NFPA®

730

Guide for Premises Security

2018

NFPA®

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA STANDARDS

NFPA® codes, standards, recommended practices, and guides ("NFPA Standards"), 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 NFPA 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 NFPA Standards. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Standards 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 NFPA Standards. 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.

REVISION SYMBOLS IDENTIFYING CHANGES FROM THE PREVIOUS EDITION

Text revisions are shaded. A Δ before a section number indicates that words within that section were deleted and a Δ to the left of a table or figure number indicates a revision to an existing table or figure. When a chapter was heavily revised, the entire chapter is marked throughout with the Δ symbol. Where one or more sections were deleted, a • is placed between the remaining sections. Chapters, annexes, sections, figures, and tables that are new are indicated with an *N*.

Note that these indicators are a guide. Rearrangement of sections may not be captured in the markup, but users can view complete revision details in the First and Second Draft Reports located in the archived revision information section of each code at www.nfpa.org/docinfo. Any subsequent changes from the NFPA Technical Meeting, Tentative Interim Amendments, and Errata are also located there.

REMINDER: UPDATING OF NFPA STANDARDS

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that NFPA Standards may be amended from time to time through the issuance of a Tentative Interim Amendment (TIA) or corrected by Errata. An official NFPA Standard at any point in time consists of the current edition of the document together with any TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of Tentative Interim Amendments or corrected by Errata, go to www.nfpa.org/docinfo to choose from the list of NFPA Standards or use the search feature to select the NFPA Standard number (e.g., NFPA 13). The document information page provides up-to-date document-specific information as well as postings of all existing TIAs and Errata. It also includes the option to register for an "Alert" feature to receive an automatic email notification when new updates and other information are posted regarding the document.

ISBN: 978-145591703-7 (Print)
ISBN: 978-145591704-4 (PDF)
ISBN: 978-145591786-0 (eBook)

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Standards

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") 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 or corrected by Errata. An official NFPA Standard 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 Standards

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing the Development of NFPA Standards 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 referenced in, related to, or asserted in connection with an NFPA Standard. The users of NFPA Standards bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Standards.

NFPA adheres to the policy of the American National Standards Institute (ANSI) regarding the inclusion of patents in American National Standards ("the ANSI Patent Policy"), and hereby gives the following notice pursuant to that policy:

NOTICE: The user's attention is called to the possibility that compliance with an NFPA Standard may require use of an invention covered by patent rights. NFPA takes no position as to the validity of any such patent rights or as to whether such patent rights constitute or include essential patent claims under the ANSI Patent Policy. If, in connection with the ANSI Patent Policy, a patent holder has filed a statement of willingness to grant licenses under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, copies of such filed statements can be obtained, on request, from NFPA. For further information, contact the NFPA at the address listed below.

Law and Regulations

Users of NFPA Standards 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

NFPA Standards are copyrighted. They are made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making these documents available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to these documents.

Use of NFPA Standards for regulatory purposes should be accomplished through adoption by reference. The term "adoption by reference" means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA Standards, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Standards 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 standards 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; email: stds_admin@nfpa.org.

For more information about NFPA, visit the NFPA website at www.nfpa.org. All NFPA codes and standards can be viewed at no cost at www.nfpa.org/docinfo.

NFPA® 730

Guide for

Premises Security

2018 Edition

This edition of NFPA 730, *Guide for Premises Security,* was prepared by the Technical Committee on Premises Security and acted on by NFPA at its June Association Technical Meeting held June 4–7, 2017, in Boston, MA. It was issued by the Standards Council on August 17, 2017, with an effective date of September 6, 2017, and supersedes all previous editions.

This edition of NFPA 730 was approved as an American National Standard on September 6, 2017.

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 was updated to add new requirements for industrial security. Specifically, new material was added for the protection of water treatment facilities. Other changes reflected corrections, updated references, and clarifications.

The 2011 edition updated many of the references. The guide also added more material on crime prevention through environmental design (CPTED). The majority of the other changes were editorial in nature.

The 2014 edition was revised to update many of the referenced publications. Section 4.3 was revised to clarify some of the requirements of security planning, including the prioritization of risks identified in the security vulnerability assessments (SVA) and the frequency of when to review and update the SVA. This edition also added a graph that could be used as a guide to sort the risks identified in the SVA. The responsibility for the SVA was clarified, and other changes relative to the qualifications of the SVA provider were addressed. Section 8.4 also was revised to further detail both the need and criteria for protective lighting.

The major changes to the 2018 edition include the following:

(1) All definitions in Chapter 3 were reviewed and correlated with those of NFPA 731, *Standard for the Installation of Electronic Premises Security Systems.*
(2) The term *key* was replaced by *key/credential* throughout the document to provide for more modern technology such as access control cards and other means for unlocking or locking doors.
(3) Subsections 5.2.3 and 5.3.2 pertaining to security planning and SVAs were revised to recognize that there are comparable security risk assessment methodologies and to provide guidance for certification organizations in security or crime prevention.
(4) The terms *lockdown*, *lockout*, and *shelter-in-place* were added. Paragraph 11.1.3.2 pertaining to educational facilities, colleges, and universities was revised to provide for education and training for these conditions and to provide for semiannual security-related drills. Paragraph 11.2.1.3 addresses visitor identification. Paragraph 11.3.4.6 provides criteria for exterior portal windows and sidelights.

Technical Committee on Premises Security

James P. Simpson, *Chair*
Electrical Training Alliance, MN [L]
Rep. International Brotherhood of Electrical Workers

David Abbott, Ohio State University, OH [U]

Sean A. Ahrens, Jensen Hughes/AON Fire Protection Engineering, IL [I]

Randall I. Atlas, Atlas Safety & Security Design, Inc., FL [IM]

George Bish, MasTec, NC [IM]
Rep. Electronic Security Association

Josh D. Brown, The Fauquier Bank, VA [U]
Rep. Virginia Crime Prevention Association/National Crime Prevention Council

Louis Chavez, UL LLC, IL [RT]

David S. Collins, The Preview Group, Inc., OH [SE]
Rep. American Institute of Architects

Stephen B. Coppola, Vivint, MA [IM]
Rep. Central Station Alarm Association

David A. Dagenais, Wentworth-Douglass Hospital, NH [U]
Rep. NFPA Health Care Section

Michael D. DeVore, State Farm Insurance Company, IL [I]

Daniel P. Finnegan, Siemens Industry, Inc., IL [M]

Louis T. Fiore, L. T. Fiore, Inc., NJ [IM]
Rep. Professional Alarm Services Organizations of North America

Charles E. Hahl, GHD Inc., VA [SE]

Charles B. King, III, U.S. Department of Homeland Security, VA [E]

Jerry D. Loghry, EMC Insurance Companies, IA [I]

Scott Lord, All Systems Designed Solutions, KS [IM]
Rep. Partner Alliance for Safer Schools

Anthony Mucci, Tyco Integrated Security, FL [M]

James Murphy, Vector Security Inc., PA [IM]

Kevin Patterson, Bosch Security Systems, NY [M]
Rep. National Electrical Manufacturers Association

Michael C. Peele, Georgetown University, VA [U]

Tom G. Smith, Oklahoma City, OK [IM]
Rep. National Electrical Contractors Association

Robert H. Stagg, Guardsmark, LLC, NC [SE]

Barry Stanford, AEG, CA [U]

Michael Tierney, Kellen Company, CT [M]
Rep. Builders Hardware Manufacturers Association

William F. Wayman, Jr., JENSEN HUGHES, MD [SE]

Alternates

Douglas P. Bassett, XFinity Home, FL [IM]
(Alt. to George Bish)

Shane M. Clary, Bay Alarm Company, CA [IM]
(Alt. to Stephen B. Coppola)

Mark A. Farus, Siemens Industry, Inc., GA [M]
(Alt. to Daniel P. Finnegan)

Patrick D. Harris, National Crime Prevention Association, VA [U]
(Alt. to Josh D. Brown)

Gordon G. Hope, Jr., Honeywell, Inc., NY [M]
(Alt. to Kevin Patterson)

Bruce E. Johnson, UL LLC, NY [RT]
(Alt. to Louis Chavez)

Mark I. Morrison, State Farm Insurance Company, IL [I]
(Alt. to Michael D. DeVore)

Douglas Quick, Tyco/SimplexGrinnell, GA [M]
(Alt. to Anthony Mucci)

Kurt A. Roeper, ASSA ABLOY, CT [M]
(Alt. to Michael Tierney)

James W. Tosh, IBEW Local 46, WA [L]
(Alt. to James P. Simpson)

Richard J. Roux, 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

2018 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 Standards." They can also be viewed at www.nfpa.org/disclaimers or obtained on request from NFPA.

UPDATES, ALERTS, AND FUTURE EDITIONS: New editions of NFPA codes, standards, recommended practices, and guides (i.e., NFPA Standards) are released on scheduled revision cycles. This edition may be superseded by a later one, or it may be amended outside of its scheduled revision cycle through the issuance of Tentative Interim Amendments (TIAs). An official NFPA Standard at any point in time consists of the current edition of the document, together with all TIAs and Errata in effect. To verify that this document is the current edition or to determine if it has been amended by TIAs or Errata, please consult the National Fire Codes® Subscription Service or the "List of NFPA Codes & Standards" at www.nfpa.org/docinfo. In addition to TIAs and Errata, the document information pages also include the option to sign up for alerts for individual documents and to be involved in the development of the next edition.

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

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 G. Extracted text may be edited for consistency and style and may include the revision of internal paragraph references and other references as appropriate. 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 G.

Chapter 1 Administration

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

Δ **1.1.1** NFPA 730 is referred to herein as "this guide" or "the guide."

1.1.2 This guide should not 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.

1.3 Application. The application of this guide is based on the risk considerations determined in Chapter 5.

1.4 Retroactivity.

1.4.1 This guide applies to both new and existing buildings, structures, and premises.

1.4.2 Existing buildings or installations that do not comply with the provisions of the referenced documents should be permitted to be continued in service.

1.5 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 prescribed by this guide.

1.6 Units and Formulas.

1.6.1 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).

1.6.2 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 the standard; the given equivalent value might be approximate.

1.6.3 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.

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 72®, National Fire Alarm and Signaling Code, 2016 edition.

NFPA *101®, Life Safety Code®,* 2015 edition.

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* 2017 edition.

2.3 Other Publications.

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

ANSI/BHMA A156 Series, *Categories of Builders Hardware.*

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

ANSI/UL 294, *Standard for Access Control System Units*, 2013.

ANSI/UL 305, *Standard for Panic Hardware*, 1997, revised 2012.

ANSI/UL 437, *Standard for Key Locks*, 2013.

ANSI/UL 768, *Standard for Combination Locks*, 2013.

ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*, 2011.

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

UL 2802, *Standard for Performance Testing of Camera Image Quality*, 2014.

2.3.3 Other Publications.

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

2.4 References for Extracts in Advisory Sections.

NFPA 72®, National Fire Alarm and Signaling Code, 2016 edition.

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* 2017 edition.

NFPA 5000®, Building Construction and Safety Code®, 2015 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 act of managing ingress or egress through a portal by validating a credential or an individual. [**731,** 2017]

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. [**731,** 2017]

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

3.3.4* Annunciator. A unit containing one or more indicator lamps, alphanumeric displays, computer monitors, audible indicators, or other equivalent means on which each indication provides status information about a circuit, condition, system, or location. [**731,** 2017]

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

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

3.3.7 Change Key/Credential. See 3.3.27.1.

3.3.8 Confidential Information. See 3.3.25.1.

3.3.9 Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [**72,** 2016]

3.3.10 Controlled Area. See 3.3.5.1.

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

3.3.12 Device.

3.3.12.1* *Duress Alarm Initiating Device.* An initiating device intended to enable a person at a protected premises to initiate a signal indicating a need for assistance. [**731,** 2017]

3.3.12.2 *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. [**731,** 2017]

3.3.13 Duress Alarm Device. See 3.3.12.1.

3.3.14 Duress Alarm System. See 3.3.46.1.

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

3.3.16 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.

3.3.17 Facility Classification.

3.3.17.1 *Educational Facility.* An occupancy used for educational purposes through the twelfth grade by six or more persons for 4 or more hours per day or more than 12 hours per week.

Δ **3.3.17.2*** ***Health Care Facilities.*** Buildings, portions of buildings, or mobile enclosures in which medical, dental, psychiatric, nursing, obstetrical, or surgical care is provided. [**5000,** 2015]

3.3.17.3 ***Industrial Facility.*** A facility in which products are manufactured or in which processing, assembling, mixing, packaging, finishing, decorating, or repair operations are conducted.

3.3.17.4 ***Lodging Facility.*** Facilities that provide housing and generally, but not always, food, beverage, meeting facilities, retail shops, recreational facilities, and other services, including but not limited to hotels, motels, motor hotels, resort hotels, inns, country clubs, and conference centers.

3.3.17.5 ***Multi-Dwelling Unit.*** A facility with more than three dwelling units.

3.3.17.6 ***Office Building.*** A facility used for office, professional, or service-type transactions, including but not limited to storage of records and accounts.

3.3.17.7 ***One- and Two-Family Dwelling.*** Facilities containing one or two dwelling units that are occupied primarily on a permanent basis.

3.3.17.8 ***Parking Facility.*** A structure or space where the primary use is storage of vehicles.

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

3.3.17.10 ***Retail Establishment.*** A facility used for the display and sale of merchandise.

3.3.17.11 ***Shopping Center.*** A group of retail and other commercial establishments that is planned, developed, and managed as a single property.

3.3.18 False Alarm. See 3.3.3.1.

3.3.19* Foil. An electrically conductive ribbon used for a sensing circuit. [**731,** 2017]

3.3.20 Grandmaster Key/Credential. See 3.3.27.2.

3.3.21 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.

3.3.22 Holdup Alarm. See 3.3.3.2.

3.3.23 Holdup Alarm System. See 3.3.46.2.

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

3.3.25 Information.

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

3.3.25.2 ***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.

3.3.26 Intrusion Detection System. See 3.3.47.3.

3.3.27 Key/Credential.

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

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

3.3.28 Keypad. A device that is a type of human/machine interface (HMI) with numerical or function keys that can incorporate an annunciator or a signaling device. [**731,** 2017]

3.3.29* 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.

N **3.3.30 Lockdown.** A state where the building is secured and occupants are sequestered in the nearest safe location and not allowed to move within the building.

N **3.3.31 Lockout.** A state where the perimeter of the building or property is secured for ingress and occupants are free to move within the building.

3.3.32* Machine Readable Credential. A device or scheme containing some knowledge, an identifying credential, or a biometric identifier. [**731,** 2017]

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

3.3.34* 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. [**731,** 2017]

• **3.3.35 National Security Information.** See 3.3.25.2.

Δ **3.3.36 Perimeter Protection.** A scheme of protection that uses devices to detect or deter intrusion into a protected area.

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

• **3.3.38* Reader.** A device that allows a machine readable credential to be entered into an access control system. [**731,** 2017]

3.3.39 Restricted Area. See 3.3.5.2.

3.3.40* Screens. An array of wires usually interwoven every 6 in. (2.5 cm) either horizontally or vertically on a screen or alarm screening that protects areas or openings, such as skylights and crawl spaces. [**731,** 2017]

3.3.41 Security Signaling Device. See 3.3.12.2.

3.3.42* Security Vulnerability Assessment (SVA). A systematic and methodical process for examining ways an adversary might exploit an organization's security vulnerabilities to produce an undesired outcome.

N **3.3.43* Shelter-in-Place.** Occupants within the building remain indoors until given further instructions.

