant access to a particular area, and who is responsible for issuing keys. Also, only authorized locksmiths should be permitted to change or repair locks.

11.13 Access Control Systems.

11.13.1 As a result of increased security awareness on campuses, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. One major advantage of access control systems is the ease with which codes can be changed to delete lost or stolen identification credentials from the system.

11.13.2 Access control systems can range from basic systems that operate a single lock on a door to computer-operated systems that electronically tie together hundreds of locks. In these systems, an identification credential serves as a key to operate the lock on a door. The same principles of key control apply to the issuance of identification credentials.

11.13.3 Newer technologies are available with cards that can perform a variety of functions. In addition to being a photo ID and an access card, the card can function as a library card, debit card, meal-plan card, and long-distance telephone card.

11.14 Security for Campus Housing. Colleges and universities that provide housing for students assume a greater responsibility to provide for their safety and security. A security program for residence halls should include the following considerations:

(1) Training students regarding their security responsibilities and role in maintaining the integrity of the security program
(2) Requiring that the doors to residence halls be locked at all times
(3) Limiting access to residence halls at night through only one door (without conflicting with life safety code requirements)
(4) Requiring that one key or access card be used to gain entrance into the residence hall and another key or access card into student rooms
(5) Changing locks or access codes to student rooms whenever a key or access card is lost
(6) Having security patrols check that accessible doors and windows are locked at night
(7) Having programs to address the propping open of doors by students for convenience (e.g., self-closers on doors and local alarms that sound when doors are left propped open)
(8) Providing an intercom system at the main entrance for visitors to call residents
(9) Requiring that visitors and delivery persons be supervised at all times in residence halls
(10) Having special security procedures for housing students during low-occupancy periods, such as holidays and vacation periods

11.15 Security for College Research Laboratories. Since the events of September 11, 2001, government and university officials have strongly recommended that college research laboratories tighten security. In particular, special attention should be paid to security for all college research laboratories that handle any materials that could be used for chemical or biological weapons. Additionally, research with commercial potential should benefit from the same level of security that private industry would utilize to protect valued intellectual property. A security program for college research laboratories should include the following considerations:

(1) Training faculty and students in the proper handling and security of sensitive materials

(2) Fostering a security culture with respect to laboratories and sensitive materials
(3) Controlling access to laboratories and material storage areas to essential personnel
(4) Establishing effective inventory control and handling processes
(5) Providing facilities to secure sensitive materials
(6) Electronic monitoring of laboratories and storage areas of sensitive materials
(7) Increased or dedicated security patrols of research areas
(8) Providing reliable means for laboratory occupants to alert security personnel of off-normal events such as an accidental material release, materials theft, and intrusion/duress situation

11.16 Security Equipment.

11.16.1 Integration of security equipment with fire alarm and building management equipment provides for centralized control of these functions and savings in personnel and equipment costs. Security equipment used on campuses includes closed-circuit television systems (video surveillance) and intrusion alarms.

11.16.2 Video surveillance systems are widely used on college and university campuses as a means of providing safety and security for students and staff. They can be used at entrances to residence halls to identify visitors requesting entry, in parking lots to monitor potential criminal activity, and on campus grounds for surveillance purposes and as a deterrent to crime.

11.16.3 The video surveillance system should be connected to a video recorder to provide a record of events. Recorded tapes can be studied to determine access control and traffic patterns and reviewed for evidence of a crime.

11.16.4 Intrusion alarms should be used in areas where access is not permitted at certain times and where a quick response to an intrusion is desired. They can be tied into a video surveillance system so that on activation of an alarm, a recording is made of the scene.

11.17* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors or contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Chapter 12 Health Care Facilities

12.1 General. A health care facility, for the purpose of this chapter, is a facility used for medical service or other treatment to four or more persons simultaneously where one of the following conditions applies:

(1) The occupants are mostly incapable of self-preservation due to age or physical or mental disability or because of security measures not under the occupants' control.
(2) On an outpatient basis, treatment is provided that renders the patients incapable of taking action for self-preservation under emergency conditions without the assistance of others.
(3) On an outpatient basis, anesthesia is provided that renders the patients incapable of taking action for self-preservation under emergency conditions without the assistance of others.

12.2 Application. This chapter addresses measures to control security vulnerabilities in health care facilities.

12.3* Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as described in Chapter 5, should be conducted. The SVA should take into consideration the factors listed in A.12.3.

12.4 Security Policies and Procedures. The elements of a security program for a health care facility should include the following:

(1) Employee involvement
(2) Training
(3) Employment practices
(4) Security measures

12.4.1 Employee Involvement. For a security program to be effective, it should have the full support of management. Management also should encourage employees to become involved in the decision-making process that shapes the security program. Methods of obtaining this involvement should include the following:

(1) Employee participation in developing a written security program that is communicated to all employees (the program should be endorsed by the management of the institution)
(2) An employee suggestion/complaint procedure that allows workers to take their concerns to management and receive feedback without fear of reprisal
(3) A procedure that requires prompt and accurate reporting of all incidents regardless of the seriousness of the injury
(4) Employee participation in the analysis of the security reports and in the making of recommendations for corrections
(5) Employee participation in identifying problem patients who can be prone to violence and methods to handle such patients
(6) Employee participation in emergency teams that are trained in responding to violent incidents
(7) Employee participation in training and refresher courses

12.4.2 Training. Employee training should be a critical element of any security program.

(A) All employees should be trained prior to job placement, and the training should be periodically updated. The training program should include the location and use of alarm systems and other protection devices, methods of de-escalating aggressive behavior, use of a buddy system, policies and procedures for reporting incidents and obtaining medical care and counseling, and the rights of employees versus patient rights.

(B) Supervisors and managers should be responsible for ensuring that workers are not placed in assignments that compromise safety and that workers feel comfortable in expressing their concerns and reporting incidents. They should ensure that employees follow safe work practices and receive appropriate training to enable them to do so. Supervisors and managers should undergo training that will enable them to recognize potentially hazardous

situations and to make changes in the physical plant, patient care, treatment program, staffing policy and procedures, or other such situations that are contributing to the hazardous condition.

12.4.3* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors or other personnel) are used, management should ask the vendors or contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

12.4.4* Security Measures. A security program for a health care facility should be designed to protect both its tangible assets, such as its workers and property, and its intangible assets, such as its reputation and good will.

12.4.4.1* Protection for exterior areas includes measures described in 12.4.4.1(A) through 12.4.4.1(C).

(A) Fencing the entire perimeter, including parking lots, can discourage unauthorized access to the facility and deter the opportunistic criminal.

(B) Shrubbery should be kept trimmed to provide for adequate surveillance of the property.

(C) After hours, the number of access routes onto the property should be limited. Visitors (and workers) should be channeled away from isolated areas and into areas that are under surveillance.

12.4.4.2 Protection for parking facilities should include measures described in 12.4.4.2(A) through 12.4.4.2(D).

(A) Entrances and exits to the parking facility should be as few in number as practicable. The preferred method of controlling access to the facility should be to have one means of entry and exit for vehicles; the volume of traffic at the facility, however, can require more than one entry and exit for vehicle parking.

(B) For parking garages, the ground floor and, if easily accessible, the second level of the structure should be completely enclosed. Sturdy screening that reaches from floor to ceiling is preferred to solid walls, since screening provides for visibility into the structure from the street, which can serve as a deterrent to criminal activity. All exterior doors should be securely locked in compliance with the requirements of local building, fire prevention, and life safety codes.

(C)* Illumination levels for parking facilities should be as recommended in the IESNA *Lighting Handbook*.

(D) Arrangements should be made to provide close-in parking for workers on night shifts, for those who will be coming or leaving during nighttime hours, and for those on call. Alternatively, escort services should be provided.

12.4.4.3 Building access control measures should include those described in 12.4.4.3(A) through 12.4.4.3(F).

(A) Consideration should be given to establishing a program to control access by personnel, vendors, and visitors.

(B) Identification cards should be issued to all employees, physicians, volunteers, students, and contract staff according to the hospital's SVA. The cards should have, as a minimum, a photograph of the bearer, at least the bearer's first name, and the bearer's position title. Employees should be required to display their identification cards at all times.

(C) Visitors should not be able to access patient areas without passing the reception area. Facilities should consider the use of visitor logs or badges.

(D) A policy should be established regarding the protection of patient information as required by the Health Insurance Portability and Accountability Act (HIPAA).

(E) Access to uniforms, such as for maintenance workers, and, if possible, patients' gowns and doctors' scrubs should be controlled. When intruders are able to obtain such garments, they are able to blend in with health care staff.

(F) A messenger center for packages, flowers, and other deliveries should be established. Messengers should not be allowed to roam the building freely.

12.4.4.4 Interior areas should be protected by measures described in 12.4.4.4(A) through 12.4.4.4(D).

(A)* Access to maternity/labor and delivery/nursery/pediatric areas should be strictly controlled.

(B) In emergency rooms, administrators should consider using various security measures intended to reduce the risk of violence, including constant security staffing, the use of security equipment (metal detectors, video surveillance, and alarm systems), and the training of emergency room staff in management of aggressive behavior.

(C) State and federal laws require health care facilities to provide for the safe storage and distribution of controlled substances.

(D) Storage areas and other areas that are not used regularly for patient care should be kept locked at all times.

12.4.4.5 Security equipment includes those described in 12.4.4.5(A) through 12.4.4.5(G).

(A) A video surveillance system, if used, should cover entrances, exits, entrance ramps, elevators, stairwells, walkways, and parking areas of the premises.

(B) Signs stating that the area is under video surveillance should be installed to serve as deterrence to crime.

(C) Recording equipment should be installed in a secure and protected part of the premises and should be under the control of authorized personnel.

(D) Emergency exits should be alarmed and monitored to detect unauthorized usage.

(E) Burglar alarm, fire alarm, and video surveillance systems should be monitored at a central security console that is constantly staffed.

(F) Duress alarm devices should be installed at strategic locations as needed, such as emergency rooms, triage stations, reception areas, registration desks, and other areas.

(G) All security systems should be tested and maintained as deemed appropriate by the hospital's SVA.

12.4.4.6 Security personnel should be screened, trained, and deployed according to the guidelines of 12.4.4.6(A) through 12.4.4.6(D).

(A) Security personnel should be thoroughly screened before being hired. The screening should include psychological testing and evaluation to ensure that personnel are emotionally suited to perform in a health care setting.

(B) After being hired, security personnel should be trained in the routine details of their assigned posts, the policies, procedures, and philosophy of health care departments, and especially in methods of nonviolent crisis intervention.

(C)* These patrols should be monitored by a watchclock service, with records maintained.

(D)* If weapons are used by security staff, special training should be required to prevent inappropriate use of the weapon and the creation of additional hazards.

12.4.4.7 Employers should provide a training program on personal safety for home health care workers. This program should, at the minimum, be provided by local police departments or other agencies and should include training on awareness, avoidance, and action to take to prevent mugging, robbery, rapes, and other assaults.

(A) To provide some measure of safety and to keep the employee in contact with headquarters or a source of assistance, cellular phones should be provided for official use when staff are assigned duties that take them into private homes and the community. Handheld alarms, noise devices, or beepers that alert a central office of problems should be investigated and provided where deemed necessary.

(B) Employees should be instructed not to enter any location where they feel threatened or unsafe. This decision should be the judgment of the employees. Procedures should be developed to assist employees to evaluate the relative hazard in a given situation. In hazardous cases, the managers should facilitate and establish a "buddy system." This buddy system should be required whenever an employee feels insecure regarding the time of activity, the location of work, the nature of the client's health problem, or a history of aggressive or assaultive behavior or potential for aggressive acts.

(C) Police assistance and escorts should be required in dangerous or hostile situations or at night. Procedures for evaluating and arranging for such police accompaniment should be developed and training provided.

Chapter 13 One- and Two-Family Dwellings

13.1 General. One- and two-family dwellings, for the purpose of this chapter, are residential facilities containing one or two dwelling units, where dwellings are primarily occupied on a permanent basis.

13.2 Application. This chapter addresses measures to control security vulnerabilities in one- and two-family dwellings.

13.3 Security Policies and Procedures. There are various procedural and physical security measures that can be implemented to help protect a one- and two-family dwelling from the crime of burglary. Most of these procedural measures can be considered minimum recommendations implemented with relative ease. Other precautions involve physical enhancements that will structurally strengthen the perimeter openings. If these precautions and enhancements do not provide a sufficient level of security, then detection devices and advanced physical hardware should be considered.

13.4 Special Considerations. The characteristics of a residence can make the residence enticing to an intruder. When determining the level of security appropriate for the residence, the following should be taken into consideration:

(1) Type of residence
(2) Demographics
(3) Lighting
(4) Pedestrian and vehicular traffic
(5) Activity in the area

13.4.1 Basic and Environmental Precautions. A few simple precautions can effectively reduce the possibility of crime by reducing the perception of opportunity. The following recommendations are simple procedures that can be implemented with a minimal amount of effort. After reducing the perception of opportunity, the guide offers recommendations to deter the commission of the crime or to minimize its impact or loss. Most burglars devote little time to planning a residential break-in. Taking basic precautions can prevent the home from being perceived as an easy target and can potentially deter the intruder away to an easier target. The more of the following precautions that are taken, the safer the residence:

(1) In the event you arrive home and believe someone has entered your residence, immediately notify the police. Do not enter the home or disturb any potential evidence.
(2) Whenever the house is to be unoccupied, day or night, lock all doors and windows, keep a radio playing loud enough so that it can be heard just outside the door, and leave a light burning at night, preferably on a timer that turns it on and off automatically at random times.
(3) Do not leave notes or messages on answering machines or voice mails indicating you are away.
(4) Do not discuss your vacation plans (or business trips) with anyone but family and trusted neighbors.
(5) Provide a trusted neighbor with a phone number and an address (if available) where you can be reached in the event of an emergency.
(6) If you will be away for an extended period, advise the police of the duration of your absence and contact information. Make arrangements to have the lawn mowed when necessary, snow shoveled in winter, and other routine maintenance jobs performed. Give the house a lived-in look. Leave shades and blinds in a partially opened position. Use timers that will activate lights at irregular time intervals to give the appearance that the house is occupied.
(7) Do not allow strangers in your home even to use the telephone. If requested, have the person remain outside while the police are called.
(8) When on vacation or a long weekend trip, do not stop delivery of newspapers and mail — this only announces to others that you are away. Ask a neighbor to pick them up.
(9) Be extra vigilant when leaving home to attend weddings or funerals. Burglars have been known to read marriage and funeral notices to determine when a family will be away from home.
(10) Keep doors to enclosed porches and entryways securely locked at all times. A door or window within an enclosed porch or entryway is a preferred point of illegal access since it affords the burglar an opportunity to work without fear of being seen by neighbors. Do not rely on screen doors to provide a dependable level of security unless the door is a decorative steel security door with a heavy duty security lock.

(11) Never leave the garage door open, even if you will be away for only a short while. An open garage serves as an indicator that a house might be unoccupied and provides a burglar with the opportunity to work undetected. Also, an open garage can provide a burglar with a ladder for entry through a second-story window or with the tools for prying open a door.
(12) Do not have identification tags with your name and address on house key rings. In the event the keys are lost or stolen, a burglar would have easy access to your home.
(13) When moving into a residence with a radio-operated garage door opener, or if installing a new unit (manufacturers factory-set all devices to the same code), change the signal code for the device as soon as possible. Consult the installation or user manual for changing digital codes.
(14) The exterior lock or keypad for opening an electric garage door should be protected to prevent a would-be burglar from removing the lock or keypad and compromising the wiring, resulting in the door opening. Mounting hardware for the lock or keypad should not be easily removable from the outside. Devices should be mounted whenever possible using thru-bolts to reduce the possibility of the device being removed, disconnected, or tampered with.
(15) Make the job of the burglar as difficult as possible in the event that entry is accomplished. Conceal valuables. Do not leave jewelry on bureaus or money in dresser drawers. The master bedroom is typically the first room a burglar will head for.
(16) Request a residential crime prevention survey from your police department. Most police departments have crime prevention units that will inspect a home and make security recommendations.
(17) If you consent to a telephone survey, do not answer personal questions and do not tell anyone you are alone.
(18) Do not list marital status or first name on mailboxes or telephone listings.
(19) Remove names from the exterior of the house. The name on a door plaque or mail box can be used to obtain the telephone number. If a burglar feels the house is unoccupied, a simple call from a cell phone can be used to confirm that. An unlisted phone number will also help to increase your security.
(20) Install house numbers on mailboxes or in a location that is readily observable by emergency responders. Reflective decals should be used and should be a minimum of 4 in. (101.6 mm) high.
(21) Do not leave keys or combinations hidden outside the home. Burglars have an uncanny ability to find hiding spots. The best place to hide a key is in the hands of a trusted neighbor.
(22) Display decals or signs indicating that your home is protected by a burglar alarm system, whether or not you have one. Studies have shown that burglars are deterred if they think a house might have an alarm system.
(23) If a visit by service personnel is unexpected, ask for identification and verify it with their employers before allowing them in.
(24) Inventory all valuable items using a camera. Take pictures of the valuables, recording pertinent information on the reverse side. Information such as make and model, distinguishing marks, serial numbers, price, and date of purchase all become very important in the event the item is stolen and the information is required for a police investigation or an insurance claim. Keep the information in a safe, secure place, preferably outside the home. A bank safe deposit box is an excellent storage place.
(25) Join a Neighborhood Watch Program. Be your neighbor's keeper — report all suspicious persons, automobiles, and service trucks to the police immediately.
(26) Participate in Operation Identification, which involves marking all valuables with an identification number. In this way, recovered items can be returned to you. Display an Operation Identification decal indicating that all items of value have been marked. The inscribing tools often can be borrowed, free of charge, from sponsoring local police departments. Consider engraving the item with a driver's license number. Consult with local police for their recommendations.
(27) Do not display valuables in plain view of a window.
(28) Since burglars tend to avoid situations that create noise, dogs that bark when someone approaches the home can be effective deterrents to burglary. This is especially true of amateur thieves, who account for the majority of residential burglaries.
(29) Keep shrubbery trimmed as neatly as possible to enhance the visibility of openings. Neatly trimmed, low-cut shrubbery and bushes will provide maximum visibility for neighbors and passing police and will reduce the concealment opportunities for intruders.