3.3.44 Supervised Lines. Interconnecting lines in an alarm system that are electrically supervised against tampering. *(See also 3.3.29, 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 or portion thereof that connects to duress alarm initiating devices. [**731,** 2017]

3.3.46.2* ***Holdup Alarm System.*** A system or portion thereof that connects to holdup alarm initiating devices. [**731,** 2017]

•

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 (as related to premises security). A fixed-in-place structure with all boundary surfaces constructed of reinforced materials such as poured concrete or engineered modular panels designed for such applications and secured with listed doors and locks. [**731,** 2017]

3.3.50 Zone. A defined area within a protected premise. A zone can define an area from which a signal can be received, an area in which a signal can be sent, or an area in which a form of control can be executed.

Chapter 4 General

4.1 Fundamental Principles.

4.1.1 The primary goals of this guide should be as follows:

(1) To provide an environment for the occupants inside or near a building that is reasonably safe from security threats
(2) To provide reasonable safeguards for protection of property from security threats

4.1.2 Implementing the goals of this guide should require a security plan.

4.1.3 A security plan should address the following security objectives:

(1) Restrict area perimeter — secure and monitor the perimeter of the facility
(2) Secure site assets — secure and monitor restricted areas or potentially critical targets within the facility
(3) Screen and control access — control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including the following:
    (a) Measures to deter the unauthorized introduction of dangerous substances and devices that could facilitate an attack or actions having serious negative consequences
    (b) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures
(4)* Deter, detect, or delay — deter, detect, or delay an attack, creating sufficient time to implement countermeasures between detection of an attack and the point at which the attack becomes successful
(5) Shipping, receipt, and storage — secure and monitor the shipping, receipt, and storage of hazardous materials for the facility
(6) Theft and diversion — deter theft or diversion of assets
(7) Sabotage — deter insider sabotage
(8) Response — develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders
(9) Monitoring — maintain effective monitoring, communications, and warning systems, including the following:
    (a) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained
    (b) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection
    (c) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions
(10) Training — ensure proper security training, exercises, and drills of facility personnel
(11) Personnel surety — perform appropriate background checks on and ensure appropriate credentials for facility personnel and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including the following:
    (a) Measures designed to verify and validate identity
    (b) Measures designed to check criminal history
    (c) Measures designed to verify and validate legal authorization to work
    (d) Measures designed to identify people with terrorist ties
(12) Elevated threats — escalate the level of protective measures for periods of elevated threat
(13) Significant security incidents and suspicious activities — identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site
(14) Officials and organization — establish official(s) and an organization responsible for security and for compliance with these guides
(15) Records — maintain appropriate records

4.1.4 A security plan should include a security vulnerability assessment (SVA).

4.2 Classification of Assets.

4.2.1 Assets should be classified by risk.

4.2.2* The security assessment for assets should be in accordance with the applicable occupancy chapter (Chapters 11 through 20).

4.2.3 Classification of assets should be subject to the ruling of the owner or the owner's designee where there is a question of proper classification in any individual case.

4.3 Security Planning.

4.3.1 The security plan should comply with all of the following:

(1) Chapter 5
(2) Chapters 11 through 20 for the occupancy involved
(3) Chapters 6 through 10 when referenced from Chapters 11 through 20 for the occupancy involved

4.3.2 The SVA should identify the security risks in the physical and operational environment of the organization.

4.3.3* Risks identified in the SVA should be arranged by frequency and severity.

4.3.4 Procedures and controls should be implemented to satisfy all of the following:

(1)* The organization's tolerance to risk
(2) The goals listed in 4.1.1
(3) The objectives listed in 4.1.3

4.4 Security Plan Evaluation.

4.4.1* Periodic drills should be conducted at various times and locations.

4.4.1.1 The drills should be critiqued for plan effectiveness and to identify opportunities for improvement.

4.4.1.2 Identified opportunities for improvement should be incorporated into the security plan.

4.4.2* The review and update of the SVA should be based on the level of risk, threats, crime, and change of conditions within the organization.

4.5 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 adopted codes and standards, including NFPA 731, the manufacturer's specifications, applicable UL standards, the AHJ, and nationally recognized industry standards, guides, and practices.

4.6 Maintenance.

4.6.1 Any device, equipment, system, condition, arrangement, level of protection, or any other feature provided in accordance with this guide, should be maintained to function as installed.

4.6.2* Emergency and security equipment should be repaired on a priority based on the SVA.

4.6.3 A repair log should list repairs, including but not limited to the following:

(1) The system impairment
(2) The time and date of the impairment
(3) Repairs that were completed
(4) The time and date of each repair

4.6.4 Repair logs should be retained for not less than 1 year.

Chapter 5 Security Planning

5.1 General.

5.1.1 The security plan should document the protection of an organization's defined critical assets.

5.1.2 The property building owner, or owner's designated representative should be responsible for the SVA.

5.2 Security Vulnerability Assessment (SVA).

5.2.1* Security planning should begin with an SVA.

5.2.2* An SVA should assess the current status of an organization's vulnerabilities, including but not limited to threat exposures, security features, and preparedness.

Δ **5.2.3** A security vulnerability assessment should utilize a recognized, analytical methodology to assess the security-related risks and vulnerabilities of an organization, its property, and personnel. This assessment should include, but not be limited to the following:

(1)* *Step 1: Formation of team.* Form a team of personnel from pertinent organizational areas and other stakeholders.
(2)* *Step 2: Organization/facility characterization.* Characterize the organization and the facilities to be protected.
(3) *Step 3: Threat assessment.* Classify threats using an assessment process that includes but is not limited to the following:
    (a) Classification of critical assets
    (b) Identification of potential targets
    (c) Consequence analysis (i.e., effect of loss, including potential off-site consequences)
    (d) Definition of potential threats (i.e., identifying potential adversaries and what is known about them)
(4)* *Step 4: Threat vulnerability analysis.* Conduct a threat vulnerability analysis identifying actual and potential threat scenarios and estimate a relative security risk level.
(5)* *Step 5: Define specific security countermeasures.* Define countermeasures using information from the previous four steps, including characterization, threat, and vulnerability analysis.
(6) *Step 6: Assess risk reduction.* Reassess the relative security risk levels developed in Step 4, taking into account the countermeasures defined in Step 5, and implement additional security risk reduction measures (security countermeasures) where appropriate.
(7) *Step 7: Document findings and track implementation.* Document findings and recommendations and track the implementation of accepted recommendations.

5.3 Qualifications.

5.3.1 The SVA provider should provide evidence of its qualifications, education, certification, or experience when requested by the property building owner or the owner's designated representative.

5.3.2* The SVA provider's personnel conducting the SVA should be certified by a nationally recognized certification organization in security or crime prevention.

5.4 Security Plan.

5.4.1 The security plan should include but not be limited to the following *(for special events, see Annex E)*:

(1) Statement of purpose
(2) Organizational policies and procedures
(3) Description of the facility and organizational structure
(4) Security vulnerability assessment, including threat assessments and risks
(5) Instructions for using the plan

(6) Description of the features of protection
(7) Organization's security-related measures and procedures
(8) Information needed to implement the security measures and procedures
(9) List of the intended users of the plan
(10) Plan distribution list
(11) Location of the master copy
(12) Organization for security operations
(13) Procedures for employee, visitor, and vendor safety

5.4.2 Plan components should be based on the potential threats facing the organization or facility as determined by the SVA.

5.4.3 The objectives of the security plan should be specific, measurable, achievable, relevant, and timely.

5.4.4 The security plan should follow the organizational mission and policies.

5.4.5 The security plan should include procedures for movement, communication, facility management, reacting to security incidents, and reporting and analyzing incidents.

5.4.6 Supporting information should be documented and maintained.

5.4.7 Supporting information should include but not be limited to the following:

(1)* Personnel contact information
(2) A list of cooperating agencies, contact people, telephone numbers, and radio frequencies
(3) Mutual aid agreements
(4)* Important outside contacts
(5)* Maps
(6)* Emergency supply inventory

5.4.8* The plan should include response actions to be implemented in the event of a security incident.

5.4.9 An emergency action plan should include but not be limited to the following:

(1) Nature of expected incidents
(2)* Incident response procedures
(3) Emergency contact information
(4) Division of responsibilities and authority among the facility personnel, including who can initiate the plan
(5) Identification of who is covered by the plan (e.g., who is to be evacuated)
(6) Resources needed for the management of the incident
(7) Guidance on the emergency use of funds, disposition of project property, and personal effects
(8) List of annexes to the plan, including but not limited to maps, floor plans, forms, location of personnel, telephone numbers, radio frequencies, and extraordinary procedures

5.4.10 Since the security plan has public and private components, the private components should be maintained as confidential information.

5.5 Planning for Acts of Intimidation or Violence. An organization or facility should include in the security plan, to the extent identified by the SVA, measures to be taken in the event of acts of intimidation or violence.

Chapter 6 Administrative Controls

6.1 General. The recommendations of Chapter 6 should apply when specifically referenced from Chapters 11 through 20.

6.2 People Management.

6.2.1 Employees.

6.2.1.1* Employers should promote trustworthiness by using the following personnel practices for employees with access to critical assets:

(1)* Background screening
(2) Verification of background screening of contracted personnel acting in the capacity of employees
(3) Drug testing program

6.2.1.2* Identification badges should have a photograph of the bearer and the bearer's name.

6.2.1.3 When identification badges are issued, employees should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.2 Visitors. When identification badges are issued, visitors should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.3* Vendors and Contractors.

6.2.3.1 Employers should verify the background screening of vendors and contractors with access to critical assets.

6.2.3.2 When identification badges are issued, vendors and contractors should, as indicated in the security plan, do one of the following:

(1) Display the badge at all times
(2) Display the badge on demand

6.2.4* Security Personnel. Security personnel deployed at a protected premises should comply with the recommendations of this section.

6.2.4.1 Personnel Requirements.

6.2.4.1.1 The number of security personnel should be determined by the security plan and the person responsible for facility security.

6.2.4.1.2 Selection criteria for security personnel should include but not be limited to the following:

(1) Federal, state, and local laws and regulations
(2) Knowledge of criminal activities and proper law enforcement response procedures
(3) Good judgment and emotional stability
(4) Experience and demonstrated ability to retain composure under pressure
(5)* Disclosure of charges or convictions for felonies or crimes involving dishonesty or moral turpitude

6.2.4.2* Security Duties. Security personnel should perform the services prescribed in the post orders.

6.2.4.2.1 Facilities with security personnel should have post orders.

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

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

6.2.4.2.2.2 Post orders should list security personnel duties, including but not be limited to the following:

(1) Authority of security personnel
(2) Emergency response procedures
(3) Job classification
(4) Uniforms
(5) Authorized weapons, including firearms, batons, and mace
(6) Reporting times
(7) Security patrols
(8) Hours of coverage
(9) Facility rules and regulations
(10) Applicable federal, state, and local laws
(11) Other duties to be assigned

6.2.4.2.2.3* Instructions should be lawful and endeavor to protect the safety of security personnel and those they interact with in performance of their duties.

6.2.4.2.3 Post orders should be reviewed and updated as required by the SVA.

6.2.4.2.3.1 Facility management and security management should frequently assess post orders to identify and correct operational problems.

6.2.4.2.3.2 A procedure should be established to inform security personnel of changes in post orders.

6.2.4.3* Supervision.

6.2.4.3.1* Security patrols should be supervised.

6.2.4.3.2 Records should be kept, including but not limited to the following:

(1) Crimes discovered by or reported to security personnel
(2) Frequency of patrols
(3) Activity log
(4)* Exceptions log

6.2.4.3.3 Security records should be retained for not less than 5 years or until the expiration of the appropriate statute of limitations, whichever is longer.

6.2.4.4 Security Personnel Communications. Field security personnel should have a process and means to communicate with a security office or public safety agencies.

6.2.4.5* Weapons and Equipment.

6.2.4.5.1 Security personnel should carry only authorized equipment.

6.2.4.5.2 Where weapons are authorized, policies and procedures governing their storage, handling, and use should be established.

6.2.4.6* Training.

6.2.4.6.1 Security personnel should be trained in the performance of their duties.

6.2.4.6.2 Security personnel who carry weapons should be trained in their storage, handling, and use.

6.2.4.6.3 Armed security personnel should have firearms training.

6.3 Material Receiving.

6.3.1 Commercial Receivables.

6.3.1.1* Shipments coming into facilities should be stopped for entry authorization and dock assignment.

6.3.1.1.1 Shipments coming in should be expected and have corresponding purchase orders or requisitions.

6.3.1.1.2 Undocumented deliveries should not be accepted.

6.3.1.2 Receipt of hazardous materials should be documented and tracked.

6.3.2 Package Deliveries.

6.3.2.1 Packages being delivered should be inspected for evidence of tampering or damage.

6.3.2.2* Any damaged or suspicious packages should be reported to the carrier.

6.3.3 Mail.

6.3.3.1* Employees who handle mail should evaluate the appearance of incoming packages to determine if they fit the characteristics of mail normally received.

6.3.3.2 The recipient of a letter or package should evaluate the delivery to determine if a package is from an unknown, unsolicited source.

6.3.4 Couriers.

6.3.4.1 Couriers making deliveries should provide identification.

6.3.4.2 Courier identification should be entered into a delivery log or attached to the item being delivered.

6.4 Information and Data Security. Organizations should have a policy and procedure for the storage, handling, and use of sensitive information and data, both electronic and printed.

6.4.1 Management of Sensitive Security Information. (Reserved)

6.4.2 Physical Security. (Reserved)

6.4.3 Electronic Security. (Reserved)

6.4.4 Retention and Disposal. (Reserved)

6.5 Workplace Violence.

6.5.1* Employers should develop a program for workplace violence prevention.

6.5.2* An effective approach to preventing workplace violence should include but not be limited to the following key components:

(1) Management commitment
(2) Employee involvement
(3) Worksite hazard analysis
(4) Hazard prevention and control
(5) Safety and health training
(6) Evaluation

Chapter 7 Security Perimeters

7.1 General.

7.1.1 The recommendations of Chapter 7 should apply when specifically referenced in Chapters 11 through 20.

7.1.2 The area covered by the security plan should be defined in the security vulnerability assessment (SVA).

7.1.3* The primary security perimeter should include the total area in the security plan.

7.1.4* Secondary security perimeters within the primary security perimeter should be areas identified as either secured or unsecured.

7.1.5* Movement through every portal in a secured perimeter should be controlled.

7.1.6 Physical barriers or security systems utilized or installed in security perimeters should comply with applicable fire code or other life safety requirements.

7.2* Area Designations. Areas within secondary security perimeters should be designated as one of the following:

(1) Unsecured
  (a) Open
  (b) Protected
(2) Secured
  (a) Controlled
  (b) Restricted

7.3 Exterior Perimeters.

7.3.1* General. Exterior security devices and systems should include but not be limited to the following:

(1) Fences and other physical barriers
(2) Walls
(3) Roofs
(4) Protective lighting
(5) Ironwork (e.g., bars and grilles)
(6) Glazing materials
(7) Passive barriers
(8) Electronic security devices

7.3.2 Fences.

7.3.2.1* Sight lines should be maintained at fence lines.

7.3.2.2* Warning signs should be maintained.

7.3.2.3* Fences should be maintained for integrity.

7.3.3* Walls. When a wall serves as a component of an exterior security perimeter, it should be resistant to penetration.

7.3.4* Roofs. Roofs serving as a component of an exterior security perimeter should comply with 7.3.4.1 through 7.3.4.3.

7.3.4.1 The roof should be protected against unauthorized access.

7.3.4.2 The roof should be resistant to penetration.

7.3.4.3 Openings in the roof should be protected.

7.3.5* Openings to Be Secured. Openings should be protected against entry by unauthorized persons.

7.4 Interior Perimeters.

7.4.1* Where a secure area designation defines an interior room or space, the interior perimeter of such room or space should be protected so that only authorized personnel are permitted to enter.

7.4.2* Access to controlled or restricted areas should be in accordance with Section 7.5.

7.4.3 Factors to be considered in securing an interior perimeter should include but not be limited to the following:

(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 vulnerability to intrusion
(5) Other forms of protection in place or available
(6) Law enforcement or responder capability
(7) Occupants of the area
(8) Life safety, egress, and information dissemination

7.5 Portal Control.

7.5.1 General.

7.5.1.1 The number of portals in a security perimeter should be restricted to the minimum required for safe and efficient operation of the facility.

7.5.1.2* Movement through portals in security perimeters should be controlled.

7.5.2 Exterior Portals.

7.5.2.1 Exterior entrances should be provided with locking devices.

7.5.2.2 Exterior hinge pins on doors in security perimeters should be secured against removal.

7.5.3 Locks.

7.5.3.1* Egress and fire resistance provisions relating to doors and hardware should be maintained.

Δ **7.5.3.2** Individual products should be listed to the following standards as applicable:

(1)* ANSI/BHMA A156 Series, *Categories of Builders Hardware*, for builders' hardware
(2) ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*, for burglary-resistant electronic locking mechanisms
(3) ANSI/UL 437, *Standard for Key Locks*, for key locks
(4) ANSI/UL 768, *Standard for Combination Locks*, for combination locks
(5) ANSI/UL 294, *Standard for Access Control System Units*, for access control system units
(6) UL Subject 2058, *High Security Electronic Locks*, for high security electronic locks
(7) ANSI/UL 305, *Standard for Panic Hardware*, and ANSI/BHMA A156.3, *Exit Devices*, for exit panic devices

7.5.3.3 Locking devices should be properly installed and in good working order.

7.5.3.4* Doors intended to be continuously secured should automatically close and securely latch.

7.5.4* Key/Credential Control.

7.5.4.1 The integrity of key/credential systems should be protected by the use of key/credential control.

Δ **7.5.4.2** Key/credential control procedures should include but not be limited to the following:

(1) Re-keying when a key to a designated controlled or restricted area is lost
(2) Maintaining access lists for persons authorized to draw master keys
(3)* Maintaining security of key/credential storage containers and cabinets
(4) Performing security checks of key/credential storage containers and cabinets
(5) Performing an inventory of keys/credentials annually or as dictated by the security plan
(6) Maintaining a record of key/credential issuance requests, approvals, and issuances
(7) Destroying or maintaining security on keys/credentials not issued or no longer needed
(8) Discretely identifying keys/credentials and key/credential tags by use of a coding system
(9)* Training employees on key/credential control policy and procedure

7.5.4.3* Key/credential control records should include but not be limited to the following:

(1) Number assigned to each key/credential and lock
(2) Location of each lock (room number)
(3) Person to whom each key/credential has been issued
(4) Date of issuance
(5) Date of return
(6)* Documented acceptance for each key/credential issued and returned

Chapter 8 Crime Prevention Through Environmental Design

8.1* General. The recommendations of Chapter 8 should apply when specifically referenced from Chapters 11 through 20.

8.2 Crime and Loss Prevention. (Reserved)

8.3 Human Behavior. (Reserved)

8.4* Lighting. Protective lighting should accomplish the objectives in 8.4.1 through 8.4.8.

8.4.1* Lighting should meet the following criteria:

(1) Be lumen efficient
(2) Be designed to create adequate light levels without being excessive
(3) Minimize night sky pollution

8.4.2 Lighting should meet the recommendations of the security vulnerability analysis (SVA).

8.4.3* For the purpose of natural surveillance and normal use, reasonable illumination should be provided and maintained for exterior areas, including but not limited to the following:

(1) Pedestrian entrances and walkways
(2) Exterior doors
(3) Vehicular entrances
(4) Perimeter fence line where indicated by the SVA
(5) Sensitive areas or structures within the secure perimeter
(6) Parking areas

8.4.4 Constant interior lighting should be maintained for the following:

(1) Egress lighting
(2) Minimum lighting levels for areas under video surveillance

8.4.5* Guard posts should be illuminated based on the SVA.

8.4.6* Redundancy of lighting should be provided based on the SVA.

8.4.7* Security lighting should be protected from vandalism and sabotage.

8.4.8* Security lighting should be maintained.

8.5* Landscaping. Foliage and shrubbery should be trimmed and maintained.

8.6 Aesthetics. (Reserved)

Chapter 9 Security Systems

9.1 General.

9.1.1 The recommendations of Chapter 9 should apply when specifically referenced from Chapters 11 through 20.

9.1.2 Electronic premises security systems should be installed in compliance with the requirements of NFPA 731.

9.2 Contraband Detection. (Reserved)

9.2.1 Weapon Detection (Magnetometers and X-Ray). (Reserved)

9.2.2 Explosive Detection (Man Portal, Parcel/Freight, and Portable). (Reserved)

9.2.3 Radiation Detection (Man Portal, Parcel/Freight, and Portable). (Reserved)

9.2.4 Narcotics Detection (Man Portal and Portable). (Reserved)

9.2.5 Biological and Chemical Agent Detection (Fixed and Portable). (Reserved)

9.3 Personnel Safety Alerting Systems. (Reserved)

9.3.1 Emergency Communication System. (Reserved)

9.3.2 Holdup, Duress, Ambush, and Man Down Alarms. (Reserved)

9.3.3 Threat/Door/Miscellaneous Alarms. (Reserved)

9.3.4 Video Surveillance Analytics Alerting Systems. (Reserved)

9.4 Property Protection Monitoring Systems.

9.4.1 Asset Tracking. (Reserved)

9.4.2 Intrusion Detection Systems.

9.4.2.1* Intrusion detection systems should be designed to protect against vulnerabilities identified by a security vulnerability assessment (SVA).

9.4.2.2 Intrusion detection systems should be installed in accordance with the requirements of NFPA 731.

9.4.2.3 Signals from an intrusion detection system alarm should be in accordance with the requirements of 5.1.3 of NFPA 731.

9.4.2.4 The alarm system should be periodically tested and properly maintained as required in Chapter 10 of NFPA 731.

9.4.3 Access Control Systems.

9.4.3.1* Access control systems should be designed to control movement through portals as determined by the SVA.

9.4.3.2 Access control systems should be installed in accordance with the requirements of NFPA 731.

9.4.3.3 Access to unissued active machine readable credentials should be controlled.

9.4.4 Video Surveillance.

9.4.4.1* Video surveillance systems performance requirements should be designed in accordance with the intent of the SVA.

9.4.4.2 Video surveillance systems should be installed in accordance with the requirements of NFPA 731.

9.4.4.3* Where video surveillance is installed, the system should be monitored or recorded.

9.4.4.4 Where signs are installed, the signs should be maintained.

9.4.4.5* Video surveillance systems should be maintained so that the system will continue to perform as determined by the design in 9.4.4.1.

N **9.4.4.6** Where the SVA requires a particular image quality for video surveillance, the camera should be evaluated to a standard such as UL 2802, *Performance Testing of Camera Image Quality*.

9.4.5* Guard Tour Systems. (Reserved)

9.5 Security Monitoring. (Reserved)

Chapter 10 Accessory Property

10.1 General.

10.1.1 The recommendations of Chapter 10 should apply when specifically referenced from Chapters 11 through 20.

10.1.2 A security vulnerability assessment (SVA) should be conducted for accessory properties as part of the security plan.

10.2 Parking.

10.2.1 General.

10.2.1.1 Section 10.2 provides recommendations to control security vulnerabilities in parking facilities, whether a structure or a space, used for the storage of motor vehicles.

10.2.1.2* A parking facility should have a security plan complying with Chapter 5.

10.2.1.3* Owners and operators of parking facilities should take proactive measures shown as needed by the SVA.

10.2.2* Administrative Controls. Security patrols should comply with 6.2.4.

10.2.3 Security Perimeters.

10.2.3.1* Area Designations. Vehicle entrance and exit portals should be limited to the minimum required for operation of the parking facility.

10.2.3.2* Exterior. (Reserved)

10.2.3.3 Interior. (Reserved)

10.2.3.4 Portal Control. (Reserved)

10.2.4 Crime Prevention Through Environmental Design (CPTED).

10.2.4.1 Crime and Loss Prevention.

10.2.4.2* Human Behavior. Parking areas should be well marked.

10.2.4.3* Lighting. Lighting should comply with Section 8.4.

10.2.4.4 Landscaping. (Reserved)

10.2.4.5 Aesthetics. (Reserved)

10.2.5 Security Systems.

10.2.5.1* Duress Alarms. Public duress alarm systems, where present, should be installed and maintained in accordance with NFPA 731.

10.2.5.2 Access Control. Access control systems should be in accordance with 9.4.3.

10.3 Storage. (Reserved)

10.4 Exterior Areas. (Reserved)

Chapter 11 Educational Facilities, Colleges, and Universities

11.1 General.

11.1.1 Scope.

11.1.1.1 This chapter addresses measures to mitigate security vulnerabilities in educational facilities.

11.1.1.2 Facilities within the scope of this chapter should include public and private primary and secondary schools (K–12), colleges, and universities.

11.1.1.3 Assets within the primary security perimeter should be classified in accordance with their use.

11.1.1.4 Assets used as other than educational facilities should comply with the requirements of this chapter and the appropriate occupancy chapter (Chapters 12 through 20).

11.1.2 Security Plan.

11.1.2.1* An educational facility should have a security plan.

11.1.2.2 The security plan should include but not be limited to the following security vulnerabilities:

(1) Vandalism
(2) Theft
(3) Burglary
(4) Embezzlement
(5) Sexual predation

(6) Assault
(7) Weapons violations
(8) Robbery

11.1.2.3* The educational facility should conduct a security vulnerability assessment (SVA) as part of the security plan.

11.1.2.3.1* The SVA should evaluate the potential security risks posed by the physical and operational environment of the educational facility to all assets at the facility.

11.1.2.3.2 The facility should implement procedures and controls in accordance with the SVA.

11.1.2.4 The security plan should be coordinated with emergency response, disaster, and business recovery plans.

11.1.3 Responsible Person.

11.1.3.1 A person(s) should be appointed by the management of the educational facility to be responsible for security management activities.

Δ **11.1.3.2** The duties of the responsible person(s) should be as identified in the SVA and include, but not be limited to, the following:

(1) Providing identification badges or machine-readable credentials
(2) Controlling movement through portals
(3) Defining and implementing procedures for security incidents including, but not limited to, the following:
  (a) Active shooters
  (b) Access to emergency areas
  (c) Hostage situations
  (d)* Bombs
  (e) Criminal threats
  (f) Labor actions
  (g) Disorderly conduct
  (h) Workplace violence
  (i) Response to restraining orders
  (j) Abductions
  (k) Incidents involving VIPs
  (l) Incidents involving the media
(4) Managing asset protection procedures
(5) Implementing procedures for interaction with emergency services
(6) Ensuring compliance with applicable laws, regulations, and standards regarding security management operations
(7) Establishing education and training programs to address the following:
  (a) Customer service
  (b) Use of force
  (c) Response criteria
  (d) Fire watch procedures
  (e)* Lockdown, lockout, clear the halls, and shelter-in-place procedures
  (f) Emergency notification procedures
(8) Establishing recordkeeping procedures
(9)* Conducting at least one of the following security-related drills semiannually:
  (a) Lockdown
  (b) Lockout
  (c) Shelter-in-place
  (d) Clear the halls

11.2 Administrative Controls.

11.2.1 People Management.

11.2.1.1 Employees.

11.2.1.1.1 Employee practices should comply with 6.2.1.

11.2.1.1.2* Employees should be instructed how to exercise reasonable care in protecting personal property.

11.2.1.1.3* Employees and tenants should receive training on their roles in the security plan.

11.2.1.2 Students.

11.2.1.2.1 Students should be notified of significant security-related incidents.

11.2.1.2.2 Where identification badges are provided, students should display identification badges as recommended in 6.2.1.2 for employees.

11.2.1.3 Visitors.

N **11.2.1.3.1*** All visitors should enter buildings through a monitored and designated visitor entrance(s).

N **11.2.1.3.2** All visitors should be issued school visitor identification.

N **11.2.1.3.3** All visitors should be required to show government-issued, photo identification to a staff member to be issued school visitor identification.

N **11.2.1.3.4** All visitors should be required to wear school visitor identification visible at all times.

11.2.1.4* Vendors and Contractors. (Reserved)

11.2.1.5 Security Personnel.

11.2.1.5.1* The decision to provide security personnel should be based on the SVA.

11.2.1.5.2 Security personnel should comply with 6.2.4.

11.2.1.5.3 Security patrols should be conducted in accordance with the facility security plan.

11.2.2 Material Receiving. The receipt of materials should comply with Section 6.3 and the applicable occupancy chapter (Chapters 12 through 20).

11.2.3 Information and Data Security. (Reserved)

11.2.4 Workplace Violence.

11.2.4.1 A workplace violence plan should be required.

11.2.4.2 The workplace violence plan should be in accordance with Section 6.5.

11.3 Security Perimeters.

11.3.1 Area Designations.

11.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

11.3.2 Exterior — Primary School (K-12) Property.

N **11.3.2.1** Exterior security perimeters should be designated and protected in accordance with Chapter 7.

N **11.3.2.2** In accordance with Section 7.2, secondary exterior security perimeters should include, but not be limited to, the following areas:

(1) Exterior locations used by students for school activities that are designated as unsecured and protected
(2) Parking lots that are designated as secured and controlled
(3) Building exterior walls and portals that are designated as secured and controlled

N **11.3.2.2.1** Where feasible, there should be designated parking areas for the following:

(1) Staff
(2) Students
(3) Visitors
(4) Vendors
(5) Bus loading/unloading

N **11.3.2.2.2** Designated parking areas should be clearly distinguishable and protected through the use of signage and/or physical or electronic security barriers such as gates or security posts.

N **11.3.2.3** All portals in the building perimeter should be controlled in accordance with Section 7.5.

N **11.3.2.4** The building perimeter should have dedicated portals for the following occupants:

(1) Students
(2) Staff
(3) Visitors
(4) Vendors

N **11.3.2.4.1** The student portal(s) should have the following controls in place:

(1) Visual monitoring by a staff member or volunteer during student arrival and dismissal times
(2) Locks to prevent entry except at arrival and dismissal times

N **11.3.2.4.2** The staff portal(s) should be locked at all times with entry requiring a valid key/credential.

N **11.3.2.4.3** Entry at the visitor and vendor portal(s) should be controlled by one or more of the following:

(1) Monitoring by a staff member or volunteer
(2) Electronic access control

11.3.3 Interior. (Reserved)

11.3.4 Portal Control.

11.3.4.1 Portals in security perimeters should comply with Section 7.5.

11.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and student residents who have vacated the premises.

11.3.4.3 Keys/credentials should not be identified in a manner such that a person finding a lost key/credential could trace it back to the school.

11.3.4.4* The degree of portal control should be a function of the campus layout and the needs shown in the SVA.

11.3.4.5 The portal control system should be designed to meet life safety and fire code regulations, as well as legal requirements for accessibility by people with disabilities.

N **11.3.4.6** At a minimum, all exterior portal windows and sidelights should be designed to prevent or delay entry if the glazing is attacked.

N **11.3.4.7*** All classroom doors should be equipped with locking hardware that allows for a single motion egress as defined by NFPA *101*.

N **11.3.4.7.1** All classroom-locking hardware should be lockable from inside the classroom without special knowledge, tools, or credentials.

N **11.3.4.7.2** All classroom-locking hardware should be unlockable from the hallway side with a key or credential.

N **11.3.4.8** Classroom door sidelights should be located on the hinge side of the door and be designed not to allow unauthorized persons from breaking the sidelight glass and accessing the door locking hardware.

N **11.3.4.9** Classroom door sidelights and door windows should be designed so that if the glass is broken, a person cannot gain access to the interior of the classroom.

11.4* Crime Prevention Through Environmental Design (CPTED).

11.4.1 Crime and Loss Prevention. (Reserved)

11.4.2* Human Behavior. A code of conduct that clearly defines each regulation and assigns a specific penalty for each infraction should be developed, publicized, and strictly enforced.