13.4.2 Physical Enhancements. After implementing the recommended basic precautions in 13.4.1, the next logical step is to secure and fortify the perimeter with security devices. This subsection makes recommendations as to methods and procedures that can enhance the physical security of the residence. See Chapter 7 for additional information on doors, locks, and windows.

13.4.2.1 Types of Deadbolts. Locks can be of the single-cylinder or double-cylinder type.

(A) Single-cylinder deadbolts have a thumb turn on the interior side They are convenient to use and provide good security. The single-cylinder deadbolt also provides minimal delay for evacuation in the event of a fire.

(B) Double-cylinder deadbolts require a key to unlock them from either side. They provide additional security, particularly when there are glass panels in the vicinity of the lock. They reduce an intruder's ability to remove property from your home. Before installing double-cylinder deadbolts, consult the local fire department for their recommendation. A double-sided lock can delay egress from the residence during a fire. The replacement of glass panels with listed burglary-resistant glazing near the deadbolt can minimize the need for double-cylinder deadbolts.

13.4.2.2 Doors.

(A) Exterior doors should be of a solid-core design or steel construction with hinges on the interior of the door and a keyed lock with a strike bolt into a solid frame.

(B) All doors should be secured with a locking mechanism. Consideration should be given to the structure of the opening and the ability to provide a secure locking device.

(C) The following security measures are designed specifically to increase the resistance of doors to illegal entry:

(1) Assuming exterior doors are of solid construction, equip them with good deadbolts meeting the requirements of ANSI/BHMAA156.5. To resist attempts at spreading the door frame to bypass the lock (called *jimmying*) to open a door, install locks that have a bolt with at least a 1 in.

(25.4 mm) throw. A vertical deadbolt that secures the door to the door frame is particularly effective against jimmying attempts.

(2) Be sure exterior doors fit tightly in the frame with no more than ⅛ in. (3.2 mm) clearance between the door and frame. If the gap is too large, replace the door or a sturdy metal strip to the door edge to cover the gap. Locks should have a minimum of a 1 in. bolt, which will prevent the door from being pried open or being pushed back with a thin instrument.

(3) To provide protection to the lock cylinder, install a cylinder guard plate or a cylinder guard ring.

(4) Protect the hinged side on outward swinging doors by installing projecting pins in the hinged edge of the door that fit snugly into sockets in the door jamb when the door is closed. This will prevent attempts to open the door on the hinged side by removal of the hinge pin or by cutting off the hinge knuckle.

(5) If an exterior door has a glass panel within 40 in. (101.6 cm) of the lock, replace the glass with listed burglary-resisting glazing material, such as polycarbonate glazing. Alternatively, listed burglary/impact-resistant film can be attached to the inside of the door behind the glass to provide backup protection, or the glass panel can be protected with a metal security screen. This will help prevent a burglar from breaking the glass and reaching in to unlock the door.

(6) Protection for glass panels or inserts along with side panels should be addressed when determining the appropriate locking mechanism. Glass panels can easily be broken by intruders. Consider covering the glass with a break-resistant panel, Lexan®, decorative grille, or listed impact-resistant film.

(7) Install and adjust the rollers on sliding glass patio doors so that a burglar cannot lift the doors out of their tracks and remove them. Alternatively, a projecting screw placed in the track above the door or a nail inserted through the inside frame and partway through the metal door frame will prevent the door from being lifted out of the track. The same techniques can be applied to sliding windows. Secure stationary doors with locks and long screws to avoid removal.

(8) Since the lock catch on sliding glass patio doors can usually be easily pried out of the soft aluminum door frame, place a wooden dowel or a patio door bar into the track of a sliding patio glass door. This device will positively block the travel of the sliding portion of the door even if the lock is broken, .

(9) Secure exterior doors to basements (particularly "doggie doors") on the interior with a slide bolt or on the exterior with a heavy-duty padlock that has a hardened steel hasp.

(10) Underwriters Laboratories Inc. (UL) and the Builders Hardware Manufacturers Association (BHMA) have listing programs for high-security locking cylinders and door locks.

(11) When first taking possession of a residence, rekey or change locks to ensure key control.

(12) A means to view the exterior before the door is opened.

(13) Equip solid exterior doors (without glass panels) with a wide-angled viewer to provide a 180-degree view outside the door to aid in identifying visitors before opening the door.

13.4.2.3 Garage Doors. For extended vacations, all electric garage doors should be disabled by unplugging the motor of each door. The garage door(s) can then be manually secured by installing a lock on the cross bolt that was provided when it was installed. Further enhancements can be made by drilling a hole in the end of the crossbar locking mechanism at a point past the track and securing with a pin or padlock.

13.4.2.4 Windows. Most residential burglaries originate through doors; however, if the doors provide reasonable barriers, a burglar will try the windows, which generally have inadequate locks. All windows should be secured with a locking mechanism. Check with the local fire and building departments before securing windows using means that restrict the opening. The following steps should be taken for security:

(1) If there is concern that a burglar can break the glass and reach in to unlock the window, replace or back up the glass with listed burglary-resistant glazing or listed burglary/impact-resistant film.

(2) Install burglar bars, preferably on the inside, over basement windows that are hidden and provide easy and unobtrusive access into a home.

(3) Secure air conditioners in ground-floor windows to prevent their removal.

(4) Protect windows that lead to fire escapes, or that can be used in an emergency, with a folding gate that is approved by the local fire department for such use. Contact the local fire department for the name of a manufacturer.

13.4.3 Outdoor Lighting. Exterior lighting is important in reducing crime during the evening hours. Improperly illuminated areas in the rear of a house and near entry doors are targets for prowlers. Dark areas should be well lit to avoid the perception of opportunity. Lighting should be located in places where damage or vandalism by prowlers is most difficult to notice. The following steps should be taken for security:

(1) Utilize energy-efficient outdoor lighting systems that operate on photoelectric sensors and provide dusk-to-dawn lighting.

(2) Install exterior lighting controlled by motion detectors. Photoelectric sensors should be installed to disable the lighting during the day and illuminate the area when motion is detected after dark. Detectors can be installed for lighting the front walkway and rear of the residence.

13.4.4 Intrusion Detection Systems. After implementing basic precautions and fortifying the perimeter of the residence, the next logical enhancement is to detect an intrusion or an intrusion attempt. An intrusion detection system should be installed that provides perimeter protection and interior motion detection in selected areas and signals an alarm locally or to a monitoring station. Local ordinances might require a permit.

13.4.4.1 Procedures. The intent of this subsection is to provide a warning when a security level has been breached. A procedure should be developed for addressing an alert activated by a security device. Procedures can be as simple as manually viewing the property for any sign of a crime to calling 9-1-1 and requesting police response and then securing oneself in a "safe room."

13.4.4.2 Recommendations for Selecting a Security Provider.

13.4.4.2.1 This subsection provides basic recommendations in the selection of a reputable alarm company and recommends basic concepts to be developed by a professional security designer. Before allowing a total stranger into the residence to discuss sensitive information, consumers should take the following basic precautions:

(1) Check with local police agencies for three reputable alarm companies in the area. Check with state and local consumer advocacy groups for any alarm license or business license requirements. States and municipalities that have enacted registration requirements usually have conducted background checks and require fingerprinting and photographing.
(2) Remember, you will be inviting a total stranger into your residence and revealing confidential information about your lifestyle and the location of valuables.
(3) Check references. Ask the company for a minimum of five references. Be leery of any security consultant who will not release any local references citing "client confidentiality."
(4) Verify that the company has been in business for 5 or more consecutive years and is properly licensed where required. Make sure it carries professional alarm liability insurance.
(5) Request a formal written estimate listing the make and model of all major components being installed. Request that the guarantee detail any limitations or restrictions. Request a copy of the contract with the estimate and review the fine print for any long-term commitments. Make sure that the equipment being proposed is not proprietary in design and that it can be serviced by other reputable firms.
(6) Determine whether the installation is performed by employees of the company or is subcontracted.
(7) Ask for any statistics pertaining to the number of false alarms that can be anticipated. Check with local police for the accuracy of such numbers. Police departments are now starting to track the incidence of false alarms, and some departments are making the statistics public information.

13.4.4.2.2 By following the basic recommendations in 13.4.4.2.1, consumers will have taken the steps to help ensure that a security provider is reputable and will satisfy their security needs.

13.4.4.3 Levels of Security. Levels of security are determined on an individual basis. A consultant should provide various options to determine the correct level of security for an individual's lifestyle. A basic level of security should start with security contacts on all perimeter doors. Uniform crime reports indicate that the majority of home intrusions occur through a door. Protecting the doors as a basic level of security will also ensure that the doors are closed when the system is armed. Supplemental levels of security should be addressed by the security consultant.

13.4.4.4 Guidelines for Design. Alarm system design and installation should comply with the manufacturer's specifications, applicable UL standards, NFPA standards, and industry standards and be adequate in the context of the system's environment. A testing, inspection, and maintenance program should be provided on all security systems.

13.4.4.5 Guidelines for Notification. If the security system is designed to report to a monitoring station, the consumer should consider the following:

(1) Determine the type of communication to be utilized for reporting alarm signals. There are several types of communication formats utilizing phone lines, radio waves, cellular communication services, and now the Internet. Determine the transmission time along with the limitations for each technology.
(2) Review the dispatch response programs available and determine the program suitable for the needed level of security. Decisions should be based on the response time for verification calls and dispatching as provided by the security consultant.
(3) Ask for assurances that the dispatching will be handled in a timely and accurate manner. Review all the procedures for customizing the notification process to individual needs.

13.4.5 Advanced Security Precautions.

13.4.5.1 Cash, jewelry, and other valuables should be protected by the use of a safe. A listed fire-resistant safe should protect money and important paper records from damage due to fire and provide minimal burglary protection. A listed burglary-resistant safe will protect against burglary but is ineffective against fire. A combination fire- and burglary-resistant safe can satisfy both concerns.

13.4.5.2 Additional security can be provided by fastening the safe to the structure of the residence with brackets and bolts. This technique will deter the removal of the safe or take additional time to remove.

13.4.5.3 A security closet should be used to protect firearms, silverware, cameras, and furs. The security closet can be made by installing plywood on the inside walls of a closet and using a steel door in a reinforced frame. The installation of security rooms should remain a guarded secret, revealed only to family members.

Chapter 14 Lodging Facilities

14.1 General.

14.1.1 The term *lodging facility* is an all-inclusive designation for facilities that provide housing and generally, but not always, food, beverage, meeting facilities, retail shops, recreational facilities, and other services. Hotels, motels, motor hotels, resort hotels, inns, country clubs, and conference centers are among the varieties of lodging facilities, and which term is applied is based primarily on differences in layouts and design.

(A) A hotel is a structure used primarily for the business of providing lodging facilities for the general public and that furnishes one or more customary hotel services such as a restaurant, room attendant service, bell service, telephone service, laundering of linen, and use of furniture and fixtures.

(B) A motel is a lodging facility that derives the greater part of its room business from members of the general public who are traveling by automobile and that ordinarily provides space for the parking of guests' automobiles on the premises.

14.1.2 Lodging facilities can offer a variety of services and activities for their transient and permanent guests. Generally, parking facilities are available. Some have recreational facilities, such as saunas and swimming pools, while others offer tennis and racquetball courts, gyms, and exercise rooms. In states where it is legal, gambling casinos can be on the premises.

14.1.3 The lodging facility can be a high-rise building or part of a larger, high-rise office complex. It can be a resort-type facility spread out over a campus-style setting offering skiing, golf, boating, horseback riding, and other activities. In recent years, conference centers offering multipurpose meeting facilities have become popular. Some larger lodging facilities have 5000 or more guest rooms.

14.2 Application. This chapter addresses measures to mitigate security vulnerabilities in lodging facilities.

14.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

14.4 Special Considerations. Because lodging facilities offer such a diversity of facilities, activities, and clientele, no single security program will fit all properties. The security program should be designed to fit the needs and characteristics of the individual property. While crime is not always preventable, certain policies and procedures, properly implemented, can deter or discourage criminal activity. An SVA should take into consideration the following sections for applicability to the particular lodging facility.

14.4.1 Neighborhood Crime. Management should make an effort to be informed of crime trends in and around the facility by taking the following measures:

(1) Research the history of violent and property crime in the immediate neighborhood and on the premises in the past 3 years.
(2) Develop a relationship with local law enforcement agencies to make them familiar with the property.
(3) Request that local police include the facility in their patrol routes.
(4) Maintain communication with local police to keep informed of crime and crime trends in the neighborhood or area.
(5) Participate in local security associations or industry trade groups as a means of sharing common security concerns and solutions.

14.4.2 Exterior Areas. Security is commonly enhanced by fencing, shrubbery, or other architectural barriers to deter intruders, limit access from adjacent properties, and discourage unauthorized use of the facility. The following should be considered:

(1) Perimeter fences or other barriers should be kept in good repair through regular maintenance.
(2) Foliage and shrubbery should be trimmed and maintained to allow for surveillance of the property.
(3) The lighting system should illuminate building entrances, pedestrian walkways, and vehicular entrances, as well as provide illumination as described in Chapter 6.
(4) If the exterior design of the facility creates areas of concealment, the spaces should be illuminated or secured.
(5) The exterior of the facility should be periodically checked for signs of vandalism.
(6) The facility should be periodically checked for signs of transients or vagrants living on or around the property.
(7) If exterior areas are under video surveillance, the video surveillance system should be monitored or recorded.

14.4.3 Access Control. Although open to the general public, a lodging facility is a private property. Management should monitor and, when appropriate, control the access of persons onto the premises. The following measures should be considered:

(1) Building access should be limited to authorized users only.
(2) All exterior entrances into the facility, other than the lobby entrance, should be equipped with automatic door closers and locks.
(3) A program should exist to ensure that, during nighttime hours, all remote or unattended entrances are locked. This program should not, however, conflict with fire and emergency exit requirements.
(4) Exterior hinge pins on doors should be secured against removal.
(5) All exterior entrances into the facility should be illuminated *(see Chapter 6)*.
(6) Remote or unattended exterior entrances into the facility should be monitored or recorded by a video surveillance system.

14.4.4 Parking Facilities. Users of this guide should consult Chapter 21 for information concerning parking facilities.

14.4.5 Front Desk Procedures. Front desk employees should be trained in guest privacy and applicable security practices. The following measures should be considered:

(1) Front desk personnel should not announce guest room numbers when registering guests or calling for staff.
(2) Identification should be requested of guests at check-in.
(3) The issuance of guest room keys should be controlled by front desk personnel.
(4) A history log of guestroom key distribution should be maintained.
(5) Identification should be requested for the re-issuance of room keys.
(6) Procedures should be established for releasing messages and faxes to guests.
(7) Front desk personnel should make an effort to retrieve keys from guests when they check out.
(8) A well-secured key-return box should be provided in the lobby as a reminder to, and for the convenience of, guests to return keys.
(9) Personnel should be trained in procedures to follow in handling emergencies.
(10) Personnel should be instructed to report suspicious activities to management.
(11) Electronic guest room key systems should automatically rekey each time a new guest checks into a room.
(12) Phone calls to guest rooms should be connected to the room only after the caller has identified the occupant by name.
(13) Folios, credit card numbers, and other guest information should be kept confidential.

14.4.6 Common Interior Areas. Guest rooms and guest room corridors are not considered open to the general public, and management should consider evicting persons from these areas who are not guests or invitees of guests. The normal laws of trespass apply to these areas, and local laws should be consulted. The following measures should be considered:

(1) Corridors, stairwells, and elevators should be illuminated in accordance with the IESNA *Lighting Handbook*.
(2) If stairwells and elevators have video surveillance, it should be monitored or recorded.
(3) The lobby and front desk areas should be protected by a monitored or recorded video surveillance system.
(4) Elevator cars should be equipped with means to allow someone to see inside the car before entering.
(5) Access routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should be controlled and illuminated.
(6) The doors to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should have the ability to be locked.
(7) The lights in public areas, including laundry rooms, exercise rooms, and vending areas, should be controlled by tamperproof switches.

(8) Routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should be monitored or recorded.
(9) Public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, and the routes to them should be patrolled by security personnel on a regular basis.
(10) Access to all "back of the house," nonpublic areas, including kitchens, mechanical spaces, and electrical distribution rooms, should be controlled.

14.4.7 Locks and Key Control. Properly installed locks and the control of keys are elements of any lodging facility security program. However, without proper key control, a lock will provide little deterrence to illegal or unauthorized entry. The following measures should be considered:

(1) All locking devices should be as recommended in Chapter 7 and should conform to all applicable federal, state, and local requirements.
(2) All locking devices should be properly installed and in good working order.
(3) The facility should have a key control program *(see Chapter 7)*.
(4) A log of keys issued to employees and vendors should be maintained at the facility.
(5) If the facility has a master key system, the master keys should be distributed on an as-needed basis.
(6) Extra keys, especially master keys, should be stored in a secure place and access to them controlled.
(7) Keys should be returned when employees are transferred, resign, go on vacation, or are terminated.
(8) Hotel keys should not be identified in any manner such that a person finding a lost key could trace it back to the hotel for illegal use.

14.4.8 Guest Room Security. Besides a lock and key control program, management should establish other security measures to protect guests from crime on the property and, more specifically, in guest rooms. These measures include providing information to guests on room security. The following should be considered:

(1) Guest rooms should be secured as recommended in Chapter 7 and in compliance with all applicable federal, state, and local requirements regarding window and door locks and latches.
(2) Doors should be of solid wood or steel construction.
(3) Door frames should be made of steel or otherwise reinforced with the clearance between the door and frame less than ⅛ in. (3.2 mm).
(4) Entry doors should be equipped with a deadbolt. The lock should be an American National Standard Institute Grade 1 mortise lock set with a ¾ in. (19 mm) latch and a 1 in. (2.54 cm) deadbolt and automatic retraction of the latch and bolt for life safety.
(5) Entry doors should be equipped with an auxiliary locking device, such as a safety chain or night latch, that can be opened only from the inside.
(6) Individual room rekeying should be done whenever a key is reported lost or stolen.
(7) A program should exist to ensure that keys left in rooms by guests are picked up by housekeeping personnel and returned to the front desk as soon as possible.
(8) Doors should be provided with a door viewer as recommended in Chapter 7.
(9) In guest rooms designated for the handicapped, a second door viewer should be located lower on the door in accordance with the Americans with Disabilities Act.
(10) Doors and windows that face balconies, terraces, and gardens should be secured against forced entry.
(11) All operable windows should be equipped with locking devices.
(12) Connecting-room doors should be provided with 1 in. (2.54 cm) deadbolts capable of being unlocked from inside the protected guest room side only.
(13) Guest rooms should be provided with 24-hour telephone service.
(14) Guests should be informed of the availability of safe deposit boxes.
(15) Guests should be provided with brochures or other material offering safety and security tips.

14.4.9* Employment Practices. Employers can ensure a high level of integrity in the workforce, by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references should be done on all individuals with access to critical assets, guests, or guest rooms *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

14.4.10 Security Operations. Innkeepers have been sued and found liable for negligent hiring, inadequate training, and inadequate supervision of security personnel. These considerations make it essential that companies using security personnel train them in the legal and practical applications of their employment. Because of their close contact with guests and the public, hotel security staff should receive specialized training in diplomacy. Training should be an ongoing effort in response to changing regulations and the enactment of new laws. The following measures should be considered:

(1) The facility should have a dedicated security staff.
(2) Background checks, including criminal record checks, should be done on all security personnel.
(3) If contract security personnel are used, management should request details from the contracting agencies regarding their pre-employment screening procedures.
(4) If contract security personnel are used, the contracting firm should have adequate liability insurance.
(5) Posted orders should exist for each position.
(6) Security services should be provided on a 24-hour basis or as determined by an SVA.
(7) A training program for security personnel should exist, and documentation of the training should be maintained.
(8) Security personnel should patrol the premises on a regular schedule, but not in a predetermined pattern. Patrol rounds should include exterior grounds, building perimeter, parking areas, stairwells, guest room corridors, and storage, receiving, and trash disposal areas. Every guest room should be passed to determine that doors are closed and that keys have not been accidentally left in locks or dropped on the floor.
(9) Patrols should be supervised as outlined in Chapter 9.
(10) Security personnel should be provided with portable communication equipment.

(11) Procedures should exist for informing security personnel about changes in security policies and about crime trends.
(12) Meetings between management and security personnel should be held to discuss security concerns and solutions.
(13) Security incident reports should be created at the time of the incident.
(14) Security incident reports should be retained at the facility.

14.4.11 Management Considerations. An effective security program is dependent on coordination and communication management, security personnel, and employees. The following should be considered:

(1) Policies regarding security and emergency management should exist, be tested, and be reviewed on a regular basis, and all staff should be trained in these policies.
(2) Standard written work practices regarding safety and security should be developed for all employee functions, and all staff should be trained in these practices.
(3) Management should have a system to warn guests of criminal activity in and around the facility.
(4) Sales personnel, advertising literature, promotional releases, and so forth, should make no unsupported claims about the safety or security of the facility.
(5) Photo identification cards should be issued to all employees.

Chapter 15 Apartment Buildings

15.1 General.

15.1.1 Apartment buildings generally are defined as structures containing three or more dwelling units with independent cooking and bathroom facilities. They can also be referred to as apartment houses and garden apartments.

15.1.2 Owners and managers can hire employees to carry out the maintenance duties or use the services of a building management firm. The building can be serviced by elevators and can include parking garages, laundry rooms, and recreational facilities. Some buildings have commercial or professional occupancies.

15.2 Application. This chapter addresses measures to mitigate security vulnerabilities in apartment buildings. This chapter does not cover owner-occupied residences, such as townhouses, condominiums, and cooperatives.

15.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

15.3.1 In performing an SVA of an apartment building, the following factors should be considered and reviewed for applicability:

(1) Neighborhood crime experience
(2) Public access and common areas, including courtyards, playgrounds, walkways, parking areas, street-level lobbies, elevator lobbies, stairwells, laundry facilities, storage facilities, hallways, and recreational facilities
(3) Rental units
(4) Management practices
(5) Employee safety

15.3.2 Neighborhood crime experience considerations are as follows:

(1) Location of property (i.e., urban, suburban, or rural area)
(2) The crime rate in the area
(3) Recent incidents of crime in the immediate neighborhood and on the premises
(4) Location of commercial establishments nearby that will attract shoppers and outsiders
(5) The extent of the local police presence
(6) The existence of a Neighborhood Crime Watch program

15.3.3 Public access and common area considerations are as follows:

(1) Fencing around the exterior boundary of the property
(2) Lighting systems of exterior areas and entrances *(See Chapter 6.)*
(3) Signs of vandalism on the exterior of the building
(4) Signs of homeless individuals living on or around the property
(5) Maintenance and trimming of shrubs and foliage to reduce hiding spaces
(6) Accessibility of building(s)
(7) Controlling access in the lobby
(8) Verification of visitors and service people
(9) The existence of an intercom system in the lobby; the ability of tenants to automatically buzz in callers without knowing their identity
(10) Self-closing and locking exterior and lobby doors
(11) Video surveillance at common areas and public access points
(12) Exterior hinge pins on doors secured against removal
(13) Basement doors and accessible windows protected against forced entry
(14) Access to the parking area(s) controlled *(See Chapter 21.)*
(15) Controlled access to the roof, including from a fire escape or adjoining building
(16) Illumination of corridors, stairwells, and elevators
(17) Elevator cars equipped with a means to allow someone to see inside the car before entering
(18) Illumination of access routes to common areas such as laundry rooms, exercise rooms, and storage rooms
(19) Controlled access to common areas such as laundry rooms and exercise rooms

15.3.4 Rental unit considerations are as follows:

(1) Units in general compliance with statutes regarding exterior door locks and latches
(2) Entry doors of solid-core construction and with no evidence of prior forced-entry attempts
(3) Entry doors equipped with a door viewer
(4) Hinge pins secured on doors that open outward
(5) Side lites at entrance doors protected against breakage
(6) Windows equipped with an operable latch or lock
(7) Air conditioner units in windows fastened to prevent exterior removal
(8) Bars or gates on windows that allow for exiting in an emergency
(9) Controlled access to balconies, terraces, or gardens from the street or roof, or from the roof of an adjoining property or building
(10) Doors from balconies and terraces equipped with a lock
(11) Written instructions for operating an intrusion detection system, when provided *(See* NFPA 731, *Standard for the Installation of Electronic Premises Security Systems.)*
(12) Controlled access to vacant units

15.3.5 Management considerations are as follows:

(1) Communication with the local police or local apartment owners associations
(2) Having written policies regarding tenant safety
(3) Having new tenants sign a statement attesting to the fact that they read the policies regarding tenant safety
(4) Key control program for the facility *(see Chapter 7)*
(5) Locks on doors to rental units replaced or rekeyed when there is a change in tenancy
(6) Making no unsupported claims about the safety or security by sales personnel or in leases, advertising literature, or promotional releases
(7) Investigation of tenant references and employment history
(8) Security personnel policies as recommended in Chapter 9
(9) Informing tenants of serious crimes that have occurred on the premises and in the area
(10) Maintaining records of security-related incidents and when they were acted upon
(11) Maintenance of security equipment *(See Chapters 6, 7, and 8 and* NFPA 731, *Standard for the Installation of Electronic Premises Security Systems.)*
(12) When contract personnel such as plumbers or electricians are used, asking the vendors'/contractors' management about their pre-employment screening and drug testing practices
(13) Background checks, including criminal record checks, performed on employees with access to rental units
(14) Informing tenants of changes in security measures

15.3.6 Employee safety considerations are as follows:

(1) Provide written safety procedures to all personnel.
(2) Prior to showing rental units, make a record of prospective tenants' identification.
(3) Post a "No Cash Accepted" sign in a conspicuous place to cut down on the threat of robbery.
(4) Instruct employees on safety precautions to take when showing units. (The crime prevention section of the local police department can usually provide assistance.)

15.3.7 Before undertaking an SVA, under Section 15.3, a firm is encouraged to consult with counsel to verify the extent of attorney–client privilege and work product protections that are available under applicable law to work product created in the course of the assessment.

15.4* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors' or contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Chapter 16 Restaurants

16.1 General. Restaurants, for the purposes of this chapter, include fast food restaurants, convenience stores, walk-up style facilities, and larger assembly-type facilities with full table service, lounges, and so forth.

16.2 Application. This chapter addresses measures to control security vulnerabilities in restaurant establishments.

16.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

16.4 Special Considerations. An SVA of a restaurant should review the factors in the following subsections for applicability and consideration. A security program for restaurants should be designed to control robbery and burglary, the crimes to which they are most susceptible.

16.4.1 Robbery Prevention. An establishment's hours of operation, the amount of cash on hand, and whether it provides delivery services affect its risk of robbery. In general, any business with cash on the premises is a prospective target for robbers. This is true even if the amount of cash or goods on hand is not high. Robbery prevention measures should be implemented to reduce the risk of robbery and the violence that can result from robbery. The elements of a security program to control robbery should include the following:

(1) Control of cash
(2) Access control
(3) Security equipment
(4) Personnel
(5) Employee training

16.4.1.1 Control of Cash. Businesses with large amounts of cash on hand are at greater risk to robbery. Cash in cash registers should be kept at the lowest possible level by removing extra cash and depositing it in a time-delay cash drop safe for later deposit in the bank. The times and routes of bank deposits should be varied. A sign should be posted stating that only limited cash is available, that the cash is kept in a time-delay safe, and that employees do not have access to the safe.

16.4.1.2 Access Control.

16.4.1.2.1 The entrances and the interior of the premises should be illuminated. Adequate outside lighting of the parking area and approaches during nighttime hours of operation enhances employee and customer protection. The IESNA *Lighting Handbook* provides information on lighting levels for specific areas and locations.

16.4.1.2.2 Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the premises. Clear visibility into the premises enables passersby and police patrols to observe activities inside, which can serve as a deterrent to robbery. It also enables employees to observe suspicious activities outside.

16.4.1.2.3 Many robberies occur through the back door. All rear and side doors should be locked at all times against unauthorized entry; however, this should not conflict with life safety and fire code requirements for egress.

16.4.1.2.4 Garbage areas and external walk-in freezers or refrigerators should be located to ensure the safety of employees who use them. There should be good visibility and no potential hiding places for assailants near these areas. Robberies have occurred when employees were disposing of the trash at night. Procedures, such as using two employees, should be considered to ensure employee safety.

16.4.1.3 Security Equipment.

16.4.1.3.1 Security equipment includes prominently displayed surveillance cameras, silent holdup alarm systems, and

bullet-resisting vision windows and deal trays for drive-through windows. Employees should be trained in the proper use of security equipment, especially holdup alarm systems.

16.4.1.3.2 Situations have occurred where calls have been made to place a delivery order with the intent of robbing the deliverer. To reduce the risk of robbery of delivery personnel, a telephone with a caller identification system can be used. These systems allow order takers to verify the name and telephone number from which the call is being placed. If the call is considered suspicious, the order can be refused.

16.4.1.4 Personnel at Openings and Closings. Having at least two employees on duty during high-risk hours and at opening and closing times and the use of security guards or off-duty police officers can serve as deterrents to robbery. Because of the cost involved, these actions should be considered after other robbery-prevention measures have been considered.

16.4.1.5 Employee Training.

16.4.1.5.1 Studies show that resistance to a robber's demands account for 82 percent of commercial robbery killings. Management should establish a policy of nonresistance and give it top priority in a training program. Employees should be trained on what to do before, during, and after a robbery.

16.4.1.5.2 Delivery personnel should be provided with training on how to evaluate the risks in a given situation. They should be instructed not to enter any location where they feel threatened or unsafe and to hand over all goods and cash if threatened.

16.4.2 Burglary Prevention.

16.4.2.1 Burglars often look first for easy ways to enter premises: through unlocked doors, unlatched windows, and unsecured skylights. While some burglars have the expertise to pick a lock, in most cases, entry is made using physical force by smashing doors, crowbarring doors or windows, and breaking window glass. Some burglars have resorted to breaking through building walls with sledgehammers.

16.4.2.2 The risk of burglary is also influenced by the store's hours of operation. Those that operate 24 hours a day, 7 days a week are the least vulnerable to burglary.

16.4.2.3 The elements of a security program to control burglary can include the following:

(1) Physical security devices
(2) Burglary-resistant safes
(3) Intrusion detection systems

16.4.2.3.1 Physical Security Devices. Burglary is a crime of opportunity. Research into the crime indicates that burglars look for places that offer the best opportunity for success. In choosing targets, burglars look for locations that contain something worth stealing and then select those that look easy to break into. Burglars appear to be strongly influenced by the look and feel of the business they are planning to burglarize. Consequently, if the exterior of a business appears to reflect attention to security, the burglar will likely look for an easier opportunity. Good locks, ironwork, and lighting all contribute to making a building appear secure. Goods at high risk to burglary, such as meats and alcoholic beverages, should be stored in a locked closet, security cage, or locked freezer *(see Chapter 7)*.

16.4.2.3.2 Burglary-Resistant Safes. Cash should be secured during nonbusiness hours in a burglary-resistant safe. The correct type and class of safe should be chosen for the values to be protected. Safes are either fire-resistive or burglary-resistant and are available in various protection classes (or levels). The greater the values to be protected, a correspondingly higher level of protection that should be afforded by the safe. Refer to Section 7.5 for safes and their various protection classifications to determine the appropriate safe to use. The number of people with access to a safe's combination should be kept to a minimum. The combination number should not be written in an easily accessible place, such as a desk blotter. The combination number also should be changed on a regular basis.

16.4.2.3.3 Intrusion Detection Systems.

16.4.2.3.3.1 Executing a burglary involves locating and collecting items of value. Factors that affect the time burglars will spend on the premises include the skill and confidence of the burglar(s), whether valuables are stored in a safe or vault, the quality of the protection, and the anticipated response by the police or designated personnel *(see Chapter 8)*.

16.4.2.3.3.2 An intrusion detection system can deter a burglar. An alarm system that sends a signal to a monitoring station that dispatches designated personnel on receipt of the signal is preferred. An alarm system that sounds a local bell is better than no alarm at all — at the very least, it may scare off the burglar. The safe, security closet, or security cage also should be protected by the alarm system. The alarm system should be periodically tested and maintained properly.

16.5* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Chapter 17 Shopping Centers

17.1 General. A shopping center is a group of retail and other commercial establishments that is planned, developed, and managed as a single property.

17.2 Application. This chapter addresses measures to mitigate security vulnerabilities in shopping centers. Since there are many different types of shopping centers (e.g., enclosed malls, open-air centers, neighborhood centers, and strip malls), and their location warrants different security measures, no single set of security measures can apply to all shopping centers.

17.3 Security Plan and Security Vulnerability Assessment.

17.3.1 Development. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

17.3.2 Special Considerations. The security program for a shopping center often starts at the architect's desk. Every developer and architect can consider security requirements and potential security problems when designing a new shopping center or expanding or renovating an existing facility. Crime prevention through environmental design (CPTED) concepts can be considered in the layout of the shopping center as a means to reduce or eliminate potential risks and losses to the

mall owner or operator, employees, tenants, and business invitees due to criminal activity.

17.3.2.1 For a new facility, an analysis of local crime should be considered. This information is usually available from the local police. For existing facilities, past incidents of crime and violence should be analyzed. Through the analysis, a pattern of incidents can emerge that will serve as the basis for implementing crime prevention measures, including the deployment of security personnel.

17.3.2.2 Other elements of the security program can include development of a set of policies and procedures, risk assessment, implementation of security measures, law enforcement liaison, emergency procedures, and security staffing. Because of the significant risks they pose, parking facilities should be afforded special consideration. Parking facilities are discussed in greater detail in Chapter 21 of this guide.

17.3.2.3 In performing an SVA of a shopping center, Sections 17.4 through 17.12 should be reviewed for applicability and consideration.

17.4 Security Policies and Procedures. Shopping center management should develop and implement a program of security policies and procedures. A method of communicating important information to the tenants is a suggested part of any security program.

17.4.1 Security Measures. The SVA can help determine the need for physical security measures, such as fencing, lighting, video surveillance, and access control systems, as well as security personnel.

17.4.2 Law Enforcement Liaison. Establishing and maintaining liaison with local law enforcement agencies will provide for the exchange of information concerning the level of criminal activity on the property and in the immediate neighborhood, as well as crime prevention services that are available. Establishing a positive relationship with law enforcement creates a partnership that is helpful in providing crime prevention services and information to the landlord and tenants. Information on criminal activity can be requested from local law enforcement where it is available and they have the ability to reproduce it.

17.4.3 Emergency Procedures. Emergency policies and procedures are helpful when an emergency or disaster strikes. The purpose of having written policies and procedures is to provide a plan that can be used to minimize damage to property and prevent or reduce possible injury to employees and visitors. Emergencies can be caused by natural and man-made disasters, criminal acts, and mechanical or equipment failure. The effects these emergencies can have on employees, customers, and visitors range from mild disruption to possible evacuation. Emergency procedures should be developed by utilizing information provided by government agencies, such as the Federal Emergency Management Agency (FEMA), and in cooperation with local public safety and emergency management agencies. A method of communicating important information to tenants is a part of any emergency plan.