11.4.3 Lighting.

11.4.3.1 Lighting should comply with Section 8.4.

11.4.3.2 The following areas should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators

11.4.4 Landscaping. (Reserved)

11.4.5 Aesthetics. (Reserved)

11.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

11.5.1 Contraband Detection. (Reserved)

11.5.2 Personnel Safety Alerting Systems.

11.5.2.1 Emergency Communication System.

11.5.2.1.1 Emergency communication systems should comply with *NFPA 72* and applicable laws.

11.5.2.1.2* Educational facilities should have a communication policy and a communication method for providing information on safety and crime.

11.5.2.1.3* Educational facilities should have an established policy on communication with local emergency responders.

11.5.2.2 Holdup, Duress, Ambush, and Man Down Alarms. Holdup, duress, ambush, and man down alarms should comply with the requirements of NFPA 731.

11.5.2.3 Threat, Door, and Miscellaneous Alarms. Threat and door alarms and other alarms relating to the safety of people should be monitored by security personnel.

11.5.3* Property Protection Monitoring Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

11.5.3.1 Asset Tracking. (Reserved)

11.5.3.2* Intrusion Detection Systems. Intrusion detection systems should comply with 9.4.2.

11.5.3.3* Access Control Systems. Access control systems should comply with 9.4.3.

11.5.3.4* Video Surveillance Systems. Video surveillance systems should comply with 9.4.4.

11.6 Accessory Property.

11.6.1 Parking. Parking should comply with Section 10.2.

11.6.2* Campus Housing. Based upon the need shown in the SVA, schools that provide housing for students should provide a security program for residence halls, including, but not limited to, the following:

(1) Training students regarding their security responsibilities and role in maintaining the integrity of the security program
(2) Requiring that the exterior portals to residence halls be restricted or guarded at all times
(3) Limiting access to residence halls through the smallest number of portals possible (without conflicting with life safety requirements)
(4) Requiring that one key/credential be used to gain entrance into the residence hall and another key/credential into student rooms; using machine readable credentials programmed for residence hall access and limited access to the proper student room; or requiring the use of two-factor authorization for access to student rooms
(5) Immediately re-keying whenever a student room key/credential is lost or deactivating machine-readable credentials when lost
(6) Having security patrols check that accessible doors and windows to the common areas are locked at night
(7) Having rules, verification, and enforcement 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 a means for visitors to contact residents from the main entrance
(9) Requiring that visitors, vendors, contractors, and delivery persons be escorted at all times in residence halls
(10) Requiring that visitors, workers, and delivery persons always wear identification badges in residence halls
(11) Having special security procedures for housing students during low-occupancy periods, such as holidays and vacation periods

11.6.3* Educational Research Laboratories. Based upon need shown in the SVA, a security program for research laboratories should include but not be limited to the following:

(1) Training faculty and students in the proper handling and security of sensitive, hazardous, or dangerous 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) Electronically monitoring laboratories and storage areas with sensitive materials
(7) Providing increased or dedicated security patrols of research areas
(8) Providing reliable means for laboratory occupants to alert security personnel to off-normal events such as an accidental material release, materials theft, and intrusion/duress situation
(9) Providing proper disposal of sensitive, hazardous, or dangerous materials

Chapter 12 Health Care

12.1 General.

12.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in health care facilities.

12.1.2 Security Plan.

12.1.2.1* A health care facility should have a security management plan.

12.1.2.2 A security vulnerability assessment (SVA) should be conducted for the health care facility as part of the security plan.

12.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the health care facility to all assets in the facility.

12.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

12.1.3 Responsible Person.

12.1.3.1 A person(s) should be appointed by the management of the health care facility to be responsible for security management activities.

12.1.3.2 The duties of the responsible person(s) should include but not be limited to the following:

(1) Providing identification, as shown by review of the SVA, for patients, staff, and other people entering the facility
(2) Controlling access into and out of security-sensitive areas as identified in the SVA
(3) Defining and implementing procedures for the following situations:
    (a) Security incident
    (b) Hostage situation
    (c)* Bomb
    (d) Criminal threat
    (e) Labor action
    (f) Disorderly conduct
    (g) Workplace violence
    (h) Restraining orders
    (i) Infant or pediatric abduction
    (j) Situations involving VIPs or the media
    (k) Ensuring access to emergency areas

(4) Providing security at alternative care sites or vacated facilities
(5) Controlling vehicular traffic control on the facility property
(6) Protecting the facility assets, including property and equipment
(7) Establishing a policy for interaction with law enforcement agencies
(8) Ensuring compliance with applicable laws, regulations, and standards regarding security management operations
(9) Putting into place education and training of the facility security force to address the following:
    (a) Customer service
    (b) Use of physical restraints
    (c) Use of force
    (d) Response criteria
    (e) Fire watch procedures
    (f) Lockdown procedures
    (g) Emergency notification procedures

12.2 Administrative Controls.

12.2.1 People Management.

12.2.1.1 Employees. Employee screening should comply with 6.2.1.

12.2.1.2 The Public. Public visitation controls should be enforced.

12.2.1.2.1 After-hours entrance by the public should be restricted to designated areas such as entrance lobbies and emergency departments.

12.2.1.2.2 Health care facility security controls and procedures should comply with life safety requirements for egress.

12.2.1.3* The Media. The security management plan should include procedures to accommodate media representatives.

12.2.1.3.1 A person should be designated to serve as media contact and representative for the organization in regard to media interactions.

12.2.1.3.2 An area should be designated for assembly of media representatives.

12.2.1.3.2.1 A security or facility staff member should remain with the media representative(s) at all times.

12.2.1.3.2.2* Media representatives should be escorted when granted access to the health care facility outside of the area designated in 12.2.1.3.2.

12.2.1.4* Crowd Control.

12.2.1.4.1 The security management plan should provide procedures for control of a crowd demanding access to a health care facility.

12.2.1.4.2 The procedures for managing crowd control should provide for coordination and collaboration of security and law enforcement.

12.2.1.5 Security Personnel.

12.2.1.5.1 The use of security personnel should comply with 6.2.4.

12.2.1.5.2 Security personnel in health care facilities should have additional training, including but not limited to the following:

(1) Customer service
(2) Emergency procedures
(3) Patrol methods
(4) De-escalation training
(5) Use of physical restraints
(6) Use of force

12.2.2 Material Receiving. The receipt of materials into a health care facility should comply with Section 6.3.

12.3 Security Perimeters.

12.3.1 Area Designations.

12.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

12.3.1.2 The areas in 12.3.1.2.1 through 12.3.1.2.7 should be classified as controlled or restricted.

12.3.1.2.1 Emergency department security should include but not be limited to appropriate protection such as the following:

(1)* A visible security presence
(2) A private duress alarm at the nurse's station and reception for summoning immediate assistance
(3) An access-controlled treatment area
(4) A lockdown procedure to secure the area when conditions threaten the viability of the department
(5) Bullet-resisting glazing material as shown by review of the SVA

12.3.1.2.2 Pediatric and infant care areas should have a security plan for the prevention of and response to pediatric and infant abduction, including but not limited to appropriate protections such as the following:

(1) Controlling and limiting access by the general public
(2) Screening by nursing staff of persons seeking access to infant care areas
(3) Establishing a protocol with staff clearance to match infants with their parents
(4) Establishing a system to monitor and track the location of pediatric and infant patients
(5)* Requiring facility alert system, lockdown, and staff inspection of all packages leaving the premises
(6) Using electronic monitoring, tracking, and access control equipment
(7) Using an automated and standardized facility-wide alerting system to announce pediatric or infant abduction
(8) Using remote exit locking or alarming
(9) Establishing facility lockdown procedures and requiring staff inspection of all persons and packages leaving the premises
(10) Prohibiting birth announcements by staff
(11) Ensuring detection of the presence of non identified individuals, which constitutes a security breach
(12) Requiring the movement of infants to bassinets only, no hand carries
(13) Requiring unique identification or uniforms for health care staff
(14) Setting up secure storage of scrubs and uniforms, both clean and dirty

(15) Providing education about pediatric and infant abduction as follows:
  (a) To familiarize health care staff with infant abduction scenarios
  (b) To let parents know not to leave a child or infant unattended or in the care of an unidentified person
(16) Informing visiting family and friends that they are not permitted to enter any nursery area with an infant or newborn from the outside
(17) Conducting infant abduction drills periodically to test effectiveness of chosen measures

12.3.1.2.3* Medication storage and work areas should be secured against admittance of unauthorized personnel through the use of the following:

(1) Physical access control
(2) Unique identification for the area
(3) Secure storage and controlled dispensing of drugs

12.3.1.2.4 Clinical and research laboratories should be secured against admittance of unauthorized personnel through appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3) Secure storage and controlled dispensing of regulated chemical, biological, and radiological materials

12.3.1.2.5 Dementia and behavioral health units should be secured against the admittance or release of unauthorized personnel or contraband through appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3)* A procedure to prevent entry of contraband prior to a person being admitted into the unit or department
(4) Elopement precautions
(5) Information in patient files to aid in identification

12.3.1.2.6 Forensic patient treatment areas should provide appropriate protections such as the following:

(1) Law enforcement attending the patient at all times
(2) Treatment performed in an area separate from other patients
(3) Restraints applied or removed only under forensic staff control

12.3.1.2.7 Communications, data infrastructure, and medical records storage areas should be secured against the admittance of unauthorized personnel or unauthorized release of confidential information through the use of appropriate protections such as the following:

(1) Physical access control
(2) Unique identification for the area
(3) Surveillance equipment
(4) Data encryption and password protection

12.3.2 Exterior Perimeters. The security plan should include processes and procedures for controlling access to the health care facility.

12.3.3 Interior Perimeters. (Reserved)

12.3.4 Portal Control. Entrances to health care facilities should comply with Section 7.5 for portal control.

12.4 Crime Prevention Through Environmental Design (CPTED).

12.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

Chapter 13 Reserved

Chapter 14 Lodging

14.1 General.

14.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in lodging facilities.

14.1.2 Security Plan.

14.1.2.1* A lodging facility should have a security management plan.

14.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a lodging facility.

14.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the lodging facility to all assets in the facility.

14.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

14.2 Administrative Controls.

14.2.1* People Management.

14.2.1.1 Employees.

14.2.1.1.1 Employee screening should comply with 6.2.1.

14.2.1.1.2 Staff should be trained in security and emergency procedures.

14.2.1.1.3 Staff should wear photo identification badges.

14.2.1.1.4 Staff should be instructed to report suspicious activities to management.

14.2.1.2 Guests. Guests should receive warning of criminal activity in and around the facility.

14.2.1.3 Vendors and Contractors. Vendors and contractors should comply with 6.2.3.

14.2.1.4 Security Personnel.

14.2.1.4.1 The decision to provide security personnel should be based on the SVA.

14.2.1.4.2 Security personnel should comply with 6.2.4.

14.2.1.4.3* Security patrols should be conducted in accordance with the facility security plan.

14.2.2* Material Receiving. The receipt of materials should comply with Section 6.3.

14.2.3 Information and Data Security. Front desk personnel should be trained in guest privacy and security procedures, including but not limited to those outlined in 14.2.3.1 through 14.2.3.6.

14.2.3.1 Front desk personnel should not announce guest room numbers when registering guests or calling for staff.

14.2.3.2 Identification should be required of guests at check-in.

14.2.3.3 Front desk personnel should control issuance of guest room keys/credentials.

14.2.3.3.1 A history log of guestroom key/credential distribution should be maintained.

14.2.3.3.2 Identification should be requested for the re-issuance of room keys/credentials.

14.2.3.3.3* Guest keys/credentials should be retrieved or expire at check-out.

14.2.3.4 Guests should show identification to retrieve fax or written messages.

14.2.3.5 Phone calls to guest rooms should be connected to the room without the room number being identified.

14.2.3.6 Folios, credit card numbers, and other guest information should be kept confidential.

14.3 Security Perimeters.

14.3.1 Area Designations.

14.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

14.3.1.2* Access to the property should be monitored or controlled.

14.3.1.3* Unauthorized persons should be evicted from guest rooms and guest room corridors.

14.3.1.4* Nonpublic areas should be classified as controlled or restricted, including but not limited to the following:

(1) Kitchens
(2) Laundries
(3) Mechanical spaces
(4) Electrical distribution rooms

14.3.2 Exterior.

14.3.2.1* Exterior entrances other than the main lobby entrance(s) should have automatic door closers and locks.

14.3.2.2 Exterior doors should comply with 7.5.2.

14.3.2.3 The exterior of the facility should be regularly checked for the following:

(1) Signs of vandalism
(2) Transients or vagrants living on or around the property

14.3.3 Interior.

14.3.3.1 Guest room doors and windows should comply with the following:

(1) Applicable federal, state, and local requirements regarding locks and latches
(2) Solid wood or steel construction
(3) Frames made of steel or otherwise reinforced, with the clearance between the door and the frame less than 1/8 in. (3.2 mm)
(4)* Deadbolts on entry doors
(5)* Auxiliary locking device on entry doors
(6) Individual room re-keying whenever a key/credential is reported lost or stolen
(7) Housekeeping personnel pick up keys/credentials left in rooms by guests and return them to the front desk as soon as possible
(8)* Door viewer
(9) Locking devices on operable windows and windows or doors that face balconies, terraces, and gardens
(10) Connecting-room doors provided with 1 in. (25.4 mm) deadbolts capable of being unlocked from inside the protected guest room side only

14.3.3.2 Guest rooms should be provided with 24-hour telephone service.

14.3.3.3 Guests should receive notice of the availability of safe deposit boxes.

14.3.3.4 Guests should be provided with brochures or other material offering safety and security tips.

14.3.4 Portal Control.

14.3.4.1 Portals in security perimeters should comply with Section 7.5.

14.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and guests who have vacated their rooms.

14.3.4.3 Hotel keys/credentials should not be identified in a manner such that a person finding a lost key/credential could trace it back to the hotel.

14.4* Crime Prevention Through Environmental Design (CPTED).

14.4.1 Crime and Loss Prevention. Management should be informed of crime trends in and around the facility by taking the following measures:

(1) Researching the history of violent and property crime in the immediate neighborhood and on the premises in the past 3 years
(2) Developing a relationship with local law enforcement agencies to make them familiar with the property
(3) Requesting that local police include the facility in their patrol routes
(4) Maintaining communication with local police to keep informed of crime and crime trends in the neighborhood or area
(5) Participating in local security associations or industry trade groups as a means of sharing common security concerns and solutions

14.4.2 Human Behavior. (Reserved)

14.4.3 Lighting.

14.4.3.1 Lighting should comply with Section 8.4.

14.4.3.2 The following areas should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators
(4) Access routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth

14.4.3.3 Lights in public areas, including laundry rooms, exercise rooms, and vending areas, should be controlled by tamper-proof switches.

14.4.4 Landscaping. (Reserved)

14.4.5 Aesthetics. (Reserved)

14.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

14.5.1 Contraband Detection. (Reserved)

14.5.2* Personnel Safety Alerting Systems. Elevator cars should have means to allow seeing inside the car before entrance.

14.5.3 Property Protection Monitoring Systems.

14.5.3.1 Asset Tracking. (Reserved)

14.5.3.2 Intrusion Detection Systems. (Reserved)

14.5.3.3 Video Surveillance.

14.5.3.3.1 The lobby and front desk areas should have video surveillance.

14.5.3.3.2 Routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should have video surveillance.

14.6 Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 15 Multi-Dwelling Unit Buildings

15.1 General.

15.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in multi-dwelling unit buildings of more than three units.

Exception: The recommendations herein do not apply to one- and two-family dwellings.

15.1.2 Security Plan.

15.1.2.1* A residential facility should have a security management plan.

15.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a residential facility.

15.1.2.2.1* The SVA should evaluate the potential security risks posed by the physical and operational environment of the facility.