17.5 Security Personnel. Management can regularly review its security needs and provide personnel to respond to emergencies and assist customers and employees as required. If security personnel are proprietary, management should develop a program for the selection, training, and supervision of security employees. If contract security is utilized, the security contractor is responsible for the selection, training, and supervision and for complying with all state and local laws, rules, and regulations.

17.5.1 Security Manual. Management should consider developing a security manual for the guidance of security personnel. This manual could include information regarding security authority and responsibilities, operations and emergency response procedures, facility rules and regulations, and applicable statutes and local ordinances. Security personnel should be familiar with the security manual.

17.5.2 Selection and Training. Management should consider establishing standards for the selection and training of security personnel. Some states require, as a minimum, an FBI fingerprint check of applicants. Security officers, whether proprietary or contract, should be required to complete the training required by applicable state laws.

17.5.3 Security Visibility. Management should consider having some of their security personnel visible in an effort to deter criminal activity. This deterrence can be accomplished when security personnel are on patrol.

17.5.4 Security Patrols. Management should deploy their security personnel to provide appropriate coverage of problem areas, as determined by both the security plan and local requirements. The number of security personnel on patrol can vary by time of day, day of the week, and the season of the year, depending on local security problems, peak traffic periods, and special events. An analysis of crime trends can be used to determine the most effective means of deploying security personnel.

17.5.5 Equipment.

17.5.5.1 Security personnel should carry only specifically authorized equipment. Security personnel who are permitted to carry weapons, such as batons and chemical mace, should be trained in both when and how to use them.

17.5.5.2 When any weapons are authorized, specific policies governing their use, which are consistent with applicable statutes, should be established. Firearms training should emphasize the defensive use of weapons and the responsibility inherent in carrying one. State licensing laws generally mandate training that is more extensive for armed security officers.

17.5.6 Security Communications. Management should have an appropriate communications system to respond to emergencies, including the dispatch of security personnel, if applicable.

17.5.7 Reports and Records. All crimes discovered by or reported to security personnel should be reported to the appropriate law enforcement agency. Security reports should be reviewed by management or security supervisors for accuracy and legibility and retained on file until the expiration of the appropriate statute of limitations.

17.5.8 Security Supervision. Management should provide appropriate supervision for all security functions and personnel. This can include daily inspections of all security equipment and periodic audits of all security programs. All complaints alleging misconduct by security personnel should be investigated and appropriate action taken if the allegation is sustained. The use of watch clocks, daily logs, activity reports, and spot checks by supervisors are all acceptable means of supervision.

17.6 Security for Parking Facilities. Users of this guide should consult Chapter 21 for additional information concerning parking facilities.

17.7 Perimeter Protection. Where circumstances warrant, consideration should be given to establishing perimeter security. Fencing or other physical barriers, if appropriate, at the perimeter of the protected asset can discourage unauthorized access to the protected asset and might deter the opportunistic criminal.

17.8 Landscaping. Landscaping serves the primary purpose of aesthetics but can also create security problems. For example, overgrown shrubbery can provide concealment, and trees planted too close to the fence line can serve as a means for scaling fences. Management might want to consider providing a clear zone between the tops of shrubbery and the bottom branches of the trees, for surveillance purposes.

17.9 Lighting. Lighting is basic to any security program. Local ordinances and building codes can mandate lighting requirements. The IESNA *Lighting Handbook* provides information on lighting levels for specific areas and locations.

17.10 Security Equipment. If utilized, a video surveillance system can cover all entrances, exits, entrance ramps, elevators, stairwells, walkways, and parking areas. Lighting levels might have to be increased for proper operation of the video surveillance system. Signs stating that the area is under surveillance can serve a deterrent function. Fake cameras should never be used — they give a false sense of security. Video surveillance is a tool that can be used to record historical data that can assist the police in solving crimes.

17.11 Security Patrols. Patrols, where used, should be supervised, with records maintained. Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension.

17.12 Security Reviews. Regular reviews should be performed of security procedures. In this way, management can be informed that maintenance programs are up to date, security personnel are patrolling the premises as required, and reports are being filed. The findings of the review should be adequately addressed by management. Management should also review all security-related incidents and complaints and how they were resolved.

17.13* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors or other personnel) are used, management should ask the vendors'/ contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Chapter 18 Retail Establishments

18.1 General. Retail establishments are primarily engaged in the direct sale of goods and products to consumers.

18.2 Application. This chapter addresses measures to control security vulnerabilities in retail establishments.

18.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

18.4 Security Policies and Procedures. A security program for retail establishments should be designed to control employee theft, robbery, burglary, shoplifting, fraud, and workplace violence.

18.4.1 Employee Theft Prevention. The key to reducing employee theft is for management to admit that theft is possible and then create an environment that makes stealing as difficult as possible. By analyzing the opportunities for theft within a company, strategies can be developed to reduce or limit the exposure.

18.4.1.1* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references, should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors' or contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

18.4.1.2 Procedural Controls and Devices.

(A) The following procedures and devices that make theft more difficult and apprehension more likely are intended to limit the opportunity for theft:

(1) Arranging work flow and task assignments so that the work of one employee acts as a control on that of another employee.
(2) Dividing responsibilities and functions so that no one employee has control over all facets of a transaction. For example, the person who has the authority to write checks and make deposits should not be responsible for reconciling the bank statement.
(3) Reducing the exposure of inventory to pilferage by keeping storage areas clean and unobstructed.
(4) Implementing a program of regular and random (surprise) inventory checks, audits, and petty cash counts.
(5) Using devices to control theft, such as video surveillance.
(6) Securing expensive items that are prone to theft to limit opportunity

(B) In any event, the application of these procedures and devices should be performed with the knowledge and agreement of employees; otherwise, there can be a damaging effect on employee morale and productivity.

18.4.2 Robbery Prevention. A retail establishment's hours of operation and the amount of cash on hand affect its risk of robbery. In general, any business with cash on the premises is a prospective target for robbers, even though the amount of cash on hand might not be high. As such, robbery prevention measures must be implemented to reduce the risk of robbery and the violence that can result from robbery. The elements of a security program to control robbery include control of cash, access control, security equipment, personnel, and employee training.

18.4.2.1 Control of Cash. Businesses with cash on hand are at greatest risk of robbery. The amount of cash in cash registers should be kept at the lowest possible level by removing extra cash for later deposit in the bank. The times and routes of bank deposits should be varied.

18.4.2.2 Access Control.

(A) The interior and the front and rear entrances of the premises should be well lit. Adequate outside lighting of the parking area and approaches during nighttime hours of operation enhance employee and customer protection. The IESNA *Lighting Handbook* provides information on lighting levels for specific areas and locations.

(B) Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the store. Clear visibility into the store can serve as a deterrent to robbery since it will enable passersby and police patrols to observe activities inside. It will also enable employees to observe suspicious activities outside the store.

(C) Many robberies occur through the back door. All rear and side doors should be kept locked at all times; however, this should not conflict with life safety and fire code requirements.

(D) Garbage areas should be located to ensure the safety of employees who use them. There should be good visibility and no potential hiding places for assailants near these areas. Robberies have occurred when employees were disposing of the trash at night. Procedures, such as using two employees, should be instituted to ensure employee safety.

18.4.2.3 Security Equipment. Security equipment includes surveillance cameras and silent holdup alarm systems. Employees should be trained in the proper use of security equipment, especially holdup alarm systems.

18.4.2.4 Personnel. Having at least two employees on duty during high-risk hours and at opening and closing times can serve as deterrents to robbery.

18.4.2.5 Employee Training. Management should establish a policy of nonresistance and give it top priority in a training program. Employees should be trained on what to do before, during, and after a robbery. Additional training should be provided on how to be an effective witness by observing details and events and providing descriptions.

18.4.3 Burglary Prevention. Burglars first look for easy ways to enter a premises — through unlocked doors, unlatched windows, and unsecured skylights. While some burglars have the expertise to pick a lock, in most cases, entry is made using physical force by smashing doors, crowbarring doors or windows, or breaking windows. Some burglars resort to breaking through building walls with sledgehammers. The risk of burglary is also influenced by the store's hours of operation. Those that operate 24 hours a day, 7 days a week are the least vulnerable to burglary. The elements of a security program to control burglary can include physical security devices, burglary-resistant safes, and intrusion detection systems.

18.4.3.1 Physical Security Devices. Burglary is a crime of opportunity. Research into the crime indicates that burglars look for places that offer the best opportunity for success. In choosing targets, burglars look for locations that contain something worth stealing and then select those that look easy to break into. Burglars appear to be strongly influenced by the look and feel of the business they are planning to burglarize. Consequently, if the exterior of a business appears to reflect attention to security, the burglar will likely look for an easier opportunity. Good locks, ironwork, and lighting all contribute to making a building appear secure. Goods at high risk to burglary, such as wines, liquor, and meats, should be stored in a locked closet, security cage, or locked freezer.

18.4.3.2 Burglary-Resistant Safes. Cash should be secured during nonbusiness hours in a burglary-resistant safe. The right type and class of safe should be chosen for the valuables to be protected. Safes are either fire-resistive or burglary-resistant and are available in various protection classes (or levels). The higher the value of the items to be protected, the higher should be the level of protection afforded by the safe. UL has listings for safes in various protection classifications. The number of people with access to the combination should be kept to a minimum. The combination number should not be stored in an easily accessible place, such as a desk blotter, and the safe should never be put in "day mode," in which only one number is needed to complete the combination. The combination should be changed on a regular basis.

18.4.3.3 Intrusion Detection Systems.

(A) Executing a burglary involves locating and collecting items of value. Factors that affect the time burglars will spend on the premises include the skill and confidence of the burglar(s), whether valuables are stored in a safe or vault, the quality of the protection, and the anticipated response by the police or designated personnel *(see Chapter 8)*.

(B) An intrusion detection system can deter a burglar. An alarm system that sends a signal to a monitoring station, which then dispatches designated personnel, is preferred. An alarm system that sounds a local bell is better than no alarm at all — at the very least, it may scare off the burglar. The safe, security closet, or security cage also should be protected by the alarm system. The alarm system should be periodically tested and maintained properly.

18.4.4 Shoplifting Prevention. Shoplifting occurs when it is easy and convenient for the shoplifter. While it is impossible to eliminate shoplifting losses completely, it should be the goal of the business to deter the would-be shoplifter as much as possible through the proper use of people and equipment. A shoplifting prevention program generally consists of procedural controls and a policy of arrest and prosecution.

18.4.4.1 Procedural Controls. Procedural controls are intended to eliminate the opportunity for shoplifting. The physical layout of the store should be such that it discourages shoplifting. Merchandise should not be located near doors, and aisles should not be cluttered. Preferably, cash registers should be located so that customers have to pass by them to exit the store. The number of entrances and exits should be limited to that required by life safety and building codes. Customers should not be allowed to use fire exits except in an emergency. Prevention methodologies, such as convex mirrors and video surveillance, should also be considered.

18.4.4.2 Arrest and Prosecution.

(A) It is generally agreed that the most important element of any shoplifting prevention program is the arrest and prosecution of shoplifters who will not otherwise be deterred. Prosecution not only serves to impress upon the individual arrested that shoplifting will not be tolerated by the store, but it establishes an attitude that becomes known in the community.

(B) Because of ignorance of the law and fear of lawsuits, however, many retail businesses are reluctant to detain or arrest shoplifters. What can begin as a criminal apprehension of a suspected thief can be converted into grounds for a civil suit against the business owner if proper procedures are not followed. Detaining someone (even momentarily) without hard evidence of theft can lead to a lawsuit for false arrest. Staff

should be trained in the procedures to follow in detaining or arresting shoplifters.

(C) All states have laws called *merchant's privilege laws,* which are intended to protect stores from civil lawsuits and criminal charges arising from the detention and questioning of suspected shoplifters. These laws provide protection against suits for false arrest provided the suspect has been detained in a reasonable manner and for a reasonable period of time and that there is reasonable assurance that the suspect has taken merchandise with no intention of paying for it.

(D) A person is not necessarily guilty of shoplifting just because he or she did not pay for an item. It is not a crime to forget to pay for something. For a person to be guilty of shoplifting, it is necessary to prove that there was intent to steal. This requires that the shoplifter be seen taking the merchandise, be seen concealing it without having paid for it, be watched continuously to be sure that the merchandise has not been "ditched" (if there is any break at all in the surveillance of the suspected shoplifter, the business will be taking a poorly calculated risk in attempting to make an arrest), and be apprehended past the last possible point where payment could be made.

(E) A retailer must develop clear and legally sound procedures for detaining suspected shoplifters and safeguarding evidence. Local police departments can usually offer advice on the proper procedures to follow.

(F) Almost all states also have laws called *civil recovery* or *civil demand* statutes, which allow retailers to forgo the hassles of the legal system and simply ask shoplifters to make restitution, including some costs. While some retailers make such requests while the suspected shoplifter is still in the custody of security personnel, loss prevention experts generally recommend that civil recovery be handled after the suspect has been released. At such time, a letter from the victimized business, on its own or via an attorney or third-party company, can be sent to the shoplifter demanding statutorily set compensation, including the value of the item(s) stolen and damages.

18.4.5 Fraud Prevention. Procedures should be established to prevent and control check, credit card, and counterfeit currency fraud by customers.

18.4.5.1 Check Fraud.

(A) Because of the risk of check fraud, some retail businesses have a policy of not accepting checks as payment for goods. For those that accept checks, a check acceptance policy should be established. The policy should be posted in a location readily seen by customers, and clerks should be trained in the policy.

(B) Elements of a check acceptance policy should include requiring two forms of identification, and listing them on the back of the check; not accepting third-party checks, such as payroll or government checks, since these can be stolen; and using an electronic check verification system.

18.4.5.2 Credit Card Fraud. To prevent credit card fraud, retail businesses should establish a credit card payment policy and train clerks in the policy. Elements of the policy should include requiring all credit card transactions to be checked electronically; checking the signature on the sales receipt against the signature on the card; and checking the validation and expiration dates on the credit card.

18.4.5.3 Counterfeit Currency. Retail businesses should train clerks in how to detect counterfeit currency and provide them with equipment that can be used to detect counterfeit currency.

18.4.6 Workplace Violence. Workplace violence is a serious safety and health hazard in many workplaces. Although it can appear to be random, many incidents can be anticipated and avoided. Even where a potentially violent incident occurs, a timely and appropriate response can prevent the situation from escalating and resulting in injury or death. Retail establishments, in particular establishments that operate late at night, can benefit from an examination of their workplaces to determine if workplace violence is a potential hazard for their employees.

18.4.6.1 OSHA Violence Prevention Guidelines.

(A) In response to this problem, the Occupational Safety and Health Administration (OSHA) has developed workplace violence prevention guidelines for use in the late-night retail industry, especially for convenience stores, liquor stores, and gasoline stations. Other types of retail establishments providing services during evening and night hours also can find this information helpful. The guidelines are intended to help retail employers design, select, and implement violence prevention programs based on the specific risk factors they identify in their particular workplaces.

(B) The goal of the guidelines is to encourage employers to implement programs to identify the potential risk of workplace violence and to implement corrective measures. The guidelines are not a model program or a rigid package of violence prevention steps uniformly applicable to all establishments. Indeed, no single strategy is appropriate for all businesses. Environmental and other risk factors for workplace violence differ widely among workplaces. Employers can use a combination of recommended strategies, as appropriate, for their particular workplace.

18.4.6.2 Employers' Duties and Workplace Violence. Under the Occupational Safety and Health Act of 1970 (the OSHA Act), the extent of an employer's obligation to address workplace violence is governed by the General Duty clause, which states the following: "Each employer should furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees."

18.4.6.3 Elements of an Effective Violence Prevention Program.

18.4.6.3.1 General.

(A) An effective approach to preventing workplace violence includes the following key components:

(1) Management commitment and employee involvement
(2) Worksite analysis
(3) Hazard prevention and control
(4) Safety and health training
(5) Evaluation

(B) Using these basic elements, employers can fashion prevention plans that are appropriate for their establishment, based on the hazards and circumstances of the particular situation. Employers should develop a written program for workplace violence prevention. A written statement of policy serves as a touchstone for the many separate plans, procedures, and actions required for an effective violence prevention program. The extent to which the components of the program are in writing, however, is less important than how effective the program is in practice. In smaller establishments, a program can be effective without being heavily documented. As the size of a workplace or the complexity of hazard control increases, written guidance becomes more important as a way to ensure clear communication and consistent

application of policies and procedures. An employer could create a separate workplace violence prevention program or incorporate this information into an existing accident prevention program, employee handbook, or manual of standard operating procedures.

18.4.6.3.2 Management Commitment and Employee Involvement. Management commitment and employee involvement are complementary elements of an effective safety and health program. To ensure an effective program, management, front-line employees, and employee representatives need to work together on the structure and operation of the violence prevention program.

18.4.6.3.2.1 Management Commitment. Management's role is to provide the motivation and resources to deal effectively with workplace violence. The visible commitment of management to worker safety and health is an essential precondition for its success. Management can demonstrate its commitment to violence prevention through the following actions:

(1) Create and disseminate a policy to managers and employees that expressly disapproves of workplace violence, verbal and nonverbal threats, and similar actions.
(2) Take all violent and threatening incidents seriously, investigate them, and take appropriate corrective action.
(3) Outline a comprehensive plan for maintaining security in the workplace.
(4) Assign responsibility and authority for the program to individuals or teams with appropriate training and skills. This means ensuring that all managers and employees understand their obligations.
(5) Provide necessary authority and resources for staff to carry out violence prevention responsibilities.
(6) Hold managers and employees accountable for their performance. Stating expectations means little if management does not track performance, reward it when it is competent, and correct it when it is not.
(7) Take appropriate actions to ensure that managers and employees follow administrative controls or work practices.
(8) Institute procedures for prompt reporting and tracking of violent incidents that occur in and near the establishment.
(9) Encourage employees to suggest ways to reduce risks, and implement appropriate recommendations from employees and others.
(10) Ensure that employees who report or experience workplace violence are not punished or otherwise suffer discrimination.
(11) Work constructively with other parties, such as landlords, lessees, local police, and other public safety agencies, to improve the security of the premises.

18.4.6.3.2.2 Employee Involvement.

(A) Employee involvement is important for several reasons. First, front-line employees are an important source of information about the operations of the business and the environment in which the business operates. This can be particularly true for employees working at night in retail establishments when higher level managers are not routinely on duty. Second, inclusion of a broad range of employees in the violence prevention program has the advantage of harnessing a wider range of experience and insight than that of management alone. Third, front-line workers can be valuable problem solvers — their personal experience often enables them to identify practical solutions to problems and to perceive hidden impediments to proposed changes. Finally, employees who have a role in developing a violence prevention program are more likely to support and carry out that program.

(B) Methods for cooperation between employees and management vary. Some employers choose to deal with employees one-on-one or assign program duties to specific employees. Other employers elect to use a team or committee approach. The National Labor Relations Act can limit the form and structure of employee involvement. Employers should seek legal counsel if they are unsure of their legal obligations and constraints.

(C) Employees and employee representatives can be usefully involved in nearly every aspect of a violence prevention program. Their involvement can include the following:

(1) Participate in surveys and offer suggestions about safety and security issues.
(2) Participate in developing and revising procedures to minimize the risk of violence in daily business operations.
(3) Assist in the security analysis of the establishment.
(4) Participate in performing routine security inspections of the establishment.
(5) Participate in the evaluation of prevention and control measures.
(6) Participate in training current and new employees.
(7) Share on-the-job experiences to help other employees recognize and respond to escalating agitation, assaultive behavior, or criminal intent and discuss appropriate responses.

18.4.6.3.3 Worksite Analysis.

18.4.6.3.3.1 Common Risk Factors in Retail Establishments. The National Institute for Occupational Safety and Health (NIOSH) has identified a number of factors that can increase a worker's risk for workplace assault. Those pertaining to late-night retail establishment include the following:

(1) Contact with the public
(2) Exchange of money
(3) Delivery of passengers, goods, or services
(4) Working alone or in small numbers
(5) Working late-night or early-morning hours
(6) Working in high-crime areas

(A) Employees in some retail establishments can be exposed to multiple risk factors. The presence of a single risk factor does not necessarily indicate that the risk of violence is a problem in a workplace. The presence of multiple risk factors or a history of workplace violence, however, should alert an employer that the potential for workplace violence is increased.

(B) Research indicates that the greatest risk of work-related homicide comes from violence inflicted by third parties, such as robbers and muggers. Robbery and other crimes were the motive in 80 percent of workplace homicides across all industries in 1996. A large proportion of the homicides occurring in the retail sector are associated with robberies and attempted robberies. On average, one in 100 gun robberies results in a homicide. For this reason, effective programs that reduce the number of robberies should result in a decrease in the number of homicides.

(C) Sexual assault is another significant occupational risk in the retail industry. Indeed, the risk of sexual assault for women is equal to or greater than the risk of homicide for employees in general. Sexual assault is usually not robbery related but can occur more often in stores with a history of robbery. These assaults occur disproportionately at night in the great majority of cases

and involve a female clerk alone in a store. The risk factors for robbery and sexual assault overlap (e.g., working alone, working late at night, high-crime areas), so actions to reduce robbery can also be effective for preventing sexual assaults.

18.4.6.3.3.2 Workplace Hazard Analysis.

(A) A worksite hazard analysis involves a step-by-step, common-sense look at the workplace to find existing and potential hazards for workplace violence. This entails the following steps:

(1) Review records and past experiences.
(2) Conduct an initial worksite inspection and hazard analysis.
(3) Perform periodic safety audits.

(B) Because the hazard analysis is the foundation for the violence prevention program, it is important to select carefully the person(s) who will perform this step. The employer can delegate the responsibility to one person or to a team of employees. A large employer that uses a team approach might want to draw the team members from different parts of the enterprise, such as senior management, operations, employee assistance, security, occupational safety and health, legal, human resources staff, and employees or union representatives. Small establishments might assign the responsibility to a single staff member or a consultant.

18.4.6.3.3.3 Review of Records and Past Incidents.

(A) As a starting point for the hazard analysis, the employer should review the experience of the business over the previous 2 or 3 years. This involves collecting and examining existing records that can shed light on the magnitude and prevalence of the risk of workplace violence. For example, injury and illness records, workers' compensation claims, and police department robbery reports can help identify specific incidents related to workplace violence. Finding few documented cases of workplace violence does not necessarily mean that violence is not a problem in a workplace, because incidents can be unreported or inconsistently documented. In some cases, management might not be aware of incidents of low-intensity conflict or threats of violence to which their employees have been exposed. To learn of such incidents, the employer can canvass employees about their experience while working for the business. The following questions can be helpful in compiling information about past incidents:

(1) Has your business been robbed during the last 2 to 3 years? Were robberies attempted? Did injuries occur due to robberies or attempts?
(2) Have any employees been assaulted in altercations with customers?
(3) Have any employees been victimized by other criminal acts at work (including shoplifting that became assaultive)? What kind?
(4) Have any employees been threatened or harassed while on duty? What was the context of those incidents?
(5) In each of the cases with injuries, how serious were the injuries?
(6) In each case of violence, was a firearm involved? Was a firearm discharged? Was the threat of a firearm used? Were other weapons used?
(7) What part of the business was the target of the robbery or other violent incident?
(8) At what time of day did the robbery or other incident occur?
(9) How many employees were on duty?
(10) Were the police called to your establishment in response to the incident? (When possible, obtain reports of the police investigation.)
(11) What tasks were employees performing at the time of the robbery or other incident? What processes and procedures might have put employees at risk of assault? Similarly, were there factors that might have facilitated an outcome without injury or harm?
(12) Were preventive measures already in place and used correctly?
(13) What were the actions of the employees during the incident? Did these actions affect the outcome of the incident in any way?

(B) Employers with more than one store or business location can review the history of violence at each operation. Different experiences in those stores can provide insights into factors that can make workplace violence more or less likely. Contacting similar local business, community, and civic groups and local police departments is another way to learn about workplace violence incidents in the area. In addition, trade associations and industry groups often provide useful information about conditions and trends in the industry as a whole.

18.4.6.3.3.4 Workplace Security Analysis.

(A) The team or the coordinator can conduct a thorough initial risk assessment to identify hazards, conditions, operations, and situations that could lead to violence. The initial risk assessment includes a walk-through survey to provide the data for risk identification and the development of a comprehensive workplace violence prevention program. The assessment process includes the following:

(1) Analyze incidents, including the characteristics of assailants and victims; give an account of what happened before and during the incident; and note the relevant details of the situation and its outcome.
(2) Identify any apparent trends in injuries or incidents relating to a particular worksite, job title, activity, or time of day or week; identify specific tasks that can be associated with increased risk.
(3) Identify factors that can make the risk of violence more likely, such as physical features of the building and environment, lighting deficiencies, lack of telephones and other communication devices, areas of unsecured access, and areas with known security problems.
(4) Evaluate the effectiveness of existing security measures and assess whether those control measures are being properly used and whether employees have been adequately trained in their use.

(B)* Figure A.18.4.6.3.3.4(B) provides a sample checklist that illustrates a number of questions that can be helpful for the security analysis.

18.4.6.3.3.5 Periodic Safety Audits. Hazard analysis is an ongoing process. A good violence prevention program will institute a system of periodic safety audits to review workplace hazards and the effectiveness of the control measures that have been implemented. These audits also can evaluate the impact of other operational changes (such as new store hours and changes in store layout) that were adopted for other reasons but that can affect the risk of workplace violence. A safety audit is important in the aftermath of a violent incident or other serious event for reassessing the effectiveness of the violence prevention program.

18.4.6.3.4 Hazard Prevention and Control. After violence hazards have been assessed, the next step is to develop measures to protect employees from the identified risks of injury and violent acts. Workplace violence prevention and control programs include specific engineering and work practice controls to address identified hazards. The tools listed in this section are not intended to be a "one-size-fits-all" prescription. No single control will protect employees. To provide effective deterrents to violence, the employer should use a combination of controls in relation to the hazards identified through the hazard analysis.

18.4.6.3.4.1 Prevention Strategies.

(A) Since the major risk of death or serious injury to retail employees is from robbery-related violence, an effective prevention program would include, but not be limited to, steps to reduce the risk of robbery. In general, a business can reduce the risk of robbery by doing the following:

(1) Increasing the effort the perpetrator must expend (target hardening, controlling access, and deterring offenders)
(2) Increasing the risks to the perpetrator (entry/exit screening, formal surveillance by employees and others)
(3) Reducing the rewards to the perpetrator (removing the target, identifying property, and removing inducements)

(B) Other deterrents that can reduce the potential for robbery include security cameras, time-release safes, other 24-hour business at the location, no easy escape routes or hiding places, and closing the store during the late-night hours.

18.4.6.3.4.2 Engineering Controls and Workplace Adaptation. Engineering controls remove the hazard from the workplace or create a barrier between the worker and the hazard. The following physical changes in the workplace can help reduce violence-related risks or hazards in retail establishments:

(1) Improve visibility. Visibility is important in preventing robbery in two respects: Employees should be able to see their surroundings, and persons outside the store, including police on patrol, should be able to see into the store. Employees in the store should have an unobstructed view of the street, clear of shrubbery, trees, or any form of clutter that a criminal could use to hide. Signs located in windows should be either low or high to allow good visibility into the store.
(2) Maintain adequate lighting within and outside the establishment to make the store less appealing to a potential robbery by making detection more likely. The parking area and the approach to the retail establishment should be well lit during nighttime hours of operation. Exterior illumination might need upgrading in order to allow employees to see what is occurring outside the store.
(3) Use fences and other structures to direct the flow of customer traffic to areas of greater visibility.
(4) Use drop safes to limit the availability of cash to robbers. Employers using drop safes can post signs stating that the amount of cash on hand is limited.
(5) Install video surveillance equipment and closed-circuit TV (video surveillance) to deter robberies by increasing the risk of identification. This can include interactive video equipment. The video recorder for the video surveillance should be secure and out of sight. Posting signs that surveillance equipment is in use and placing the equipment near the cash register can increase the effectiveness of the deterrence.
(6) Put height markers on exit doors to help witnesses provide more complete description of assailants.
(7) Use door detectors to alert employees when persons enter the store.
(8) Control access to the store with door buzzers.
(9) Use silent or wireless holdup alarm devices to notify police in the event of a problem.
(10) Install physical barriers such as bullet-resistant enclosures with pass-through windows between customers and employees to protect employees from assaults and weapons in locations with a history of robberies or assaults that are located in high-crime areas.

18.4.6.3.4.3 Administrative and Work Practice Controls. Administrative and work practice controls affect the way employees perform jobs or specific tasks. The following examples illustrate work practices and administrative procedures that can help prevent incidents of workplace violence:

(1) Integrate violence prevention activities into daily procedures, such as checking lighting, locks, and security cameras, to help maintain worksite readiness.
(2) Keep a minimal amount of cash in each register, especially during evening and late-night hours of operation. In some businesses, transactions with large bills can be prohibited. Cash levels should be as low as is practical. Employees should not carry business receipts on their person unless it is absolutely necessary.
(3) Adopt proper emergency procedures for employees to use in case of a robbery or security breach.
(4) Establish systems of communication in the event of emergencies. Employees should have access to working telephones in each work area, and emergency telephone numbers should be posted by the phones.
(5) Adopt procedures for the correct use of physical barriers, such as enclosures and pass-through windows.
(6) Increase staffing levels at night at stores with a history of robbery or assaults that are located in high crime areas. It is important that clerks be clearly visible to patrons.
(7) Lock doors used for deliveries and disposal of garbage when not in use; also, do not unlock delivery doors until the delivery person is identified. Take care not to block emergency exits — doors must open from the inside without a key to allow persons to exit in case of fire or other emergency.
(8) Establish rules to ensure that employees can walk to garbage areas and outdoor freezers or refrigerators without increasing their risk of assault. The key is for employees to have good visibility, thereby eliminating potential hiding places for assailant near these areas. In some locations, taking trash out or going to outside freezers during daylight can be safer than doing so at night.
(9) Keep doors locked before business officially opens and after closing time. Establish procedures to ensure the security of employees who open and close the business, when staffing levels can be low. The day's business receipts can be a prime robbery target at store closing.
(10) Limit or restrict areas of customer access, reduce the hours of operation, or close portions of the store to reduce risk.
(11) Adopt safety procedures and policies for off-site work, such as deliveries.
(12) Administrative controls are effective only if they are followed and used properly. Regular monitoring helps ensure that employees continue to use proper work practices. Giving periodic, constructive feedback to employees helps to ensure that they understand these procedures and their importance.

18.4.6.3.4.4 Post-Incident Response. Post-incident response and evaluation are important parts of an effective violence prevention program. Standard operating procedures should be developed for management and employees to follow in the aftermath of a violent incident. Such procedures can include the following:

(1) Ensure that injured employees receive prompt and appropriate medical care, including transportation to medical care. Prompt first-aid and emergency medical treatment can minimize the harmful consequences of a violent incident.
(2) Report the incident to the police.
(3) Notify other authorities as required by applicable laws and regulations.
(4) Inform management about the incident.
(5) Secure the premises to safeguard evidence and reduce distractions during the post-incident response process.
(6) Prepare an incident report immediately after the incident, noting details that might be forgotten over time.
(7) Arrange appropriate treatment for victimized employees. In addition to physical injuries, victims and witness can suffer psychological trauma; fear of returning to work; feelings of incompetence, guilt, and powerlessness; and fear of criticism by supervisors or managers. Post-incident debriefing and counseling can reduce psychological trauma and stress among victims and witnesses. An emerging trend is to use critical incident stress management to provide a range or continuum of care tailored to the individual victim or the organization's needs.

18.4.6.3.5 Training and Education. Training and education ensure that all staff are aware of potential security hazards and the procedures for protecting themselves and their coworkers. Employees with different roles in the business will need different types and levels of training.

18.4.6.3.5.1 General Training.

(A) Employees need instruction on the specific hazards associated with their jobs and the worksite to help them minimize their risk of assault and injury. Such training includes information on potential hazards identified in the establishments and the methods to control those hazards. Topics can include the following:

(1) An overview of the potential risk of assault
(2) Operational procedures, such as cash-handling rules, that are designed to reduce risk
(3) Proper use of security measures and engineering controls that have been adopted in the workplace
(4) Behavioral strategies to defuse tense situations and reduce the likelihood of a violent outcome, such as techniques of conflict resolution and aggression management
(5) Specific instructions on how to respond to a robbery (such as the instruction to turn over money or valuables without resistance) and how to respond to attempted shoplifting
(6) Emergency action procedures to be followed in the event of a robbery or violent incident

(B) Training should be conducted by persons who have a demonstrated knowledge of the subject and should be presented in language appropriate for the individuals being trained. Oral quizzes or written tests can ensure that the employees have actually understood the training. An employee's understanding also can be verified by observing the employee at work.

(C) The need to repeat training varies with the circumstances. Retraining should be considered for employees who violate or forget safety measures. Similarly, employees who are transferred to new job assignments or locations can need training even though they received some training in their former positions. Establishments with high rates of employee turnover need to provide training more frequently.

18.4.6.3.5.2 Training for Supervisors, Managers, and Security Personnel.

(A) To recognize whether employees are following safe practices, management personnel should undergo training comparable to that of the employees and additional training to enable them to recognize, analyze, and establish violence prevention controls. Knowing how to ensure sensitive handling of traumatized employees is an important skill for management. Training for managers also could address specific duties and responsibilities they have that could increase their risk of assault. Security personnel need specific training about their roles, including the psychological components of handling aggressive and abusive customers and ways to handle aggression and defuse hostile situations.

(B) The team or coordinator responsible for implementation of the program should review and evaluate annually the content, methods, and frequency of training. Program evaluation can involve interviewing supervisors and employees, testing and observing employees, and reviewing responses of employees to workplace violence incidents.

18.4.6.3.6 Evaluation.

18.4.6.3.6.1 Record Keeping.

(A) Good records help employers determine the severity of the risks, evaluate the methods of hazard control, and identify training needs. An effective violence prevention program uses records of injuries, illnesses, incidents, hazards, corrective actions, and training to help identify problems and solutions for a safe and healthful workplace.

(B) Employers can tailor their record-keeping practices to the needs of their violence prevention program. The purpose of maintaining records is to enable the employer to monitor ongoing efforts, to determine if the violence prevention program is working, and to identify ways to improve it. Employers can find the following types of records useful for this purpose:

(1) Records of employees' and others' injuries and illnesses at the establishment.
(2) Records describing incidents involving violent acts and threats of such acts, even if the incident did not involve an injury or a criminal act. Records of events involving abuse, verbal attacks, or aggressive behavior can help identify patterns and risks that are not evident from the smaller set of cases that actually result in injury or crime.
(3) Written hazard analyses.
(4) Recommendations of police advisors, employees, or consultants.
(5) Up-to-date records of actions taken to deter violence, including work practice controls and other corrective steps.
(6) Notes of safety meeting and training records.

18.4.6.3.6.2* Prevention Programs. Violence prevention programs benefit greatly from periodic evaluation. The evaluation process can involve the following:

(1) Review the results of periodic safety audits.
(2) Review post-incident reports. In analyzing incidents, the employer should pay attention not just to what went wrong, but to actions taken by employees that avoided further harm, such as handling a shoplifting incident in such a way as to avoid escalation to violence.
(3) Examine reports and minutes from staff meetings on safety and security issues.
(4) Analyze trends and rates in illnesses, injuries, or fatalities caused by violence relative to initial or baseline rates.
(5) Consult with employees before and after making job or worksite changes to determine the effectiveness of the interventions.
(6) Keep abreast of new strategies to deal with violence in the retail industry.
(7) Communicate to all employees lessons learned from evaluation of the workplace violence prevention program. Management could discuss changes in the program during regular meetings of the safety committee, with union representatives, or with other employee groups.