15.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

15.1.3* Property Management Responsibility.

15.2 Administrative Controls.

15.2.1 People Management.

15.2.1.1 Employees.

15.2.1.1.1* Employee screening should comply with 6.2.1.

15.2.1.1.2 Staff should be trained in security and emergency procedures.

15.2.1.1.2.1 Staff should record identification information for prospective tenants prior to showing rental units.

15.2.1.1.2.2* Security procedures should include instructions on safety precautions when showing units.

15.2.1.1.3* Staff should be instructed to report suspicious activities to management.

15.2.1.2* Residents.

15.2.1.2.1 Residents should receive security plan procedures and policies that relate to resident safety.

15.2.1.2.2 Residents should sign a statement attesting to their receipt of the information required in 15.2.1.2.1.

15.2.1.2.3 Residents should receive warning of criminal activity in and around the facility.

15.2.1.3* Vendors and Contractors.

15.2.1.4 Security Personnel.

15.2.1.4.1 The decision to provide security personnel should be based on the SVA.

15.2.1.4.2 Security personnel should comply with 6.2.4.

15.2.1.4.3* Security patrols should be conducted in accordance with the facility security plan.

15.2.2 Material Receiving. (Reserved)

15.2.3 Information and Data Security. (Reserved)

15.2.4* Workplace Violence.

15.3 Security Perimeters.

15.3.1 Area Designations.

15.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

15.3.1.2 Nonpublic areas should be classified as controlled or restricted, including but not limited to the following:

(1) Dwelling units
(2)* Common spaces separated from public entry lobbies
(3)* Roofs
(4) Laundry rooms
(5) Exercise rooms

15.3.2 Exterior.

15.3.2.1* Exterior entrances to common areas should have automatic door closers and locks.

15.3.2.2 Exterior doors should comply with 7.5.2.

15.3.2.3 Exterior-accessible openings should be protected against forcible entry, including but not limited to the following:

(1) Basement doors
(2) Accessible windows
(3) Air-conditioning units
(4) Doors to balconies
(5) Exterior doors of dwelling units

15.3.2.4 Bars or gates on windows or doors of dwelling units should be designed to allow emergency egress in case of fire.

15.3.3 Interior.

15.3.3.1 Entry doors to dwelling units should have a door viewer.

15.3.3.2* Entry doors to dwelling units should be of solid-core construction.

15.3.4 Portal Control.

15.3.4.1 Portals in security perimeters should comply with Section 7.5.

15.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and vacated tenants.

15.3.4.3 Locks on doors to rental units should be replaced or re-keyed/credentialed when there is a change in tenancy.

15.4 Crime Prevention Through Environmental Design (CPTED).

15.4.1 Crime and Loss Prevention. Neighborhood crime experience evaluation should include but not be limited to the following criteria:

(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

15.4.2 Human Behavior. (Reserved)

15.4.3 Lighting.

15.4.3.1 Lighting should comply with Section 8.4.

15.4.3.2 The following area should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators
(4) Access routes to common areas such as laundry rooms, exercise rooms, and storage rooms

15.4.4* Landscaping.

15.4.5 Aesthetics. (Reserved)

15.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

15.5.1 Contraband Detection. (Reserved)

15.5.2* Personnel Safety Alerting Systems. Elevator cars should have means to allow users to see inside the car before entering.

15.5.3 Property Protection Monitoring Systems

15.5.3.1 Asset Tracking. (Reserved)

15.5.3.2 Intrusion Detection Systems. Where an intrusion detection system is installed, residents should receive written instructions on how to operate the system.

15.6 Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 16 Restaurants

16.1 General.

16.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in restaurant establishments.

16.1.2 Security Plan.

16.1.2.1 A restaurant should have a security management plan.

16.1.2.2* A security vulnerability assessment (SVA) should be conducted as part of the security plan for a restaurant.

16.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the facility.

16.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

16.2 Administrative Controls.

16.2.1 People Management.

16.2.1.1 Employee screening should comply with 6.2.1.

16.2.1.2* Staff should be trained in security and emergency procedures.

16.2.1.2.1* Management should establish a policy of nonresistance and give it top priority in a training program.

16.2.1.2.2* Delivery personnel should be instructed not to enter any location where they feel threatened or unsafe and to hand over all goods and cash if threatened.

16.2.1.3* Delivery orders should be verified by a telephone number identification system.

16.2.2 Material Receiving. (Reserved)

16.3 Security Perimeters.

16.3.1 Area Designations.

16.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

16.3.1.2 Access to employee-only areas should be controlled.

16.3.2* Exterior. Garbage areas and external walk-in freezers or refrigerators should be located to enhance the safety of employees who use them.

16.3.3 Interior.

16.3.3.1 Goods at high risk to burglary, such as meats and alcoholic beverages, should be stored in a locked closet, security cage, or locked freezer.

16.3.3.2* Cash should be secured during non-business hours in a burglary-resistant safe or vault or other means as determined by the SVA.

16.3.3.2.1 The safe combination should be guarded by limiting the distribution to the minimum number of people requiring access.

16.3.3.2.2 The combination should not be written in an easily accessible place such as on a desk blotter.

16.3.3.2.3 The combination number should be changed on a regular basis.

16.3.4 Portal Control.

16.3.4.1* Other than entry doors, doors should be locked at all times.

16.3.4.2 Locked doors should comply with Section 7.5.

16.4* Crime Prevention Through Environmental Design (CPTED).

16.4.1 Crime and Loss Prevention.

16.4.1.1* Cash on the premises should be kept at the lowest possible amount required to conduct business.

16.4.1.2* The elements of a security program to control burglary should include but not be limited to the following:

(1) Physical security devices
(2) Burglary-resistant safes
(3) Intrusion detection systems

16.4.2 Human Behavior. (Reserved)

16.4.3 Lighting.

16.4.3.1 Lighting should comply with Section 8.4.

16.4.3.2* The entrances and the interior of the premises should be illuminated.

16.4.4 Landscaping. (Reserved)

16.4.5* Aesthetics. Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the premises.

16.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

16.5.1 Contraband Detection. (Reserved)

16.5.2 Personnel Safety Alerting Systems. (Reserved)

16.5.3 Property Protection Monitoring Systems.

16.5.3.1 Asset Tracking. (Reserved)

16.5.3.2 Intrusion Detection Systems.

16.5.3.2.1* The safe, security closet, or security cage should be protected by the alarm system.

16.5.3.2.2 The alarm system should be periodically tested and properly maintained.

Chapter 17 Shopping Centers

17.1 General.

17.1.1* Scope. This chapter addresses measures to mitigate security vulnerabilities in shopping centers.

17.1.2 Security Plan.

17.1.2.1* A shopping center should have a security management plan.

17.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a shopping center.

17.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the shopping center to all assets in the facility.

17.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

Δ **17.1.2.3** Individual tenants should comply with the recommendations of the applicable occupancy chapter(s).

17.1.3 Responsible Person. The duties of the person responsible for security should include but not be limited to the following:

(1) Development of policies and procedures
(2) Risk assessment
(3)* Implementation of security measures
(4)* Law enforcement liaison
(5)* Emergency procedures
(6) Security staffing

17.2 Administrative Controls.

17.2.1 People Management.

17.2.1.1 Employees.

17.2.1.1.1 Employee screening should comply with 6.2.1.

17.2.1.1.2 Staff should be trained in security and emergency procedures.

17.2.1.2* Tenants. Tenants should be notified of significant security-related incidents.

17.2.1.3 Security Personnel.

17.2.1.3.1* The decision to provide security personnel should be based on the SVA.

17.2.1.3.2 Security personnel should comply with 6.2.4.

17.2.1.3.3* Security patrols should be conducted in accordance with the facility security plan.

17.2.1.3.4 Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension.

17.2.2 Material Receiving. The receipt of materials should comply with Section 6.3.

17.3* Security Perimeters.

17.3.1 Area Designations.

17.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

17.3.1.2 Access to employee-only areas should be controlled.

17.4* Crime Prevention Through Environmental Design (CPTED).

17.4.1 Crime and Loss Prevention. (Reserved)

17.4.2 Human Behavior. (Reserved)

17.4.3* Lighting. Lighting should comply with Section 8.4.

17.4.4* Landscaping.

17.4.5 Aesthetics. (Reserved)

17.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

17.5.1 Contraband Detection. (Reserved)

17.5.2 Personnel Safety Alerting Systems. (Reserved)

17.5.3 Property Protection Monitoring Systems.

17.5.3.1 Asset Tracking. (Reserved)

17.5.3.2 Intrusion Detection Systems. (Reserved)

17.5.3.3* Video Surveillance.

17.6* Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 18 Retail Establishments

18.1 General.

18.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in retail establishments.

18.1.2 Security Plan.

18.1.2.1* A retail establishment should have a security management plan.

18.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan for a retail establishment.

18.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the retail establishment to all assets in the facility.

18.1.2.2.2 The facility should implement procedures and controls in accordance with the risks identified by the SVA.

18.1.2.3* The elements of a security program to control robbery should include but not be limited to the following:

(1) Control of cash
(2) Access control
(3) Security equipment
(4) Personnel
(5) Employee training

18.2 Administrative Controls.

18.2.1 People Management.

18.2.1.1 Employees.

18.2.1.1.1 Employee screening should comply with 6.2.1.

18.2.1.1.2 Staff should be trained in security and emergency procedures.

18.2.1.1.2.1 A policy of nonresistance should be established and given top priority.

18.2.1.1.2.2 Employee training should include but not be limited to the following:

(1)* What to do before, during, and after a robbery
(2) How to be an effective witness through observation and reporting of details, events, and descriptions
(3) Proper use of security equipment, especially holdup alarm systems
(4) Procedures to follow in detaining or arresting shoplifters
(5) Check cashing procedures
(6) Credit card acceptance procedures
(7) Detection of counterfeit currency

18.2.1.1.3* Employee theft should be managed by using procedures and devices, including but not limited to the following:

(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
(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 such as video surveillance to control theft
(6) Securing expensive items to limit opportunity for theft

18.2.1.2 Customers.

18.2.1.2.1* Shoplifting Prevention. A program against shoplifting in retail establishments should consist of procedural controls and policies consistent with laws and ordinances.

18.2.1.2.2 Check Fraud.

18.2.1.2.2.1* For those retail establishments that accept checks, a check acceptance policy should be established.

18.2.1.2.2.2 Elements of a check acceptance policy should include but not be limited to the following:

(1) Requiring two forms of identification
(2) Listing identification on the back of the check
(3)* Not accepting third-party checks
(4) Using an electronic check verification system

18.2.1.2.3* Credit Card Fraud. Retail establishments should establish a credit card payment policy.

18.2.1.2.4 Counterfeit Currency. Retail businesses should have equipment used to detect counterfeit currency.

18.2.1.3* Contractors and Vendors. Access by contractors and vendors should be monitored by management.

18.2.1.4 Security Personnel.

18.2.1.4.1* The decision to provide security personnel should be based on the SVA.

18.2.1.4.2 Security personnel should comply with 6.2.4.

18.2.1.4.3* Security patrols should be conducted in accordance with the security plan.

18.2.1.4.4 Patrols should be conspicuous, since the emphasis is on deterrence rather than apprehension.

18.2.2 Material Receiving. The receipt of materials should comply with Section 6.3.

18.2.3 Information and Data Security. (Reserved)

18.2.4* Workplace Violence. Retail establishments should have a workplace violence prevention program in accordance with Section 6.5.

18.3 Security Perimeters.

18.3.1 Area Designations.

18.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

18.3.1.2 Access to employee-only areas should be controlled.

18.3.2* Exterior. Garbage areas should be located to enhance the safety of employees who use them.

18.4 Crime Prevention Through Environmental Design (CPTED).

18.4.1 Crime and Loss Prevention.

18.4.1.1* Cash on the premises should be kept at the lowest possible amount required to conduct business.

18.4.1.2* Means to mitigate loss from burglary or theft should include but not be limited to the following:

(1) Physical security devices
(2) Burglary-resistant safes
(3) Intrusion detection systems

18.4.1.3* Cash should be secured during non-business hours in a burglary-resistant safe, vault, or other means as determined by the SVA.

18.4.2 Human Behavior. (Reserved)

18.4.3* Lighting. Lighting should comply with Section 8.4.

18.4.4* Landscaping.

18.4.5* Aesthetics. Product displays, posters, and advertisements in windows should not obstruct visibility into or out of the store.

18.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

18.5.1 Contraband Detection. (Reserved)

18.5.2 Personnel Safety Alerting Systems. (Reserved)

18.5.3 Property Protection Monitoring Systems.

18.5.3.1 Asset Tracking. (Reserved)

18.5.3.2* Intrusion Detection Systems. When an intrusion detection system is installed, it should also protect the safe, security closet, or security cage.

18.5.3.3* Video Surveillance.

18.6* Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 19 Office Buildings

19.1 General.

19.1.1* Scope.

19.1.1.1 This chapter addresses measures to mitigate security vulnerabilities in office buildings.

19.1.1.2* Buildings operated by federal, state, or local government that have tenants, including law enforcement agencies, court-related agencies and functions, or government records and archives, or that have tenants that perform functions critical to national security are not within the scope of this chapter.

19.1.2 Security Plan.

19.1.2.1* Office buildings should have a security management plan.

19.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan.

19.1.2.2.1 The SVA should evaluate the potential security risks posed by the physical and operational environment of the office building to all assets in the building.

19.1.2.2.2 The office building management should implement procedures and controls in accordance with the risks identified by the SVA.

19.1.2.2.3 Regardless of the measures utilized, security should not conflict with fire or life safety code requirements.

19.1.2.3 The security plan should synchronize with emergency response, disaster, and business recovery plans.

19.1.3 Responsible Person.

19.1.3.1 A person(s) should be appointed by the management of the office building property to be responsible for security management activities.

19.1.3.2 The duties of the responsible person(s) should include but not be limited to the following:

(1) Establishing security measures for exterior areas, common interior areas, and parking areas
(2) Implementing access control at basement-, ground-, and street-level entrances and exits
(3) Implementing a key/credential control program
(4) Setting up training and supervision of security personnel
(5) Carrying out employee background checks and drug testing
(6)* Reviewing local neighborhood crime trends

19.2* Administrative Controls. Emergency telephone numbers and building management contact information should be posted.

19.2.1 People Management.

19.2.1.1 Employees and Tenants.

19.2.1.1.1 Employee practices should comply with 6.2.1.

19.2.1.1.2* Employees and tenants should be instructed how to exercise reasonable care in protecting personal property.

19.2.1.1.3* Employees and tenants should receive training on their roles in the security plan.

19.2.1.1.4* Tenants should be notified of significant security-related incidents.

19.2.1.1.5 Where identification badges are provided, tenants should display identification badges as recommended in 6.2.1.2 for employees.

19.2.1.2 Visitors.

19.2.1.2.1* When an office building is a secure area as designated in the security plan, visitors should be required to identify the person they are visiting.

19.2.1.2.2* Visitors should be required to wear a visitor's badge.

19.2.1.3* Vendors and Service Personnel.

19.2.1.4 Security Personnel.

19.2.1.4.1 The decision to provide security personnel should be based on the SVA.

19.2.1.4.2 Security personnel should comply with 6.2.4.

19.2.1.4.3 Security patrols should be conducted in accordance with the facility security plan.

19.2.2* Material Receiving. The receipt of materials into an office building should comply with Section 6.3.

19.3 Security Perimeters.

19.3.1 Area Designations.

19.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

19.3.1.2* Shipping and receiving areas should be secure areas.

19.3.1.3* Security-sensitive areas identified in the SVA should be protected as appropriate.

19.3.1.4 Restrooms should be secured as determined by the SVA.

19.3.1.5 Access to utility connections and mechanical areas should be controlled.

19.3.2 Exterior Perimeters.

19.3.2.1* Entrances to office buildings should be controlled to allow access for employees or tenants and to funnel visitors to reception.