Chapter 19 Office Buildings

19.1 General. An office building is a facility used for office, professional, or service-type transactions, including storage of records and accounts. The term *office buildings,* as used in this chapter, does not include buildings that are operated by the federal, state, or local government; that have tenants that can include law enforcement agencies, court/related agencies and functions, or government records and archives; or that have tenants that perform functions critical to national security. Security for such buildings should be designed according to the requirements of the U.S. Department of Justice (DOJ) publication *Vulnerability Assessment of Federal Facilities.*

19.2 Application. This chapter addresses measures to control security vulnerabilities in office buildings. This information serves only as a guide to setting up a security program for an office building. It is important to note that no general guide is adequate to the task of addressing the unique security needs of each specific site.

19.3 Security Plan and Security Vulnerability Assessment.

19.3.1 Development. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

19.3.2 Special Considerations. The dilemma that office building owners and managers face is how to keep the building secure while allowing entry to legitimate users and exit under emergency conditions. While authorized personnel should be allowed to come and go with relative ease, unauthorized individuals require restricted access.

19.3.2.1 Ideally, security for an office building should be considered during the architectural planning stages. It is then that crime prevention measures, including access control systems, can be most economically implemented. Unfortunately, security considerations are often after the fact, occurring only after the building has been designed.

19.3.2.2 Different business settings or structures, such as high-rise office buildings or campus-style settings of multiple buildings, require different access control approaches.

(A) In an office building occupied by one company, ground- or street-level access control, combined with additional controls at sensitive areas, can be set up.

(B) In multitenant buildings, security is more complex. Access control in the main lobby will usually serve as a first line of defense. For tenants that occupy one entire floor above the lobby level, the elevator lobby on the floor can serve as a second control point. If there are several tenants on a floor, the tenants should provide some type of control at their entrance door. For tenants that occupy several floors served by one elevator bank, access control can be set up at the street-level lobby to their elevator bank. If there is no dedicated elevator bank, programming elevators to stop at only one floor, especially during nonbusiness hours, coupled with the use of internal stairs allows for economical single-point control.

(C) In a campus-style environment with several buildings, multiple visitor reception points can be needed. A lobby with a receptionist controlling access to the interior is typical. An economical alternative is a telephone in a secured lobby.

19.3.2.3 The level of security needed will depend on the degree of risk involved. Businesses with valuable products, trade secrets, confidential or sensitive company information, expensive equipment and furnishings, or valuable art collections are at greater risk to unauthorized intruders and therefore require a higher level of access control.

19.3.2.4 The types of tenants and their respective business activities also affect the level of security needed. An example is an office building with a restaurant or theater tenant. This type of tenant is usually open after normal business hours and on weekends, requiring additional security during these periods. An office building with residential tenants, who require 24-hour access, is another example of unique security needs.

19.4 Security Policies and Procedures. A security program for an office building should consist of security measures for exterior areas, common interior areas, and parking areas; access control at basement-, ground-, and street-level entrances and exits; a lock and key control program; training and supervision of security personnel; employee background checks and drug testing; and regular research into local neighborhood crime trends. Regardless of the measures utilized, security should not conflict with life safety code requirements.

19.4.1 Neighborhood Crime.

19.4.1.1 Research should be conducted to determine the state of the neighborhood surrounding the facility. The research should focus on whether the neighborhood has remained stable or deteriorated.

19.4.1.2 A history of violent and property crime in the immediate neighborhood and on the premises should be compiled and reviewed.

19.4.1.3 A relationship with local law enforcement agencies should be developed to make them familiar with the property.

19.4.1.4 The local police should be requested to include the facility in patrol routes.

19.4.1.5 An open line of communication should be maintained with the local police and federal authorities to obtain information on crime and crime trends in the neighborhood or area.

19.4.1.6* Management should be active in local security associations or industry trade groups as a means of sharing common security concerns and solutions.

19.4.2 Ground- or Street-Level Entrance Areas. Entrance areas provide the first impression of the level of security awareness in a building. An office building should not give the appearance of being open to casual visitors, and building traffic should be controlled. Establishing a policy of identification and control sends a psychological message about management's commitment to secure the building against individuals without a legitimate purpose for being in the building.

19.4.2.1 If a reception or security desk is provided in the lobby of the building, it should be positioned to provide for the best view of doorways and persons entering the building. A uniformed receptionist or guard should be stationed at the desk when the building is open.

19.4.2.2 If there is an automated access control system for employees, the entrance should be located as close as practically possible to the reception desk. If there is no automated access control system, a guard or receptionist should check employee identification.

19.4.2.3 Visitors should be funneled to the reception desk and not be able to access secure areas without proper authorization. All visitors should be required to identify the person they are visiting, and that person should be called to confirm the appointment. If policy requires it, visitors should be escorted to their destination.

19.4.2.4 Visitors should be required to wear a visitor's badge; however, it should be noted that if employees are not required to wear badges, visitors have only to remove theirs to look like employees.

19.4.2.5 A messenger center for packages, lunches, and other deliveries should be established. Messengers should not be allowed to roam the building freely.

19.4.2.6 The doors from emergency stairwell exits on the ground or street level should not have exterior door handles, and exterior hinge pins should be secured against removal. Door locks should comply with local building, fire prevention, and life safety codes.

19.4.2.7 Emergency telephone numbers and building management contact information should be readily available at the reception desk.

19.4.2.8 Twenty-four-hour video surveillance and recording are desirable at all locations as a deterrent. Requirements depend on the results of an assessment of the security threat. Time-lapse video recordings are also highly valuable as a source of evidence and investigative leads. Warning signs advising of 24-hour surveillance act as a deterrent in protecting employees and facilities. While the video surveillance system can be monitored at the reception desk, it is usually preferable that it be monitored at a separate security console.

19.4.2.9 Emergency exits should be alarmed and monitored to detect unauthorized use. NFPA *101*, *Life Safety Code*, permits the use, under specific conditions, of delayed egress locks on emergency exits.

19.4.2.10 If an intrusion detection system is provided, it should be monitored by a monitoring station.

19.4.3 Basement Level. Many office buildings have at least one basement level, usually containing the shipping and receiving docks and parking areas. A ramp from ground level provides for vehicular entrance and exit. The measures in 19.4.3.1 and 19.4.3.2 should be considered.

19.4.3.1 A door of solid construction should be used to secure the opening. A video surveillance camera can be installed for continuous surveillance of the door and ramp. An intercom should be available at the entrance to identify persons or vehicles without identification credentials.

19.4.3.2 The freight elevator doors leading into the shipping and receiving area should be secured during periods of nonuse.

19.4.4 Parking Areas. Users of this guide should consult Chapter 21 for information concerning parking facilities.

19.4.4.1 Identification credentials should be issued to tenants and employees for identifying automobiles authorized to park in the parking area.

19.4.4.2 An area separate from employee and tenant parking should be assigned for visitor parking.

19.4.4.3 Escorts to automobiles should be provided on request for employees and tenants.

19.4.4.4 Lighting should be provided to all areas of the parking area. IESNA RP-20, *Lighting for Parking Facilities*, provides information on recommended lighting levels for parking areas.

19.4.4.5 If video surveillance is provided, it should be monitored or recorded. If recorded, the video recording equipment, including storage media, should be secured from attack or removal.

19.4.4.6 Parking areas should be patrolled by security personnel on an unscheduled but frequent basis.

19.4.4.7 Records should be maintained of the frequency and results of patrols.

19.4.4.8 If adjacent parking facilities not under the control of management are used for overflow parking, management should provide for safety and security services when the lots are in use.

19.4.4.9 The design of the parking area should allow for visibility of the whole area.

19.4.4.10 Access to the parking area should be controlled.

19.4.5 Exterior Areas. Building owners and managers should secure exterior areas of their facility.

19.4.5.1 Where circumstances warrant, consideration should be given to establishing perimeter security. Fencing or other physical barriers, if appropriate, on the perimeter of the protected asset can discourage unauthorized access to the protected asset and might deter the opportunistic criminal.

19.4.5.2 The exterior of the building should be checked for design features that create areas of concealment for assailants, and these spaces should be fenced or otherwise secured to limit access.

19.4.5.3 Foliage and shrubbery should be trimmed and maintained to eliminate areas of concealment and to provide for surveillance of the property.

19.4.5.4 Lighting should be provided to illuminate building entrances, pedestrian walkways, and vehicular entrances. The IESNA *Lighting Handbook* should be consulted for recommended minimum illumination levels for these areas. The lighting system should be inspected regularly, with inoperative fixtures repaired or replaced.

19.4.5.5 Signs of vandalism should be noted and corrected.

19.4.5.6 Signs of transients or vagrants living on or around the property should be noted and corrected.

19.4.5.7 If patrols of exterior areas are conducted, they should be on a scheduled basis, without a predetermined pattern, and supervised.

19.4.5.8 If video surveillance is provided in exterior areas, it should be monitored or recorded.

19.4.6 Employee and Tenant Areas and Common Interior Areas.

19.4.6.1 Restrooms used by tenants and employees should be located so that they can be entered only from a protected or secured area. Restrooms in unprotected areas should remain locked with keys that are available only at a secure, central location on each floor. The doors to restrooms should be equipped with automatic door closers and a latch-type lock to ensure they are not accidentally left unlocked.

19.4.6.2 Employees and tenants should be advised to exercise reasonable care in protecting personal property. In unoccupied offices, purses should not be left on top of desks or on the floor, and wallets and checkbooks should not be left in jackets.

19.4.6.3 Stairwells and elevators should be provided with illumination in accordance with the IESNA *Lighting Handbook*.

19.4.6.4 If video surveillance is provided in stairwells and elevators, it should be monitored or recorded.

19.4.6.5 Elevator cars should be equipped with means(e.g., convex mirror) to allow someone to see inside the car before entering.

19.4.6.6 Unauthorized access to utility areas should be controlled.

19.4.7 Access Control.

19.4.7.1 All exterior entrances into the facility should be equipped with automatic door closers and secure locks.

19.4.7.2 Perimeter entrances should be secured during nonbusiness hours. Entry point(s) should be designated for afterhours access. A program should exist to ensure that entrances that are not needed for entry or exit are secured. This program should not conflict with fire and building code exit requirements.

19.4.7.3 Exterior hinge pins on doors should be secured against removal.

19.4.7.4 All exterior entrances to the building should be adequately illuminated.

19.4.7.5 If video surveillance is provided for exterior entrances, it should be monitored or recorded.

19.4.7.6 Identification credentials should be issued to all employees and tenants. The cards should have, as a minimum, a photograph of the bearer and the bearer's name. Identification credentials should have the bearer's signature and the signature of the individual authorized to issue the card. Employees and tenants should be required to display their ID cards at all times; at the very least, they should be required to display them on demand. For large facilities, the use of color codes on identification cards should be considered and codes established for specific buildings, floors, or areas. The stock for the cards should be controlled to ensure that the system cannot be compromised.

19.4.7.7 Custodial personnel reporting to the building after the end of the normal business day, whether employees or a contract service, should be required to check in and check out with security personnel. Custodial personnel should display identification credentials acceptable to facility management.

19.4.7.8 Contractors and other vendors should display identification credentials acceptable to facility management.

19.4.8 Locks and Key Control.

19.4.8.1 Exterior entrances should be provided with secure locking devices.

19.4.8.2 All locking devices in the building should comply with all applicable federal, state, and local requirements.

19.4.8.3 All locking devices should be properly installed and be in good working order.

19.4.8.4 The facility should operate a key control program.

19.4.8.5 A log of keys issued to employees and vendors should be maintained at the facility.

19.4.8.6 Facility keys should not be identified in any manner such that a person finding a lost key could trace it back to the facility for illegal use.

19.4.8.7 Keys should be restricted to those who need them. A responsible individual should be in charge of issuing keys and for maintaining complete, up-to-date records of the disposition of keys, including copies. The records should show issuance and return of keys, including the name of person, as well as date and time.

19.4.8.8 Extra copies of keys should be kept locked in a secure cabinet with access control.

19.4.8.9 Records of key issuance should be secured and kept separate from keys.

19.4.8.10 Procedures should be established for collecting keys from terminated employees, employees on vacation, and vacated tenants.

19.4.8.11 Lost keys should be reported immediately and procedures established for the rekeying or replacement of affected locks.

19.4.8.12 A policy should be established to restrict duplication of keys without written permission.

19.4.8.13 All keys should be marked "DO NOT DUPLICATE" to deter the unauthorized copying of keys.

19.4.8.14 A master key system should be used to limit the number of keys carried by personnel requiring access to all areas of the building. It is important that such a system not be designed so that the loss of a single key could provide an unauthorized individual unrestricted access to all areas of the building. The sophistication of the master key system should be based on an assessment of employees' or tenants' needs and the criticality, vulnerability, and sensitivity of areas.

19.4.8.15 Master key distribution should be on an as-needed basis with records kept of personnel in possession of master keys.

19.4.9* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references should be done on all individuals with access to critical assets *(see Chapter 10)*.

(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

19.4.10 Security Operations. If security guards are required, the number of guards at any given time will depend on the size of the facility, the hours of operation, and current risk factors. Many states have laws that require background checks and specific training for security personnel, especially armed personnel. It is essential that facilities using security personnel train them in the legal and practical applications of their employment. Training must be an ongoing effort in response to changing regulations and the enactment of new laws.

19.4.10.1 Guard training should include but not be limited to human relations, emergency procedures, patrol methods, and first aid training.

19.4.10.2 Background checks, including criminal records checks, should be done on all security personnel.

19.4.10.3 Details from security contracting agencies should be requested regarding their pre-employment screening procedures.

19.4.10.4 If contracting security personnel are used, the contracting firm should have adequate liability insurance.

19.4.10.5 Written job descriptions should exist for each position.

19.4.10.6 The decision not to provide 24-hour security should be based on an SVA.

19.4.10.7 A written training program and documentation of the training should exist for security personnel.

19.4.10.8 Security personnel should patrol the premises on a regular schedule but not in a predetermined pattern.

19.4.10.9 Security patrols should be conducted in accordance with the facility security plan and supervised in accordance with Section 9.7.

19.4.10.10 Security patrol records should be reviewed on a regular basis.

19.4.10.11 Security personnel should be provided with portable communication equipment.

19.4.10.12 If security personnel are armed, they should be properly trained in the use of firearms. Training should be ongoing.

19.4.10.13 Formalized procedures for informing security personnel about changes in security policies and crime trends should exist.

19.4.10.14 Regular meetings should occur between management and security personnel to discuss crime concerns and solutions. These meetings should be documented.

19.4.10.15 Procedures should be established for documenting all security-related complaints made by employees and tenants and the actions taken by building management to resolve them.

19.4.10.16 A policy should be established for notifying tenants (e.g., by a monthly newsletter) of significant security-related incidents.

19.4.10.17 Security incident reports should be maintained at the facility for not less than five years.

19.4.10.18 Security equipment should be covered under a service and maintenance agreement. Emergency and security equipment should be repaired on a priority basis with a log of the repairs kept.

19.5 Management Considerations. An effective security program will depend on coordinated development and implementation of the security plan between management, security personnel, and employees. Often, the difference between the success and failure of a security program is realized through management's degree of commitment to and support for the program.

19.5.1 Written policies regarding safety, security, and emergency management should exist and be reviewed.

19.5.2 All appropriate staff should be trained to these policies.

19.5.3 Standard written work practices for all employee functions should exist.

19.5.4 All appropriate staff should be trained to these practices.

19.5.5 Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

19.5.6 Sales personnel should be advised not to make oral promises regarding the security of the facility.

19.5.7 An emergency or disaster plan, including procedures for evacuating the building, should be developed. An emergency team should be organized on every floor. Emergency team members should be trained in evacuation procedures and response to other types of emergencies, including weapons of mass destruction. Records should be kept by property management regarding emergency team training and annual evacuation drills. This plan should be in writing and tested periodically. The plan should be developed in conjunction with the local authorities having jurisdiction (AHJs), reviewed periodically, and updated to reflect the current security climate.

19.5.8 Security awareness training should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

19.5.9 Maintenance, housekeeping, and other service personnel who operate on all floors or areas of the building should be issued distinctive uniforms and identification credentials. The supply of uniforms should be controlled.

Chapter 20 Industrial Facilities

20.1 General. An industrial facility is a facility in which products are manufactured or in which processing, assembling, mixing, packaging, finishing, decorating, or repair operations are conducted.

20.2 Application. This chapter addresses measures to control security vulnerabilities in industrial facilities.

20.3 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

20.3.1 Special Considerations. A facility safety plan and a security plan often address the same similar concerns. An evaluation of current safety and security systems should be included in the SVA. Factors that should be reviewed for applicability and consideration include the following:

(1) The location of the site in relation to other structures, facilities, and population centers
(2) The accessibility of the site
(3) The building age, construction type, and openings
(4) Hours of operation
(5) Hazardous materials or processes at the site

20.3.1.1 Sites that are close to other structures or facilities may be vulnerable from shared perimeters, buildings that are close together, or hazardous processes.

20.3.1.2 The existing security systems (e.g., fences, security lighting, security patrols, or electronic premises security systems) should be evaluated to establish if they are adequate to limit access to the site.

20.3.1.3 Older buildings might be more vulnerable because they have more windows, while some newer buildings are designed for easy access.

20.3.1.4 A facility that operates 24 hours a day might need less security, because there are always people on-site, than a facility that is unoccupied at night.

20.3.1.5 Some hazardous materials or processes can be particularly attractive targets because of the potential for greater consequences.

20.3.2 Site Security Improvements. Decisions about improving site security should be made after an evaluation of how vulnerable the site is to threats and what additional measures, if any, are appropriate to reduce this vulnerability. Decisions about security should be made based on the circumstances at the particular facility.

20.4 Security Policies and Procedures. Most security measures are intended to prevent intruders from gaining access to the site or, in the event access is gained, to limit damage. The information provided in this section presents a number of design and procedural approaches that facilities can implement. The appropriateness of any of these measures depends on site-specific conditions that would need to be considered in an assessment of the security needs of a facility.

20.4.1 Intrusion Prevention.

20.4.1.1 Facilities should restrict access to critical assets by establishing a secure perimeter.

20.4.1.1.1 The secure perimeter should be established using physical, electronic, or other means.

20.4.1.1.2 Portals and accessible openings in the secure perimeter should be protected against entry by unauthorized persons.

20.4.1.2 The location of the facilities, whether urban or suburban, and the types of structures determine how much and what type of protection a facility needs.

20.4.1.2.1 At a suburban office park or campus location, a perimeter fence allowing for the creation of stand-off distances and gates staffed by security can control vehicle access.

20.4.1.2.2 In urban areas, the use of passive barriers, such as concrete planters and bollards, can help to create room for pedestrians to walk to buildings and to protect against vehicle bombs.

20.4.1.2.3 The design and construction of buildings also influence the level of security provided. Building exteriors should be designed to eliminate hiding places for criminals.

20.4.1.2.4 Building facades of glass are vulnerable to bomb blasts; masonry facades are more secure.

20.4.1.3 Some facilities augment these measures with intrusion detection systems, video surveillance, security guards, proprietary monitoring station alarm systems, or explosive and metal detectors. If the facility has guards, consideration should be given to their training, especially with regard to their ability to respond to emergency situations.

20.4.1.4 Access to critical assets should be restricted to the following:

(1) Employees
(2) Authorized vendors and contractors
(3) Escorted visitors

20.4.1.4.1 To protect against unauthorized entry through normal entrances, security clearances, badges, procedures for daily activities and abnormal conditions, and vehicular and pedestrian traffic control can provide efficient access for employees while ensuring that any visitors are checked and cleared before entering.

20.4.1.4.2 Most facilities have procedures to recover keys from employees who leave and to immediately remove the employee's security codes from systems. At times, it can be wise to consider additional measures, such as changing locks, when a disgruntled employee leaves.

20.4.1.4.3 In addition to providing perimeter protection to the facility, it is important that systems be in place to limit the potential damage from an intruder who gains entry or from the disgruntled employee.

20.4.1.4.3.1 This damage can be done physically at the site or by hacking into the company's computers.

20.4.1.4.3.2 Most of the steps to limit physical damage should already be part of the process safety management system. These steps can be related either to the design of the facility and its processes or to procedures implemented.

20.4.2 Material Receiving. It is necessary to limit entry points, control traffic, inspect shipments, and document the entry of goods into the facility.

20.4.2.1 Commercial Receivables

20.4.2.1.1 Trucks coming into receiving docks should be stopped for entry authorization and dock assignment.

20.4.2.1.2 Shipments coming in should be expected and have corresponding purchase orders or requisitions. Undocumented deliveries should not be accepted.

20.4.2.1.3 Receipt of hazardous materials should be documented and tracked.

20.4.2.2 Package Deliveries.

20.4.2.2.1 Packages being delivered should be inspected for evidence of tampering or damage. See 20.4.2.3.2 for characteristics indicating a suspicious package.

20.4.2.2.2 Any damaged or suspicious packages should be reported to the carrier.

20.4.2.3 Mail.

20.4.2.3.1 Employees who handle mail should evaluate the appearance of incoming packages to determine if they fit the characteristics of mail normally received.

20.4.2.3.2 Suspicious mail may show any or all of the following characteristics.

(1) No return address
(2) Mailed from a foreign country
(3) Excessive postage
(4) Restrictive markings like "Personal" or "Special Delivery"
(5) Misspelled information in the address
(6) Addressed to a title rather than an individual
(7) Badly typed or written
(8) Powdery substance felt through or appearing on the package or envelope
(9) Lopsided or uneven in shape
(10) Rigid or bulky packaging
(11) Strange odor
(12) Oily stains, discoloration, or crystallization on the packaging
(13) Excessive packaging material such as masking tape or string
(14) Excessive weight
(15) Ticking sound
(16) Protruding wires or aluminum foil

20.4.2.3.3 The recipient of a letter or package should carefully evaluate the nature of the delivery to determine if a package is from an unknown, unsolicited source.

20.4.2.3.4 Suspicious packages or mail should not be opened.

20.4.2.3.5 Consideration should be given to receiving mail in a separated area away from critical functions.

20.4.2.4 Couriers.

20.4.2.4.1 Couriers making deliveries should provide identification.

20.4.2.4.2 Courier identification should be entered into a delivery log or attached to the item being delivered.

20.4.3 Procedures and Policies. The standard operating policies and procedures at a facility can limit the damage caused by a security breach. The procedural steps that are routinely taken to operate safely can also help mitigate adversarial events.

20.4.3.1 Maintaining good labor relations will help to protect the facility from actions by employees or contractors.

20.4.3.1.1 Important labor relations considerations are:

(1) Open negotiations
(2) Workplace policies emphasizing that violence and substance abuse are not tolerated
(3) Adequate training and resources

20.4.3.1.2 The goal of good labor relations should be to develop the capacity of the workforce and management to identify and solve problems by working together.

20.4.3.2 As a matter of good practice as well as site security, storage tanks and delivery vehicles not in use should be disconnected from piping, transfer hoses, or distribution systems, which are often vulnerable to an adversarial event.

20.4.3.3 Hazardous material inventory should be accurately monitored.

20.4.3.3.1 The inventory of hazardous materials should be limited to the minimum needed for operation. This practice limits the quantity of a hazardous material that could be released.

20.4.3.3.2 Another practice to consider is substituting less hazardous substances when possible to make processes inherently safer.

20.4.3.4 Written procedures are an important tool in protecting a facility.

20.4.3.4.1 Emergency shutdown procedures should be included as part of the written operating procedures.

20.4.3.4.2 Workers should be trained in emergency procedures.

20.4.3.4.3 Emergency procedures are particularly important if there are processes that operate under extreme conditions (high or low pressures or temperatures). Rapid shutdown can create further hazards if done improperly.

20.4.3.5 Security professionals should be consulted to determine the vulnerability of the facility as a target for vandalism, bomb threats, and burglary.

20.4.3.6 For processes, safety, and emergency response equipment, it is important to have a program in which all equipment is subject to inspection and to corrective and preventive maintenance. This will help to ensure that safety systems will operate as designed.

20.5 Management Considerations.

20.5.1* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references should be done on all individuals with access to critical assets *(see Section 10.6)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

20.5.2 Key Control.

20.5.2.1 Locking devices should be as recommended in Section 7.2.

20.5.2.2 Locking devices should be kept in good working order through regular inspections and maintenance.

20.5.2.3 Key control should be maintained using the procedures recommended in 7.2.2.2.

20.5.2.4 Policies should be established outlining who has authority to grant access and who is responsible for issuing keys.

20.5.3 Security Operations.

20.5.3.1 The decision to use security officers should be guided by an SVA or decisions made by other responsible parties.

20.5.3.2 Post orders should be issued as recommended in 9.4.1.

20.5.3.3 Security personnel should be supervised as recommended in Section 9.7.

20.6 Critical Infrastructure Protection. Physical plant or digital information needs to be reasonably protected from attacks that cause debilitating loss of operations. Critical infrastructure includes but is not limited to electrical power, gas and oil

networks, telecommunications, banking and finance, transport, government operations, emergency services, and water supply systems.

20.6.1 Chemical Facilities.

20.6.1.1 Because of today's increased concerns about terrorism and sabotage, industrial facilities that handle chemicals should pay increased attention to the physical security of facility sites, chemical storage areas, and chemical processes. All industrial companies, big and small, should have site security programs in place to minimize security vulnerabilities and to protect company assets. This is especially true for facilities that handle extremely hazardous substances.

20.6.1.2 The Environmental Protection Agency (EPA) has developed Risk Management Program (RMP) regulations that require facilities to examine their chemical accident risk and to develop a plan to address the reduction of the risk of criminally caused releases, the vulnerability of facilities to criminal and terrorist activity, and the security of transportation of listed toxic and flammable substances.

20.6.1.3 Considering inherent safety in the design and operation of any facility will have the benefit of helping to prevent or minimize the consequences of a release caused by criminal activity.

20.6.1.4 Some chemicals can be particularly attractive targets because of the potential for greater consequences.

20.6.1.5 Sites in densely populated areas, because of the number of people that would be exposed to a release, might need more security than those at a distance from populations.

20.6.1.6 Facility Design. A well-designed facility, by its layout, limits the possibility that equipment will be damaged and, by its process design, limits the quantity of chemical that could be released. Facility and process design (including chemicals used) determine the need for safety equipment, site security, buffer zones, and mitigation planning. To the extent practicable, eliminating or reducing any hazardous materials during facility or process design is generally preferable to simply adding safety equipment or security measures later.

20.6.1.6.1 Locating processes with hazardous chemicals in the center of a facility can limit the ability of criminals (saboteurs or vandals) to cause harm from outside the facility. Transportation vehicles, which are usually placarded to identify the contents, can be particularly vulnerable to attack if left near the fence line or unprotected. However, for some facilities and processes, the option of locating the entire process at the center of the site is not feasible. Consideration should be given to external versus internal threats, such as the threat to workers if an accidental release occurs, or the access to the process in case of an emergency response.

20.6.1.6.2 Where feasible, providing layers of security will protect equipment from damage. These layers could include passive barriers to resist vehicle attacks or blast-resistant buildings or structures. Enclosing critical valves and pumps behind fences or in buildings can make it less likely that an intruder will be able to reach them or that a vehicle will be able to accidentally collide with them.

20.6.1.6.3 Chlorine tanker valves are an example of equipment design with several layers of security. With the following security measures, as many as three different tools would be needed to breach the container's integrity:

(1) A heavy steel dome with lid
(2) A heavy cable sealing system that requires cable cutters to remove
(3) A heavy-duty valve that can withstand abuse without leaking
(4) A seal plug in each valve

20.6.1.6.4 Consideration should be given to protecting equipment containing hazardous chemicals against sabotage and accidents.

20.6.1.6.5 The idea of layers of security should also be applied to communications and computer security, particularly if processes are computer controlled. Alternative or backup capabilities to protect the communications and computer systems should be developed. Access to computer systems used to control processes should be controlled to prevent unauthorized intrusion. Computer authentication and authorization mechanisms on all computer systems and remote access should be implemented. Entrance into control rooms should be monitored and limited to authorized personnel. For emergency communications, some companies use radios and cell phones as a backup to the regular phone system. Backup power systems and air-conditioning systems are also important.

20.6.1.6.6 Well-designed equipment will usually limit the loss of materials if part of a process fails. Excess flow check valves, for example, will stop flow from an opened valve if the design flow rate is exceeded. These valves are commonly installed on chlorine tank cars and some anhydrous ammonia trailers, as well as on many chemical processes. Like excess flow valves, fail-safe systems can ensure that if a release occurs, the valves in the system will close, shutting off the flow. Breakaway couplings, for example, shut off flow in transfer systems, such as loading hoses, to limit the amount released to the quantity in the hose.

20.6.1.6.7 If hazardous liquids are stored, containment systems (e.g., buildings, dikes, and trenches) should be used to slow the rate at which the chemical evaporates and to provide time for response. Double-walled vessels can also protect against attempts to rupture a tank.

20.6.1.6.8 The installation of chemical monitors that automatically notify personnel of off-hour releases could be important if the facility is not staffed during certain periods (e.g., overnight). Such monitors, however, are not available for all chemicals. The appropriateness of monitors and any other equipment design solutions will depend on site-specific conditions.

20.6.1.7 A 10-Step Threat Analysis and Mitigation Procedure. In response to increasing concerns about chemical terrorism in the United States, the Agency for Toxic Substances and Disease Registry (ATSDR) developed a 10-step procedure to assist local public health and safety officials in analyzing, mitigating, and preventing such hazards. The 10 steps are as follows:

(1) Identify, assess, and prioritize threats.
(2) Identify local sources of chemicals that can be used in improvised weapons.
(3) Evaluate potential exposure pathways.
(4) Identify potential acute and chronic health impacts.
(5) Estimate potential impacts on infrastructure and the environment.
(6) Identify health risk communication needs.
(7) Identify methods to mitigate potential hazards.
(8) Identify specific steps to prevent the use of industrial chemicals as improvised weapons.

(9) Incorporate the threat assessment, mitigation, and prevention information into emergency response plans.
(10) Conduct training exercises to prepare to prevent and mitigate the health threats.

20.6.2 Water Treatment Facilities.

20.6.2.1 Supply interruptions include the destruction of or interference with reservoirs, reservoir dams, water towers or storage facilities, pumping stations, intakes, valves, treatment plants, wells, distribution systems, or fire hydrants.

20.6.2.1.1 Supply interruptions can be caused by any number of acts, including physical destruction, interruption of the supervisory control and data acquisition system, or acts that could reduce the water pressure in a system.

20.6.2.1.2 Supply interruptions can also occur as an indirect result of contamination.

20.6.2.2 Water treatment facilities should comply with the procedures in 20.6.2.2.1 through 20.6.2.2.3.

20.6.2.2.1 Facilities (treatment plants, reservoirs, reservoir dams, water storage facilities and towers, pumping stations, water intake facilities, chlorine booster stations, and meter and valve boxes) should be reasonably protected.

20.6.2.2.2 Supervisory control and data acquisition systems for monitoring and controlling water parameters should be protected against hacking. Computer information security should be enhanced, and passwords should be changed regularly.

20.6.2.2.3 Water authorities should reasonably ensure that fire hydrants and other entry points to the distribution system are tamper resistant.

20.6.3 Power Distribution Facilities. See NFPA 70, *National Electrical Code.*

Chapter 21 Parking Facilities

21.1 General.

21.1.1 A parking facility is a structure or space where the primary use is storage of vehicles.

21.1.2 Crime in parking garages and parking lots is a serious concern, and liability for the injuries suffered by patrons due to third-party criminal activity is a significant exposure for owners and operators of parking facilities. Owners and operators of parking facilities must take proactive measures to reduce crime and security liability exposures.

21.2 Application.

21.2.1 General. This chapter addresses measures to control security vulnerabilities in parking facilities.

21.2.2 Legislation. Some municipalities have enacted legislation that provides specific security requirements for commercial parking facilities.

21.3 Security Plan and Security Vulnerability Assessment.

21.3.1 Development. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

21.3.2 Special Considerations. In performing an SVA of a parking facility, the following sections should be reviewed for applicability and consideration.

21.4 Security Policies and Procedures. The elements of a security program for a parking facility can include the following:

(1) Facility design
(2) Security measures
(3) Training
(4) Signs
(5) Security reviews

21.4.1 Facility Design.

21.4.1.1 Consideration of All Deterrents. Typically, management response to a crime problem is to install security devices, such as alarms, cameras, and access control systems. These are all visible "signs of security" and do serve to deter crime. Nonetheless, management must consider all the deterrents available. These include adequate lighting, secure perimeters, secure elevators and stairwells, elimination of hiding spaces, and good visibility throughout all parking levels.

21.4.1.2 Crime Prevention Through Environmental Design.

(A) Security for a parking facility should be viewed with respect to the concept of crime prevention through environmental design (CPTED). Research in the 1960s indicated a correlation between crime and the design of buildings and areas. CPTED uses access control and natural surveillance to reinforce the legitimate use of the environment and minimize the opportunity for crime.

(B) The four major principles of CPTED, which are intended to work together to create a safe and secure environment, are as follows:

(1) Movement control, which is the directing of the movement of people and vehicles by utilizing security hardware and barriers, both real and symbolic
(2) Surveillance, which is the creating of visibility, thereby increasing the opportunity to observe and discourage intruders
(3) Activity support, which is the creating of conditions and situations for people to interact in a friendly manner, which discourages criminal opportunity
(4) Motivation reinforcement, which is the enacting of positive attitudes about living and working environments

(C) Criminals generally prefer not to be seen. Where CPTED principles are applied, the areas and locations that provide concealment for the criminal can be eliminated. CPTED also increases the ability of persons to observe their surroundings, which encourages the use of the area by authorized users and discourages potential criminals.

(D) The best time to implement CPTED principles is during the planning stages of the construction project. With properly designed facilities, potential opportunities for crime can be eliminated. It is also during the planning stage that security systems and equipment are most cost effectively applied. CPTED can also be implemented in existing structures. An analysis using CPTED concepts can pinpoint complex as well as simple solutions that might have been overlooked.

(E) The facility should be designed with as few structural obstacles as possible to eliminate blind spots. Where allowed by building codes, stairwells should be open or glass-enclosed to enhance visibility. Designs that limit the use of solid walls and provide for open spaces between levels provide guard patrols and attendants with enhanced visibility. The interior of the facility should be painted in light colors to increase reflective-

ness. Parking areas should be well marked, so patrons can easily remember where they left their cars.

(F) Entrances and exits to the parking facility should be as few in number as practicable and attended at all times. The preferred method of controlling access to the facility is to have one means of entry and exit for vehicles; the volume of traffic at the facility, however, can require more than one entry and exit. All exterior doors should be securely locked in compliance with the requirements of local building, fire prevention, and life safety codes.

(G) Implementing CPTED principles is more than just applying a checklist of security solutions. CPTED stresses that all environments are different and that each must be analyzed individually. The security program, therefore, needs to be tailored to the type of parking facility that is being protected, be it multilevel, above ground, underground, or open and at street level.