19.3.2.2* Exterior doors should have automatic closers and locks.

19.3.2.3* Exterior doors from emergency stairwell exits on the ground or street level should not have exterior door handles.

19.3.3 Interior Perimeters. (Reserved)

19.3.4 Portal Control.

19.3.4.1 Portals in security perimeters should comply with Section 7.5.

19.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees, employees on vacation, and tenants who have vacated the premises.

19.4 Crime Prevention Through Environmental Design (CPTED). (Reserved)

19.4.1 Crime and Loss Prevention. (Reserved)

19.4.2 Human Behavior. (Reserved)

19.4.3 Lighting.

19.4.3.1 Lighting should comply with Section 8.4.

19.4.3.2 The following areas should be illuminated in addition to those areas listed in Section 8.4:

(1) Corridors
(2) Stairwells
(3) Elevators

19.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

19.5.1 Contraband Detection. (Reserved)

19.5.2* Personnel Safety Alerting Systems. Elevator cars should have means to allow seeing inside the car before entrance.

19.5.3 Property Protection Monitoring Systems. (Reserved)

19.5.3.1 Asset Tracking. (Reserved)

19.5.3.2 Intrusion Detection Systems. Intrusion detection systems should be connected to a monitoring station in compliance with NFPA 731, Chapter 9.

19.5.3.3 Access Control Systems. (Reserved)

19.5.3.4* Video Surveillance.

19.6 Accessory Property, Parking. Parking should comply with Section 10.2.

Chapter 20 Industrial Facilities

20.1 General.

20.1.1 Scope. This chapter addresses measures to mitigate security vulnerabilities in industrial facilities.

20.1.2 Security Plan.

20.1.2.1 Industrial facilities should have a security management plan.

20.1.2.2 A security vulnerability assessment (SVA) should be conducted as part of the security plan.

20.1.2.2.1* The SVA should evaluate the potential security risks posed by the physical and operational environment of the industrial facility.

20.1.2.2.2* Management should implement procedures and controls in accordance with the risks identified by the SVA.

20.1.2.2.3 Regardless of the measures utilized, security should not conflict with fire or life safety code requirements.

20.1.2.3 The security plan should synchronize with emergency response, disaster, and business recovery plans.

20.1.3 Responsible Person.

20.1.3.1 A person(s) should be appointed by the management of the industrial facility to be responsible for security management activities.

20.1.3.2 The duties of the responsible person(s) should include but not be limited to the following:

(1) Security measures for the facility
(2) Security clearances and badges
(3) Key/credential control program
(4) Training and supervision of security personnel
(5) Employee background checks and drug testing
(6) Vehicular and pedestrian traffic controls through secure perimeters

20.2 Administrative Controls.

20.2.1 People Management. Access to critical assets should be restricted to the following:

(1) Employees
(2) Authorized vendors and contractors
(3) Escorted visitors

20.2.1.1* Employees.

20.2.1.1.1 Employee practices should comply with 6.2.1.

20.2.1.1.2* Employees should receive training on their roles in the security plan.

20.2.1.1.3* Workers should be trained in emergency procedures.

20.2.1.2 Visitors.

20.2.1.2.1 Visitors should be required to identify the person they are visiting.

20.2.1.2.2* Visitors should be required to wear a visitor's badge.

20.2.1.2.3 Visitors should be escorted to their destination as determined by the SVA.

20.2.1.3 Vendors and Service Personnel. Contractors, maintenance, housekeeping, and vendors should display identification badges acceptable to facility management.

20.2.1.4 Security Personnel.

20.2.1.4.1 The decision to provide security personnel should be based on the SVA.

20.2.1.4.2 Security personnel should comply with 6.2.4.

20.2.1.4.3 Security patrols should be conducted in accordance with the facility security plan.

20.2.2 Material Receiving.

20.2.2.1 The receipt of materials should comply with Section 6.3.

20.2.2.2* Hazardous material inventory should be accurately monitored.

20.3 Security Perimeters.

20.3.1 Area Designations.

20.3.1.1 Areas identified in the SVA should be classified in accordance with Sections 7.1 and 7.2.

20.3.1.2 Facilities should restrict access to critical assets by establishing secure perimeters.

20.3.1.3 Secure perimeter should be established using physical, electronic, or other means.

20.3.2* Exterior Perimeters.

20.3.3 Interior Perimeters. (Reserved)

20.3.4 Portal Control.

20.3.4.1 Portals in security perimeters should comply with Section 7.5.

20.3.4.2 Procedures should be established for collecting keys/credentials from terminated employees and employees on vacation.

20.4 Crime Prevention Through Environmental Design (CPTED). (Reserved)

20.5 Security Systems. The installation of electronic premises security systems should be in accordance with Section 9.4.

20.6 Accessory Property, Parking. Parking should comply with Section 10.2.

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.1.2 Security protection involves assessing the vulnerabilities and planning what to do to address those vulnerabilities. Security is more than installing a security system. This guide 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.

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.

Δ **A.3.3.1 Access Control.** Access control portals are doors, gates, turnstiles, and so forth. Controls can be operational, technical, or physical or a combination thereof and can vary depending on type of credential, authorization level, day, or time of day. [**731,** 2017]

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. (152 mm), 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

Δ **A.3.3.3.1 False Alarm.** A false alarm can 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. [**731,** 2017]

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.3.3.4 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. [**731,** 2017]

A.3.3.5.1 Controlled Area. Admittance to a controlled area is limited to persons who have official business within the area.

A.3.3.5.2 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.3.3.6 Capacitance Sensor. The protected object must be metal, electrically charged, and insulated from electrical ground potential.

Δ **A.3.3.12.1 Duress Alarm Initiating Device.** 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 commercial or proprietary monitoring station or guard post. [**731,** 2017]

A.3.3.15 Electromagnetic Lock. Electromagnetic locks use no moving parts.

N **A.3.3.17.2 Health Care Facilities.** Health care facilities include, but are not limited to, hospitals, nursing homes, limited care facilities, clinics, medical and dental offices, and ambulatory health care centers, whether permanent or movable. This definition applies to normal, regular operations and does not pertain to facilities during declared local or national disasters. A health care facility is not a type of occupancy classification as defined by NFPA *101*. Therefore, the term *health care facility* should not be confused with the term *health care occupancy*. All health care occupancies (and ambulatory health care occupancies) are considered health care facilities; however, not all health care facilities are considered health care occupancies, as health care facilities also include ambulatory health care occupancies and business occupancies. [**5000,** 2015]

Δ **A.3.3.19 Foil.** Foil is a thin metallic strip, also known as tape, commonly used on windows and other glass installations. When the glass is broken, the foil breaks and opens the electrical circuit, causing an alarm condition. [**731,** 2017]

A.3.3.25.1 Confidential Information. Confidential information 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.3.3.29 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 techniques include random tone patterns, multiplexing, authentication, data encryption, and the like.

A.3.3.32 Machine Readable Credential. Examples include a user-entered identifier, such as a personal identification number or an entry code; an identifying credential such as a magnetic stripe card, a proximity card, or a "smart" card; and biometric identifiers, which can be unique personal characteristics (fingerprint or retinal scan) or an individual behavior characteristic (a person's signature). [**731,** 2017]).

A.3.3.33 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 indoor use; bistatic and terrain-following sensors are normally used for outdoor applications.

A.3.3.34 Monitoring Station. Services offered by a monitoring station can include the following:

(1) System installation
(2) Alarm, guard, and supervisory signal monitoring
(3) Retransmission
(4) Testing and maintenance
(5) Alarm response service
(6) Record keeping and reporting
(7) Video monitoring
(8) Audio monitoring

[**731,** 2017]

•

A.3.3.38 Reader. Readers can be of many types and are intended to include car tags, electronic key, magnetic stripe, proximity badge, biometric, or other identifier. [**731,** 2017].

A.3.3.40 Screens. Skylights, windows, doors, and similar openings can be protected by screens. Intrusion is detected when conductors in the screen are broken or if the screen is removed. [**731,** 2017]

A.3.3.42 Security Vulnerability Assessment (SVA). A security vulnerability assessment (SVA) includes a risk assessment and threat assessment as well as other components that may be added to do a complete assessment of the vulnerabilities. The results of the SVA are used in developing countermeasures to address adversarial events.

N **A.3.3.43 Shelter-in-Place.** Shelter-in-place has been established by the CDC as the method in which one should "seal the room" to prevent foreign matter from entering the space. The term *shelter-in-place* should be used for this purpose as well as for severe weather emergencies.

A.3.3.46.1 Duress Alarm System. A duress alarm system can be private or public. A private duress alarm system or portion thereof is one in which the action to activate the duress signal is known only to the person activating the device. A public duress alarm system or portion thereof is one in which the ability to activate a duress signal is available to any person at the protected premises.

Δ **A.3.3.46.2 Holdup Alarm System.** A holdup alarm can be manual or semiautomatic. A manual holdup alarm system or portion thereof is one in which the initiation of a holdup signal depends solely on operation of manually operated hand or foot initiating devices installed within the working area. A semiautomatic holdup alarm system or portion thereof is one in which the initiation of a holdup signal does not depend solely on operation of manually operated hand or foot initiating devices installed within the working area.

•

A.3.3.49 Vault (as related to premises security). Vaults can provide a degree of protection against attack. Vault construction should be chosen based on the penetration delay requirements determined in the SVA. A vault can also consist of a door and modular panels constructed in compliance with the requirements in ANSI/UL 608, *Standard for Burglary-Resistant Vault Doors and Modular Panels*. [**731,** 2017]

A.4.1.3(4) Examples of ways to deter, detect, and delay attacks are as follows:

(1) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas, or otherwise presenting a hazard to potentially critical targets
(2) Deter attacks through visible, professional, well-maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets
(3) Detect attacks at early stages through surveillance, sensing systems, and barriers and barricades
(4) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning

A.4.2.2 Risk is the vulnerability of the asset against the threat. The risks in this document are classified by the occupancy type. However, every asset will have a different risk profile. So each asset needs to be evaluated based on the appropriate occupancy chapter. For example, a school would be covered under educational in Chapter 11, but if there is a service garage or mechanical area, then that area may more appropriately be covered under industrial facilities in Chapter 20.

A.4.3.3 It is easier to evaluate risks based on how often they occur and how severe the result is in cost or impact to the organization. The graph in Figure A.4.3.3 can be used as a guide to sort the risks.

A.4.3.4(1) The tolerance to risk should be the transformation of the SVA findings into a security plan that serves the organization in achieving a comfort level with the procedures and controls adopted to minimize the potential risks identified in the SVA.

A.4.4.1 The effectiveness of the security plan is tested by performing drills.

Drills should be conducted on all work schedules. Drills on all of the shifts are necessary so that all personnel are familiar with the plan. Practicing the plan helps personnel react as needed during a security incident.

A.4.4.2 When the review shows changes in activities, occupancy use, number of people, or operational environment, the security plan should be revised.

A.4.6.2 Security equipment should be covered under a service agreement.

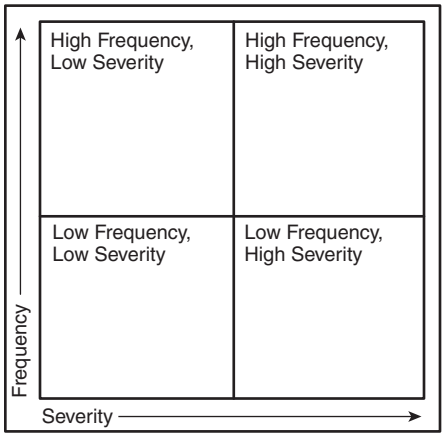


FIGURE A.4.3.3 Frequency/Severity Matrix.

A.5.2.1 There are several referenced publications in Annex G that will assist the reader in the process of conducting a security vulnerability assessment. The SVA can be used in developing and strengthening both security and safety layers of protection.

A.5.2.2 All properties have vulnerable points such that protections can be minimized or completely interrupted or circumvented. The risks posed by vulnerable points as identified in the SVA should be minimized.

A.5.2.3(1) The individual responsible for an organization's security should serve as team leader.

A.5.2.3(2) The characterization of the organization and facilities should include the following:

(1) Identification of assets (e.g., people, property, information, and mission)
(2) Physical features and operations
(3) Laws, regulations, and corporate policies
(4) Social and political environment and internal activity (e.g., community resources, crime statistics, internal activities, and loss experience)
(5) Review of "current layers of protection" (including both site security features and safety measures)

A.5.2.3(4) The relative security risk level is a function of determining the severity of the consequences of an adversarial event, the potential for such an event, and the likelihood of adversary success in carrying out the anticipated event or activity.

A.5.2.3(5) An effective countermeasure is one that drives improvements in mitigating the defined threats and results in a reduction in the security risk level. With respect to the development of security countermeasures, and in consideration of the defined threats, the SVA team's efforts to strengthen the security layers of protection begins with a focus on the concentric circles of protection design methodology, shown in Figure A.5.2.3(5).

This methodology provides for protection of defined critical assets by considering the four primary protection elements. The primary elements of an effective protection plan design are as follows:

(1) Deter — discouraging an adversary from attempting an assault by reducing the likelihood of a successful attack.
(2) Detect — determining that an undesirable event has occurred or is occurring. Detection includes sensing the event, communicating the alarm to an attended location, and assessing the alarm.
(3) Delay — impeding adversary penetration into a protected area.
(4) Respond — counteracting adversary activity and interrupting the undesirable event.

Theft, sabotage, or other malevolent acts can be prevented in two ways, by either deterring the adversary or defeating the adversary. In the development of security countermeasures, it is important to understand that a properly designed and implemented security program integrates people, procedures, and technologies for the protection of assets. The use of technologies alone is not the solution.

In developing effective countermeasures, it is important to remember that highly probable threats may not require countermeasures attention if the net loss they would produce is small. But moderately probable risks require attention if the magnitude of the loss they produce is great. The correlative of probability of occurrence is severity or criticality of occurrence. Assessing the criticality of a loss is imperative for a meaningful vulnerability assessment. Criticality is first considered on a single event or occurrence basis. For events with established frequency or high recurrence probability, criticality must be considered cumulatively.

To determine the severity or consequence of a loss, all costs associated with each loss must be considered. Kinds of loss to be considered include but are not limited to the following:

(1) *Permanent replacement.* Permanent replacement of a lost asset includes all of the cost to return it to its former location. Components of that cost are as follows:
    (a) Purchase price or manufacturing cost
    (b) Freight and shipping charges
    (c) Make-ready or preparation cost to install it or make it functional
(2) *Temporary substitute.* In regard to tools of production and other items making up the active structure of an enterprise, it may be necessary to procure substitutes while awaiting permanent replacements. Components of temporary substitute costs may be as follows:
    (a) Lease or rental
    (b) Premium labor, such as overtime or extra shift work to compensate for the missing production
(3) *Related or consequent cost.* If other personnel or equipment are idle or underutilized because of the absence of an asset lost through a security incident, the cost of the down time is also attributable to the loss event.
(4) *Lost income cost.* If cash that might otherwise be invested is used to procure permanent replacements or temporary substitutes or to pay consequence costs, the income that might have been realized from the investment must also be considered as part of the loss.
(5) *Cost abatement.* To the extent it is available, insurance, or other indemnification for the loss should be subtracted from the costs enumerated above. For precision, that portion of the insurance premium cost attributable to the lost asset should be subtracted from the available insurance before the insurance is used to offset the loss.

The "new world" we live in poses a new challenge: the increased presence and threat of adversarial attack. Our journey now involves an important dual approach, the combination of today's security methodologies with traditional safety and risk management practices to strengthen security layers of protection.

An effective security program, resulting from the completion and implementation of a comprehensive SVA, provides measurable benefits in the workplace for personnel (staff, guests, and visitors), in the protection of property, and in operations, resulting in enhanced business performance.