21.4.2 Security Measures. A number of other basic measures should be considered in the development of a security program for a parking facility.

21.4.2.1 Perimeter Protection.

(A) Landscaping serves the primary purpose of aesthetics, but it can also create security problems. Shrubbery can provide concealment for criminals when it is allowed to become overgrown, and trees can serve as a means for scaling fences if they are planted too close to the fence line. Shrubbery should be kept to a maximum of 3 ft in height and trees trimmed so that the bottom branches are a minimum of 7 ft above the ground. This will provide a clear zone of approximately 4 ft between the top of the shrubbery and bottom branches of the trees for surveillance purposes.

(B) Fencing can be a means of establishing security. Fencing at the perimeter of a parking lot will discourage unauthorized access to the facility and can deter the opportunistic criminal. For parking garages, the ground floor and, if easily accessible, the second level of the structure should be completely enclosed. Screening that reaches from floor to ceiling is preferred to solid walls, since screening provides for visibility into the structure from the street and can serve as a deterrent to criminal activity.

21.4.2.2 Lighting.

(A) Lighting is basic to any security program. In many municipalities, local ordinances and building codes mandate minimum lighting requirements. IESNA RP-20, *Lighting for Parking Facilities,* provides recommended illumination levels for parking facilities.

(B) Entrances, exits, elevators, stairwells, walkways, and parking areas should be illuminated for both safety and security. The interior lighting should provide bright and shadow-free areas. As a means of maintaining lighting levels, damaged lighting fixtures and burned-out bulbs should be replaced as soon as possible and a maintenance program instituted to ensure that all fixtures are cleaned on a regular basis.

21.4.2.3 Access Control.

(A) For public facilities, all entering and exiting vehicles and pedestrians should be required to pass by constantly attended cashiers' plazas. Cashiers' enclosures should be designed to allow 360-degree visibility. Hydraulic or motorized drop-arm gates can be used to control entry and exit of vehicles.

(B) Roll-down grilles should be provided to completely secure a plaza when it is not attended. If public restrooms are provided, they should be located near the cashiers' plaza or in an open, well-traveled area.

(C) For private facilities, a solid overhead garage door, operated by an access control system, should be provided. Once a car has entered or exited, the door should close automatically. Tenants or employees should be advised to wait until the garage door has closed completely before proceeding, to deter furtive attempts at entry by unauthorized individuals. Issuance of ID credentials should be controlled.

21.4.2.4 Security Equipment. Video surveillance can be effective in deterring criminal activity. If utilized, a video surveillance system can cover entrances, exits, entrance ramps, elevators, stairwells, walkways, and parking areas. Fake cameras should not be used, since they give a false sense of security. Video surveillance can also enhance the effectiveness of security personnel. A duress alarm system or two-way intercom system can also be utilized. Duress alarm device buttons can be located at strategic locations throughout the facility, including elevators, stairwells, and parking areas, with prominent signs posted showing their locations. The duress alarm system and intercom system can be integrated with the video surveillance system for enhanced effectiveness of the systems. The systems should be readily accessible to all users, including persons with disabilities.

21.4.2.5 Security Personnel and Patrols. Patrols of the perimeter and interior areas of the facility by security personnel should be at irregular intervals. These patrols should be supervised as recommended in Chapter 9. Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension. Security personnel or attendants should be provided with two-way radios, and patrol personnel should be in uniform. Escort services to cars can be made available to all patrons at their request. If the service is available, signs should be posted so advising patrons.

21.4.3 Training. Training of personnel is a part of any security program. Personnel should be trained to deal with on-duty responsibilities and emergencies. Further, security personnel and employees with specific security duties should have training relating to crime response.

21.4.4 Security Reviews. Periodic reviews of security procedures should be performed. Management should also review all security-related incidents and complaints and how they were resolved.

21.5* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references should be done on all individuals with access to critical assets *(see Chapter 10).*
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Chapter 22 Special Events

22.1 Planning for Special Events. Colleges, universities, office complexes, museums, and other private properties generally will have a security program to deal with normal, daily activities. There can be occasions, however, when these properties will be the scene of a special event, such as a concert, athletic event, art exhibit, or visit by a VIP, at which large crowds are expected. For such events, a security program should be implemented to control the crowds and avoid panic in the event of an emergency. When the event takes place on public property, security is generally the responsibility of law enforcement. On private property, property managers are responsible for security, although the participation and cooperation of law enforcement might be required. Also, even when a large event takes place on public property, there can be a spillover onto surrounding private property, creating unplanned-for security exposures. This section outlines the elements of a security program for managing a special event on private property.

22.2 Security Plan and Security Vulnerability Assessment. A security plan, as described in Chapter 10, should be developed. A security vulnerability assessment (SVA), as detailed in Chapter 5, should be conducted.

22.3 Security Program. Behind every successful event is a security and crowd control program. The key to making the program successful is planning and preparation. While a facility can have a general security and crowd control program in place, the program should be tailored to meet the needs of each specific event. In performing an SVA for a special event, the following sections should be reviewed for applicability and consideration.

22.3.1 Security Committee.

(A) If the magnitude of the special event warrants, a security committee should be established and should consist of representatives from facility management, risk management, safety, support personnel (ushers, ticket sales personnel, etc.), event promoters, and security. A security coordinator should be appointed, and all matters dealing with security at the event should be communicated through this individual.

(B) The committee should meet on a regular basis to review plans for the event, discuss problems, and report progress. Following the full committee meetings, individual departments should meet to review their needs and requirements.

(C) The security committee should review experiences with prior events to determine what worked, what did not, what problems were experienced, and how similar problems could affect the present event.

22.3.2 Statement of Purpose. The committee should develop a statement of purpose to provide focus for the security program. An example of a statement of purpose is: "The goal of security for this event is to provide spectators or visitors, participants, and support personnel with a safe and secure environment in which to enjoy the activity, with contingency plans in place to address any concerns that can arise before, during, or after the event."

22.3.3 Event Planning Measures.

22.3.3.1 Personnel.

(A) Police officers can be employed to meet security personnel needs; however, police officers can be called away, even during the event, to handle an emergency elsewhere *(see Chapter 9 for guidance on security personnel).*

(B) Special events can also require the hiring of temporary workers to assist in handling concessions, custodial services, and other nonsecurity tasks. Because of the short-term need for these workers, they are generally hired without undergoing any background or reference checking. One solution to this problem is to hire temporary workers only from agencies that perform background checks.

(C) The type of event (rock concert, art exhibit, etc.) and the estimated crowd size will determine the number of crowd control personnel (security personnel and law enforcement personnel, as well as ushers and ticket takers). The event planners or sales personnel should keep the security committee informed on a regular basis on the latest projected attendance figures, and staffing needs should be adjusted accordingly. While there are no rules to determine the number of crowd control personnel required at an event, a review of past events can provide a benchmark for making a determination.

(D) The telephone number for contacting emergency medical services (EMS) personnel should be readily available for all events. At large events (crowds larger than 10,000 people), EMS personnel should be on-site. Crowd control and security personnel should be instructed on how to initiate a medical response.

22.3.3.2 ID Badges. Event staff should be provided with picture ID cards that are worn visibly at all times. These cards can also function as access control cards. Temporary staff should be provided with temporary ID cards. These cards should be of a distinct and easily noticed color and should be worn at all times.

22.3.3.3 Access Control. Access control at exterior entrances and loading docks is an important consideration before and during an event. All exterior doors, except those used for visitor entrance, should be kept locked at all times, in accordance with life safety code requirements. Employees should be required to enter the facility through a controlled employee entrance. Admittance can be automated through the use of an access control system.

22.3.3.4 Control Center. Consideration should be given to establishing a control center to serve as a central communication point for coordination of all activities related to the event. Representatives from security, law enforcement, EMS, and facility management should be assigned to the center, which should be centrally located within the facility. Communication for security personnel can be by portable radio or other means.

22.3.3.5 Parking and Traffic Control.

(A) Parking and traffic control play integral roles in the success of an event, since delays caused by either can result in delays in crowd ingress, which could delay the start of the event. Traffic control can also greatly affect crowd egress. For events at which a large volume of cars is expected, law enforcement should be requested to provide traffic control on local roads.

(B) Based on the projected attendance, a determination can be made if there will be sufficient parking on the property. If on-site parking is insufficient, it might be necessary to provide for satellite parking. Providing transpiration to and from the satellite parking, as well as safety, security, and traffic control at the satellite parking, should also be addressed.

(C) Close-proximity parking problems can also affect emergency medical assistance plans. Parking areas must be monitored to ensure that emergency vehicles have access to and from the

facility. Also, a few vehicles parked in the wrong areas can create chaos both when guests are arriving and when they are leaving.

22.3.4 Ingress and Egress.

22.3.4.1 General.

(A) Since most patrons (visitors) arrive within 20 minutes before the start of an event, staffing needs for ticket personnel and/or gate personnel are greatest during this period. Once the event starts and the ingress traffic slows, staffing levels can be reduced and personnel reassigned to patrols or elsewhere.

(B) In the event of an emergency, a plan must be in place to facilitate the orderly exiting of the crowd from the facility; gate personnel should be readily contacted so they can assist in the effort. Life safety will require that means be provided for guests or patrons to exit the facility throughout the event. Emergency exits should allow for the free flow of the crowd from the facility.

(C) If turnstiles or gates are used during crowd ingress and these same portals are used for egress, at the end of the event the turnstiles and gates should be opened to facilitate the exiting crowds. While most of the crowd will exit at the end of an event, it is common, especially during athletic events, for a large portion of the crowd to begin leaving before the event ends.

22.3.4.2 Entry Screening. Entry screening can range from visual inspection and bag searches of suspicious people to searches by metal detectors and hand-held wands of all people. The goal of the screening is to remove items that can turn into dangerous missiles or weapons. The history of past events (rock concerts as compared to art exhibits) can help to determine the level of screening used. Patrons who refuse the search should be denied entry.

22.3.5 Patrols. Security personnel should be assigned to patrol the crowd during the event. Patrols serve as the eyes and ears for the staff in the control center. Patrols should check in on a regular basis to the communications center.

22.3.6 Other Considerations.

(A) Bomb threats are often used by disgruntled employees and others to disrupt an event. They have also become the weapon of choice for terrorists. A plan should be in place for handling bomb threats as well as procedures for evacuating a facility and conducting bomb searches.

(B) Special events also present an opportune time for groups to express their views through a public demonstration. These demonstrations can occur without any forewarning and, at times, escalate to violence. Local law enforcement should be contacted immediately at the first sign of a demonstration.

22.4 Handling Disturbances, Ejections, and Arrests. Event planners should develop policies and procedures as a means of providing staff with guidelines on how to handle disturbances. Staff should also be trained regarding actions that can be taken within the limits of the law in dealing with disturbances and, in particular, in ejecting or arresting spectators. Event planners should request assistance from the local police in training staff on the proper procedures to follow in ejecting a spectator or making an arrest. The following are some suggested guidelines for staff to follow:

(1) An incident report should be filed on actions taken by staff immediately after an incident has occurred.
(2) Staff should stay calm and speak clearly when dealing with those involved in the disturbance. They should also avoid being patronizing or aggressive, since these attitudes can lead to an escalation in the situation. Staff must keep a level head about what is taking place.
(3) If alcohol will be served at the event, policies should be developed and staff trained in serving alcohol and in handling intoxicated patrons.
(4) If it appears that a fight or altercation might take place between patrons, staff should immediately call for help. Depending on the circumstance, it is generally preferred that staff wait until help arrives before attempting to quell the disturbance. If possible, staff should remain in contact with the control center throughout the disturbance.
(5) One action staff can take in handling any disturbance is to ask the individual(s) involved to comply with policies.
(6) Patrons who are uncontrolled, who exhibit rowdy behavior or endanger the safety of others, or who fail to cooperate with the repeated requests of staff should be ejected from the event.
(7) A plan should be developed to respond to physical disturbances.
(8) Law enforcement should handle all ejections and arrests, since they are usually more experienced in the proper procedures to follow.

22.5* Employment Practices. Employers can ensure a high level of integrity in the workforce by considering the following practices:

(1) Background checks, including criminal records checks, employment history, and references should be done on all individuals with access to critical assets *(see Chapter 10)*.
(2) When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

Annex A Explanatory Material

Annex A is not a part of the recommendations of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.3.2.1 Approved. The National Fire Protection Association does not approve, inspect, or certify any installations, procedures, equipment, or materials; nor does it approve or evaluate testing laboratories. In determining the acceptability of installations, procedures, equipment, or materials, the authority having jurisdiction may base acceptance on compliance with NFPA or other appropriate standards. In the absence of such standards, said authority may require evidence of proper installation, procedure, or use. The authority having jurisdiction may also refer to the listings or labeling practices of an organization that is concerned with product evaluations and is thus in a position to determine compliance with appropriate standards for the current production of listed items.

A.3.2.2 Authority Having Jurisdiction (AHJ). The phrase "authority having jurisdiction," or its acronym AHJ, is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a

federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his or her designated agent assumes the role of the authority having jurisdiction; at government installations, the commanding officer or departmental official may be the authority having jurisdiction.

A.3.2.5 Listed. The means for identifying listed equipment may vary for each organization concerned with product evaluation; some organizations do not recognize equipment as listed unless it is also labeled. The authority having jurisdiction should utilize the system employed by the listing organization to identify a listed product.

A.3.3.1 Access Control. Access control portals are doors, gates, turnstiles, and so forth. Controls can be operational, technical, physical, or a combination thereof and can vary depending on type of credential, authorization level, day, or time of day.

A.3.3.2 Accessible Opening. An accessible opening has a clear cross-section area of 96 in.^{2} (619 cm^2) or more, with the smallest dimension exceeding 6 in. (15.2 cm), and conforms to the following dimensions:

(1) 18 ft (5.5 m) or less from the ground or the roof of an adjoining building
(2) 14 ft (4.3 m) or less from a directly or diagonally opposite window, fire escape, or roof
(3) 3 ft (0.9 m) or less from an opening, fire escape, ladder, and the like, that is in or projecting from the same or adjacent wall and leads to other premises

A.3.3.3.1 False Alarm. A false alarm may result from a fault or problem in the system, from an environmental condition, or from operation by the user of the system causing an unwanted condition.

A.3.3.3.2 Holdup Alarm. A holdup alarm is a high priority alarm condition that signals a dangerous situation, such as a robbery. It is usually a silent alarm to protect the cashier.

Often these silent alarms are triggered either by a holdup-initiating device such as a keypad code or from a safe when a holdup code is entered by the user in lieu of the standard code. Holdup alarms are designed to silently initiate an alarm that is annunciated at a remote station or guard post. A holdup alarm is intended to be activated by the user covertly during a robbery.

A.3.3.3.3 Local Alarm. The alarm usually uses a bell, siren, lighting system, or combination of such devices. It usually turns off automatically after a preset time, although some require a manual shutoff. A local alarm can also be linked to a monitoring station or other remote location.

A.3.3.4 Annunciator. An annunciator can log alarms or display a continuous status of devices or systems. The annunciator can signal audibly, visually, or both to indicate a change of status.

A.3.3.5.1 Controlled Area. Admittance to a controlled area is limited to persons who have official business within the area.

A.3.3.5.3 Restricted Area. Admittance to a restricted area is limited to personnel assigned to the area or persons who have been specifically authorized access to the area. Visitors to a restricted area and uncleared personnel should be escorted by personnel assigned to the area, and all confidential information should be protected from observation, disclosure, or removal.

A.3.3.7 Capacitance Sensor. The protected object must be metal, electrically charged, and insulated from electrical ground potential.

A.3.3.13.1 Duress Alarm Device. A perceived hostile situation might be an intruder. Often these alarms are triggered by unobtrusive sensors so as to not place the victim in increased danger. Duress alarms are usually designed to silently initiate an alarm, which is annunciated at a remote station or guard post.

A.3.3.19 Foil. Foil is a thin metallic strip between 0.0254 mm (0.001 in.) and 0.00762 mm (0.0003 in.) in thickness and from 3.175 mm (0.125 in.) to 25.4 mm (1.0 in.) in width. Foil, also known as tape, is commonly used on windows and other installations. When the foil breaks and opens the electrical circuit, it causes an alarm condition.

A.3.3.26 Identification Credential. Biometric identifiers can include unique personal characteristics (fingerprint or retinal scan) or individual behavior characteristic (how a person signs his/her name).

A.3.3.27.1 Confidential Information. It includes commercial secrets, personal secrets, artistic secrets, and state secrets (classified information). The terms *confidential information* and *trade secrets* are often used interchangeably, but, strictly speaking, trade secrets are a subset of confidential information in the context of business, commerce, or trade. Examples of confidential information include the following:

(1) Social security numbers
(2) Trade secrets or intellectual property (e.g., manufacturing processes, recipes, engineering and technical designs and drawings, product specifications, customer lists, business strategies, and sales and marketing information)
(3) Birth dates
(4) Health records
(5) Location of assets
(6) Passwords
(7) Legal investigations
(8) Sealed bids

A.3.3.31 Line Supervision. Various methods can be used for line supervision such as the following:

(1) Current monitoring. A known current is placed on the line. Cutting or shorting the line changes this current, which results in an alarm.
(2) Signaling techniques. These include random tone patterns, multiplexing, authentication, data encryption, and the like.

A.3.3.33.1 Bar Lock. Turning a key or bolt on the center element retracts the bars enough to let the door open. A door with a bar lock cannot be pulled out of its frame even if the hinge pins are removed.

A.3.3.33.2 Electromagnetic Lock. Electromagnetic locks use no moving parts.

A.3.3.34 Microwave Sensor. Microwave sensors are classified as either monostatic, bistatic, or terrain following. Generally, they use the Doppler effect to recognize movement within a protected area. Bistatic sensors operate on a beam break principle. Terrain-following microwave sensors are essentially bistatic sensors with antenna configurations that are not overall line-of-sight. Monostatic sensors are typically designated for