N **A.5.3.2** Some certification organizations are as follows:

(1) ASIS International — Certified Protection Professional (CPP), Physical Security Professional (PSP)
(2) Sandia Labs Risk Assessment Methodology (RAM)
(3) Critical Infrastructure and Asset Protection Automated Critical Asset Management System (ACAM) and Protected Critical Infrastructure Information (PCII)
(4) Anti-Terrorism Specialist, Anti-Terrorism Accreditation Board — International Association Of Counterterrorism And Security Professionals

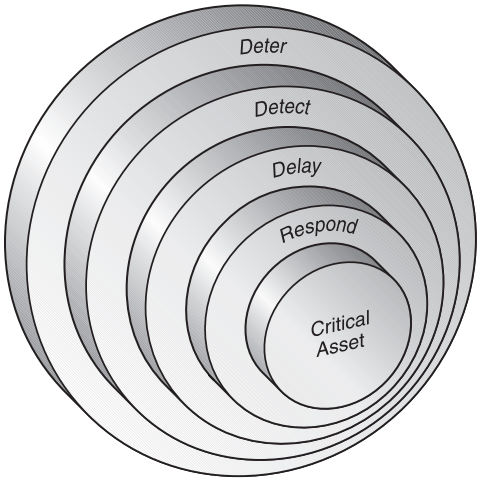


FIGURE A.5.2.3(5) Concentric Circles of Protection.
(Source: SafePlace Corporation.)

(5) Crime Prevention Through Environmental Design (CPTED)
(6) International CPTED Association
(7) International Society of Crime Prevention Practitioners, Inc.
(8) Secured By Design

A.5.4.7(1) It should not be necessary to collect personal information that might allow identity theft. This might include passport numbers and social security numbers. The security plan can link to a human resources database for contact information instead of being in the plan. Care should be taken to guard personnel personal data.

A.5.4.7(4) Outside contacts might include government officials, security personnel, airport and transportation authorities, utility companies, health care facilities and clinics, and others.

A.5.4.7(5) Maps may be regional, national, sub-regional, or local. Maps can indicate assembly points, overland routes, airfields, and border crossings.

A.5.4.7(6) Supplies can include food, medical, documents, clothing, and personal protective equipment (PPE).

A.5.4.8 Plans should include but not be limited to procedures for the following:

(1) Response of security personnel
(2) Response of emergency services
(3) Access points for emergency services
(4) Communication procedures

More information is available in NFPA 1561.

A.5.4.9(2) Plans should be structured so that if the primary response fails, there is a backup plan.

A.6.2.1.1 Employee screening is typically a function managed by the human resources department.

The increase in the number of lawsuits based on the tort of negligent hiring has resulted in employers being under a greater responsibility to use due care in selecting employees. At the same time, federal and state laws impose restrictions on employers that are intended to protect the privacy of applicants. Since many employees have access to critical assets (people, property, and information), the need for preemployment screening cannot be overemphasized.

A.6.2.1.1(1) Employers should conduct an appropriate level (based on the SVA and employee duties) of background screening varying from checking resources, criminal history, and credit, to a full background check with drivers' records, visual inspection of residence, interviews with known associates, and other formal checks. Polygraphs should be conducted only as permitted by law.

A.6.2.1.2 For large facilities, the use of color codes on identification badges should be considered and codes established for specific buildings, floors, or areas.

A.6.2.3 Employees of outside services (e.g., contractors, vendors, or other personnel) should be screened to the same requirements as employees. Management should ask contractors for their employee procedures.

A.6.2.4 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.

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.

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.

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.

A.6.2.4.1.2(5) The disclosure should be in compliance with legal, regulatory, and contractual requirements.

A.6.2.4.2 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/credential control.* Receive, issue, and account for certain keys/credentials 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.

A.6.2.4.2.2.3 Security personnel should be covered by liability insurance. Check for adequate liability insurance when contracting security services.

A.6.2.4.3 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.

A.6.2.4.3.1 Some ways to accomplish supervision are spot checks, daily logs, watchclock tours, and activity reports.

A.6.2.4.3.2(4) Signs of vandalism as well as signs of transients or vagrants living on or around the property should be noted. Security-related complaints made by employees or tenants should be noted as well.

A.6.2.4.5 Security personnel should be armed only when there are compelling reasons. 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. Many states have laws that require background checks and specific training for security personnel, especially armed personnel.

A.6.2.4.6 It is essential that facilities using security personnel train them in the legal and practical applications of their employment. Training should be repeated periodically. Training must reflect changes in regulations and the enactment of new laws.

A.6.3.1.1 While shipments typically arrive by truck, shipments also can come in through other transportation modes such as trains or barges.

A.6.3.2.2 See A.6.3.3.1 for characteristics indicating a suspicious package.

A.6.3.3.1 Suspicious packages or mail should not be opened. 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

Consideration should be given to receiving mail in an area separated from critical functions.

A.6.5.1 Employers have the obligation to address workplace violence as regulated under the Occupational Safety and Health Act of 1970 (OSHA). 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.

The goal of the OSHA 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 must use a combination of recommended strategies, as appropriate, for their particular workplace.

Under the Occupational Safety and Health Act of 1970 (OSHA), 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.”

A.6.5.2 Using these basic elements, employers must fashion prevention plans that are appropriate for their establishment based on the hazards and circumstances of the particular situation. 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 operating procedures.

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.

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.

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. 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.

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 must seek legal counsel if they are unsure of their legal obligations and constraints.

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.

A worksite hazard analysis involves a step-by-step, commonsense 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.

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.

As a starting point for the hazard analysis, 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?

Employers with more than one store or business location must review the history of violence at each operation. Different experiences in those locations 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.

The team or the coordinator should 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.

Annex F provides a sample checklist that illustrates a number of questions that can be helpful for the security analysis.

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 operational changes 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.

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 must use a combination of controls in relation to the hazards identified through the hazard analysis.

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:

(1) Improve visibility.
(2) Maintain adequate lighting.
(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. Post signs stating that the amount of cash on hand is limited when using drop safes.
(5) Install video surveillance equipment to deter robberies by increasing the risk of identification. This can include interactive video equipment. 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.

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 must 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 must 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/credential 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.

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.

Training should be conducted by persons who have a demonstrated knowledge of the subject and must 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.

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.

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 must 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.

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.

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.

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.

Violence prevention programs benefit greatly from periodic evaluation. The evaluation process will 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.
(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.

A.7.1.3 The primary security perimeter might contain areas that are not contiguous. The noncontiguous U.S. states, Hawaii and Alaska, are well-known examples.

A.7.1.4 The primary security perimeter can include multiple secondary security perimeters. It is possible for a secondary perimeter to be congruent with the primary perimeter.

A.7.1.5 Secured perimeters are physical barriers that control authorized access to secure areas. 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.

A.7.2 There are few security plans where access is intended to every area. Accordingly, access to some areas is necessarily secured.

The following 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 service
(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

The following 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

A.7.3.1 Depending on their construction, walls, floors, roofs, doors, and windows can also be considered exterior security devices and systems.

A.7.3.2.1 Fence lines be straight to provide for observation along the length of the fence. 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.

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.

A.7.3.2.2 "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.

A.7.3.2.3 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.

A.7.3.3 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.

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.

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.

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.

A.7.3.4 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.

The flat roofs most often found on commercial buildings can be very attractive to intruders. Because the walls on many commercial buildings extend 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.

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.

A.7.3.5 Openings to be secured are determined to be penetrable by unauthorized persons. The following items should be considered when protecting security perimeters:

(1) Doors and windows
(2) Roofs
(3) Vents
(4) Skylights
(5) Maintenance access ways

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.

Some consideration should be given to the construction of the walls that support the doors or windows, because 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.

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.

A.7.4.1 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. 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.

A.7.4.2 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.

A.7.4.3(4) The interior perimeters should be secured as determined by the SVA, including evaluations of openings, floors, walls, and ceilings for security vulnerabilities. For example, a partition in an interior perimeter might be penetrable by going over through a lay-in ceiling or underneath through raised floor access panels.

A.7.5.1.2 Access through portals is usually controlled for ingress, but it is possible to control movement in both directions. The decision to control in both directions is based on the SVA. When portals are not staffed, they should be 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, should be locked except when actually in use.

Δ **A.7.5.3.1** More information on fire resistance–rated opening protectives is in NFPA 80.

A.7.5.3.2(1) ANSI/BHMA A156 performance guides include security tests and are shown in the applicable sections of Annex G.

A.7.5.3.4 Doors that are always locked should have a latch-type lock and closer to ensure they are not accidentally left unlocked.

A.7.5.4 The integrity of a key system is important to safeguarding property and controlling access. Lost or stolen keys and key blanks 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 should be kept to a minimum. Keys should be issued only to persons who have an official need.

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.

Facility keys should not be identified in any manner such that a person finding a lost key could trace it back to the facility. A policy should be established to restrict duplication of keys without written permission. All keys should be marked "DO NOT DUPLICATE" to deter the unauthorized copying of keys.

A master key system should be designed so that the grandmaster key is the only key that will open every restricted area of the facility. A master key system is used to limit the number of keys carried by personnel requiring access to multiple 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 person unrestricted access to all areas of the building. The sophistication of the master key system should depend upon an

assessment of employees' or tenants' needs and the criticality, risk, and sensitivity of restricted areas. The number of grandmaster keys should be limited to the least number necessary for operation of the facility. Master key distribution should be limited to the personnel requiring access to multiple restricted areas.

A.7.5.4.2(3) Key storage containers and cabinets should be kept locked with a pick- and drill-resistant, patented high security cylinder that is not keyed to the facility master key system.

A.7.5.4.2(9) Key/credential control policies should do the following:

(1) Remind employees to keep official keys/credentials on their person or securely locked in a desk or cabinet.
(2) Have a policy against lending keys/credentials to an unauthorized person.
(3) Require employees to promptly return official keys/credentials checked out on a temporary basis.
(4) Require reporting of lost or stolen keys/credentials immediately to the appropriate official.
(5) Establish procedures for collecting keys/credentials from terminated employees, employees on vacation, and vacated tenants.

A.7.5.4.3 Records of key/credential issuance should be secured and kept separate from keys/credentials.

A.7.5.4.3(6) There are many ways to document the acceptance for keys. The recipient can sign the key control record, use a machine readable credential, or be tracked with an electronic key control system.

A.8.1 Research indicates 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.

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.

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.

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.

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 reflectiveness.

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 facility that is being protected.

Δ **A.8.4** 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.

Many multi-building facilities have their own power distribution systems that are nested within a municipality and share a perimeter with one or more serving utilities. Ownership regimes of exterior lighting systems have significant implications for security, such as the following examples:

(1) Roadway lighting systems that are within or on the perimeter of the facility for roads owned by the municipality should be owned and maintained by the municipality. Where these systems illuminate facility roadways, the owner of the roadway typically controls illumination intervals and pays for the energy, operation, and maintenance costs. Such roadway lighting systems, typically governed by the *National Electrical Safety Code* (ANSI/IEEE C2), could be a substitute for security lighting for pedestrians. As a performance-based leading practice document intended for use by serving utilities, ANSI/IEEE C2 has electrical safety requirements closely aligned to meet reliability objectives of the so-called last mile of power distribution. The reliability objectives of ANSI/IEEE C2 mean that grounding wires, service disconnect switches, and overcurrent protection for exterior lighting systems should not be present, thus presenting electrical hazards to pedestrians along with exterior illumination.
(2) Lighting for pedestrian walkways that are on the perimeter but adjacent to streets could be a substitute for roadway lighting, so-called "spillover" light.
(3) Power to fixtures installed along perimeter pedestrian walkways owned by the municipality but receiving power supply from the facility power distribution system is governed by *NFPA 70*, which has long-established requirements for disconnect switches and grounds, originating in its primary objective of premises electrical safety. The safety objectives of *NFPA 70* mean that requirements for grounding wires, service disconnect switches, and overcurrent protection for exterior lighting systems will be present to a larger degree. Unless carefully managed, these electrical safety components could present greater reliability risk to the exterior illumination system.
(4) Parking lot or area lighting systems for buildings on the perimeter should be supplied power from a serving utility but, even with the land owned by the facility, the electrical safety requirements of ANSI/IEEE C2 should apply.

Exterior lighting can be a valuable and inexpensive deterrent to crime, although there is no straight line between security and exterior lighting. The degree to which exterior illumination can contribute to security is contingent upon robust communication among representatives of the host municipality, the serving utilities, and facility officials.

A.8.4.1 Designers and owners should not assume high exterior lighting levels reduce crime, but they should investigate what lighting levels are appropriate for their design goals and security needs based on the SVA.

A.8.4.3 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. 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. 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. The design and construction of buildings also influence the level of security provided. Building exteriors should be designed to eliminate hiding places for criminals. Building facades of glass are vulnerable to bomb blasts; masonry facades are more secure. Some facilities augment these measures with intrusion detection systems, video surveillance, security guards, proprietary monitoring station alarm systems, or explosive and metal detectors.

A.8.4.5 Guard posts should be illuminated to match the intent of the SVA. Some may need to be well lit to deter intrusion, but others may need to be dimly lit to render their positions harder for intruders to pinpoint.

A.8.4.6 A single lamp outage should not result in a dark spot vulnerable to intrusion. Complete reliability should be provided so that in the event of a power failure standby illumination is available.

A.8.4.7 Fixtures should be installed high, be out of reach of potential intruders, and be of the vandal-resistant type.

A.8.4.8 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. Having a maintenance contract can help ensure that repairs are made in a timely fashion.

A.8.5 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. There are several guides for trimming of shrubbery and trees. One example is shrubbery should be kept to a maximum of 3 ft (0.9 m) in height and trees trimmed so that the bottom branches are a minimum of 7 ft (2.1 m) above the ground. This will provide a clear zone of approximately 4 ft (1.2 m) between the top of the shrubbery and bottom branches of the trees for surveillance purposes.

Landscaping can also be used as a deterrent to intrusion. Examples are as follows:

(1) Shrubbery with briars or thorns
(2) Thick plantings that are difficult to penetrate

A.9.4.2.1 All intrusion detection systems have vulnerable points by which their functioning can be minimized or completely interrupted or circumvented. Intrusion detection system vulnerability points should be minimized to accomplish the intent of the SVA.

A.9.4.3.1 Controlling access at one portal might not be enough. The access control system should be designed so that the entire perimeter is protected by the access control system, monitored by personnel, monitored by an intrusion detection system, or locked against ingress.

A.9.4.4.1 Video surveillance system design has to consider the privacy laws enacted by many jurisdictions.

A.9.4.4.3 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 and signs posted where there is no video surveillance should not be used, since they give a false sense of security. Video surveillance can also enhance the effectiveness of security personnel.

A.9.4.4.5 As a means of maintaining video surveillance, damaged components should be replaced as soon as possible and a maintenance program instituted to ensure that components are cleaned and maintained on a regular basis. Having a maintenance contract can help ensure that repairs are made in a timely fashion.

A.9.4.5 Watchclock systems are used when immediate supervision of security personnel is not provided. With this system, watchman stations that are to be visited by security personnel on a regular basis are located along the patrol route. The route is planned so that all major areas of the facility are covered and the stations located so that all potential trouble spots are checked. Watchclock systems can be either portable or stationary.

In a portable system, a key is placed at each station, and security personnel carry on the patrol a portable watchclock that contains a recording medium and a clock mechanism. The recording medium can be either the paper dial used in Newman clocks or the paper tape used in Guardsman clocks, and it is synchronized with the clock mechanism. The dial or tape is divided into hour or minute segments. Dials usually cover a 24-hour period, while tapes can be used for up to 96 hours.

Upon reaching a station during a scheduled round, security personnel insert the key, which is permanently secured to the station, into the watchclock. The keys are coded by location, and raised type on the key makes an embossed record on the dial or tape, indicating the station number and the time of the visit.

If security personnel fail to punch in at a station, the failure is indicated by an obvious space on the dial or tape. To detect unauthorized tampering, a mark is punched on the dial or tape each time a watchclock is opened or closed for any reason.

In a stationary watchclock system, station boxes are installed throughout the facility and connected electrically to a clock installed at a central location. Security personnel carry a small crank-type key that is inserted into each station box. Turning the key operates a small magneto that generates sufficient current to actuate a recording mechanism in the central clock, indicating the time the station was visited.

The effectiveness of a watchclock system is dependent on an auditing program for the dials and tapes. Management must institute a program to check the information on the dials and tapes on a daily basis to ensure that all watchman stations are visited as scheduled and that any irregularities are immediately investigated.

Electronic guard tour monitoring systems are the modern replacement of the old watchclock systems. With these systems, security personnel carry a reading device, which is swiped across or touched to the stations, located at key checkpoints along the patrol route, to electronically record the date, time, and station code.

The stations, which replace the old key stations used in watchclock systems, are small, individually coded boxes. Depending on the system used, the data are stored in magnetic code, bar code, or binary code. The readers are available in a variety of shapes and sizes and tend to be lighter and smaller than watchclocks. They function basically as an electronic clock that is "punched" at each station, and can collect data from 1000 to 2000 stations. Through the use of a modem, tour data can be sent from the station boxes to a central monitoring console.

At the conclusion of their shifts, security personnel turn in the readers, and the supervisor retrieves the information by downloading it into a computer. Through the use of available software, detailed information about a tour can be obtained, such as whether security personnel were early or late to a station, whether a station was visited out of sequence, and how fast a tour was completed.

The ability to program an electronic guard tour monitoring system provides an advantage that is not easily attainable with a standard watchclock system — variable guard tour schedules. Variable guard tour schedules have no set time or location sequence and are useful for deterring criminal activity, since their unpredictable nature can frustrate the planning of an intrusion attempt.

Where continuous reporting of the performance of security personnel is required, a supervisory watchman system can be used. With such a system, the watchman stations are essentially signal transmitters that are electrically connected to a monitoring station. Monitoring station watchman service can provide for supervised tours or compulsory tours.

For supervised tour service, security personnel successively operate, by the use of a key or reader, the stations along the patrol route, with each station causing a unique signal to be transmitted to the monitoring station. Security personnel follow a planned route through the premises and are expected to reach each station at a definite time. Failure to reach a station within a reasonable grace period causes the monitoring station to investigate the failure to signal. By prior arrangement with the monitoring station, the route can be varied so that it is not performed in a set pattern or time frame.

In a compulsory tour system, signals at the beginning and end of each tour are transmitted to the monitoring station. All intermediate stations must be visited in proper order; otherwise, the key or reader that security personnel use at all the stations cannot be used at the last station for a signal to be transmitted. This system results in reduced signal traffic to the monitoring station. In a variation of this system, called a delinquency indicator system, a signal is transmitted only if security personnel do not reach a particular station within a given time frame.

A.10.2.1.2 Some municipalities have enacted legislation that provides specific security requirements for commercial parking facilities.

A.10.2.1.3 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. The typical 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, all available deterrents must be considered. These include adequate lighting, secure perimeters, secure elevators and stairwells, elimination of hiding spaces, and good visibility throughout all parking levels.

A.10.2.2 Patrols of the perimeter and interior areas of the facility by security personnel should be at irregular intervals. 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. 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.

A.10.2.3.1 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.

For public facilities, 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.

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.

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 an unauthorized person.

A.10.2.3.2 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, because screening provides for visibility into the structure from the street and can serve as a deterrent to criminal activity.

A.10.2.4.2 Well-marked parking allows patrons to easily remember where they left their cars, and also helps patrons enter, exit, and use the lot.

A.10.2.4.3 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.

A.10.2.5.1 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.

A.11.1.2.1 Often, the difference between the success and failure of a security plan is realized through management's degree of commitment to and support for the plan.

Ideally, security for assets should be considered during the architectural planning stages. It is then that asset protection measures, including access control systems, can be most economically implemented. Unfortunately, security considerations are often after the fact, occurring only after a building has been designed.

A.11.1.2.3 Because there are many small, rural colleges and many large, urban high schools, it is more applicable to describe security based on needs. These needs vary greatly, based on risks and vulnerabilities. Some schools might conduct chemical, biological, nuclear, radiological, or explosive research. Boarding schools have special security needs, because students are on-site 24 hours per day. A facility can be a building, a campus, a set of campuses, a district, a system, or other centrally managed organization, such as a county. The SVA should be detailed enough to cover each building and each major department or division of the educational system.

A security assessment that is tailored for primary and secondary schools can be found at www.passk12.org.

A.11.1.2.3.1 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 has deteriorated. A history of violent and property crime in the immediate neighborhood and on the premises should be compiled and reviewed.

A relationship with local law enforcement agencies should be developed to make them familiar with the property. The local police should be requested to include the facility in patrol routes. 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.

Management should be active in local security associations or industry trade groups as a means of sharing common security concerns and solutions. Management should consider joining emergency response organizations, including the Department of Homeland Security Information Sharing Network (DHS INFO), which sends members real-time threat information via e-mail, pagers, and cell phones.

A.11.1.3.2(3)(d) The disaster potential inherent in the telephoned bomb threat warrants inclusion of this disaster contingency in the Educational Emergency Management Plan. Experience has shown that facility personnel have to accompany police or military bomb demolition personnel in searching for the suspected bomb, because speed is of the essence and only individuals familiar with a given area can rapidly spot unfamiliar or suspicious objects or condition in the area. This is particularly true in educational facilities. The person receiving the threat needs to obtain as much information as possible from the caller concerning the location of the supposed bomb, time of detonation, and other essential data, which have to be considered in deciding whether to evacuate all or part of the facility.

Δ **A.11.1.3.2(7)(e)** Due to a rise in active shooter incidents, many schools have instituted protocols to protect the students and faculty from both internal and external threats. The security plan should detail how to implement such protocols in a way that is both practical and practicable.

During school lockdowns, all exterior doors and windows are locked or otherwise secured against entry, lights are turned off, and blinds (where provided) are closed to restrict visual access to the interior. Occupants should stay low and away from windows and doors. Hallways, bathrooms, and any areas that cannot be secured should be cleared. Take all students, faculty, and visitors/vendors into account. Remain in place until an all clear from authorized personnel is given.

During school lockouts, all exterior doors are locked and the main entrance is monitored by an administrator, administrator designee, security officer, or school resource officer. This procedure allows the school to continue with normal inside activity but restricts outside activity.

Shelter-in-place is the use of a structure and its indoor atmosphere to temporarily separate individuals from a hazardous outdoor environment.

Confusion needs to be minimized when any of these protocols are implemented. Schools, particularly large campuses, have many groups of people who might need to have access during a lockdown, such as campus police, local police, fire, ambulance, management, counselors, emergency responders, and senior administrators. It is important that these groups and their means of access be described and documented, since several departments could be responsible for the protocols.

See FEMA 428, *Primer for Design Safe Schools Projects in Case of Terrorist Attacks,* for material on shelter-in-place.

N **A.11.1.3.2(9)** The security drills should be rotated to effectively cover each drill type.

A.11.2.1.1.2 In unoccupied offices or rooms, purses should not be left on top of desks or on the floor, and wallets and checkbooks should not be left in jackets.

A.11.2.1.1.3 Security awareness training should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

N **A.11.2.1.3.1** In this context, “monitored” is intended to mean visitors must go through the visitor management procedure as defined by the SVA.

A.11.2.1.4 When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors' or contractors' management about their preemployment screening and drug testing practices. These service providers could be treated either as employees or as visitors, depending on the contract and contact. For example, dining service contract employees might be treated similarly to regular employees, whereas a package delivery service might be considered a visitor.

A.11.2.1.5.1 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.

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.

A campus security department is often 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.

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.

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.

A.11.3.4.4 While a campus can be viewed as an open environment where students, visitors, and staff can roam freely, a portal control program should be implemented to permit authorized individuals to come and go with ease, while restricting access to unauthorized persons. 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.

N **A.11.3.4.7** The locking hardware is intended to not be disabled by an electronic means.

A.11.4 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?

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

A.11.4.2 The impact of vandalism is felt in many areas within a school, including graffiti on walls, breakage of windows, and 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, because 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.

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.

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

Studies have indicated that schools that are lax or unfair in the area of discipline have the most serious vandalism problems. Therefore, schools should enforce specific, even, and reasonable disciplinary actions.

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).

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.

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.

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

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.

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 life safety requirements, ground floor windows should be protected with wire mesh screening or the glazing replaced with burglary-resistant glazing materials.

Strict control of keys/credentials 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.

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

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.

If video surveillance systems are used, they should be tested in order to provide "recognition," and preferably "identification" of the subject.

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.

Parking areas should be designated for employees, students, or visitors. Surveillance of these areas, whether by patrols or cameras, will serve as a deterrent to the vandalism of vehicles. Controlling access to the parking areas, as well as posting allowable parking hours, can reduce the vulnerability, reduce the need for patrols, and increase the effectiveness of video surveillance after-hours.

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.

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.

A.11.5.2.1.2 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. 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.

A.11.5.2.1.3 Communication should also be established with local police agencies, fire departments, ambulance, and relevant county, state and federal agencies. Emergency responder 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.

A.11.5.3 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 video surveillance systems and intrusion alarms.

A.11.5.3.2 Intrusion detection systems 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.

A.11.5.3.3 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 machine readable credentials from the system.

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 or thousands of locks. In these systems, a machine readable credential serves as a key to operate the lock on a door. The same principles of key control apply to the issuance of machine readable credentials.

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, and meal-plan card.

When using an access control system, all exterior entrances should be connected on-line with real-time control and monitoring, or be signed and mechanically restricted as exit-only.

A.11.5.3.4 Video surveillance systems are widely used 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. Recorded video can be studied to determine access control and traffic patterns and reviewed for evidence of a crime.

A.11.6.2 Each of these considerations would be implemented based on the SVA.

A.11.6.2(8) The main entrance could have an intercom system or be staffed with a receptionist, a security guard, or another attendant.

A.11.6.3 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 any educational research laboratories that handle materials that could be used for chemical, biological, radiological, nuclear, and/or explosive 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.12.1.2.1 A health care facility security plan might be formulated from security-sensitive areas that need the highest level of protection outward to the perimeter of the health care facility campus in concentric rings. Viewed from the outside, security is thus open and welcoming to patients and visitors. As a person proceeds into the interior, public spaces might have minimum surveillance, but those sensitive areas that cannot be entered are layered with protections and countermeasures.

A.12.1.3.2(3)(c) The disaster potential inherent in a telephoned bomb threat warrants inclusion of this disaster contingency in the Health Care Emergency Management Plan. Experience has shown that facility personnel have to accompany police or military bomb demolition personnel in searching for the suspected bomb, because speed is of the essence and only people familiar with a given area can rapidly spot unfamiliar or suspicious objects or conditions in the area. This is particularly true in health care facilities. The facility switchboard operator has to be provided with a checklist to be kept available at all times, in order to obtain as much information as possible from the caller concerning the location of the supposed bomb, time of detonation, and other essential data, which have to be considered in deciding whether to evacuate all or part of the facility.

A.12.2.1.3 Patients who generate media interest should have special security procedures. VIP or media representatives bring a unique set of security requirements. Protection of VIPs is normally accomplished by restricting the use of names on charts and rooms and by assigning a dedicated security watch. Admission of a high-profile person to a health care facility creates two sets of problems that might require partial activation of the Health Care Emergency Management Plan: security and reception of news media. Provision of security forces in this situation might be provided by a governmental agency or private security forces. However, activation of facility security forces might be required to prevent curious onlookers from entering facility work areas and interfering with routine facility functioning. Routine visiting privileges and routine visiting hours might need to be suspended in parts of the facility.

A.12.2.1.3.2.2 An escort can control movement of media personnel in the facility.

A.12.2.1.4 Crowd control of persons demanding access to care will create additional demands on security. Because of the intense public interest in disaster casualties, news media representatives should be given as much consideration as the situation will permit. Ideally, news media personnel should be provided with a reception area, with access to telephone communication and, if possible, an expediter who, though not permitted to act as spokesman for news releases, could provide other assistance to the news media. The marketing department of the hospital might be best suited to assist security personnel with media control. News media personnel should not be allowed into the health care facility without proper identification. To alert off-duty health care staff and to reassure the public, use of broadcast media should be planned. Media representatives should be requested to wear some means of identification for security purposes. Where feasible, photo identifications or other means to ensure positive identification should be used. Visitor and crowd control creates the problem of distinguishing staff from visitors. Such identification should be issued to all facility personnel, including volunteer personnel who might be utilized in disaster functions. Note that care should be taken to ensure that identification badges are recalled whenever personnel terminate association with the health care facility. Members of the news media should be asked to wear some means of identification, such as press cards, on their outside garments so that they are readily identifiable by security guards controlling access to the facility or certain areas therein. Clergy also frequently accompany casualties or arrive later for visitations and require some means of identification.

A.12.3.1.2.1(1) A visible presence is normally accomplished by the placement of a Security Officer at the ambulance entrance. This serves a dual purpose for monitoring the cameras throughout the Emergency Department as well as the activity at the ambulance entrance.

A.12.3.1.2.2(5) The facility-wide alerting system should be activated for all reports of pediatric or infant abduction. The use of a standardized code alert system can facilitate the announcement, for example, "Code Pink" for an infant abduction or "Code Purple" for a pediatric abduction.

A.12.3.1.2.3 Video surveillance and motion detection can be used as additional protection for these areas. Certain controlled drugs might need to be stored in safes or electronically-controlled medication dispensing systems.

Δ **A.12.3.1.2.5(3)** Examples of contraband can be items such as tobacco, drugs, tools, or weapons that could cause harm to the patient or others as determined by staff.

A.14.1.1 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. 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.

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.

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.

A.14.1.2.1 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 effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.14.2.1 An effective security program is dependent on coordination and communication between management, security personnel, and employees. 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 receive specialized training in diplomacy. Training should be an ongoing effort.

A.14.2.1.4.3 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. Public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, and the routes to them should be included in security patrols. 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.

A.14.2.2 Deliveries to guest rooms should be screened by front desk personnel. Messengers should not be allowed to roam the building freely.

A.14.2.3.3.3 Front desk personnel make an effort to retrieve keys/credentials from guests when they check out. A well-secured key/credential-return box should be provided in the lobby as a reminder to, and for the convenience of, guests to return keys/credentials. Electronic guest room key/credential systems automatically re-key each time a new guest checks into a room.

A.14.3.1.2 Although open to the general public, a lodging facility is a private property. Management is responsible for monitoring and controlling the access of persons onto the premises.

A.14.3.1.3 Guest rooms and guest room corridors are not considered open to the general public, and management should limit access by those who are not guests or invitees of guests. The normal laws of trespass apply to these areas, and local laws should be consulted.

A.14.3.1.4 Access routes to public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, should be controlled, and doors to these rooms should have the ability to be locked.

A.14.3.2.1 There should be a program to ensure that during nighttime hours all remote or unattended entrances are locked. Video surveillance can be used to monitor these entrances.

A.14.3.3.1(4) 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. (25.4 mm) deadbolt and automatic retraction of the latch and bolt for life safety.

A.14.3.3.1(5) Auxiliary locking devices include a safety chain or a night latch that can be opened only from the inside.

A.14.3.3.1(8) 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.

A.14.4 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) If the exterior design of the facility creates areas of concealment, the spaces should be illuminated or secured.

A.14.5.2 Some examples of this type of protection for elevator cars are convex or plain mirrors or video surveillance.

A.15.1.1 It is not intended to include the individual dwelling units that are owner-occupied in townhouses, condominiums, or other similar owner cooperatives. These owner-occupied units follow the recommendations in Annex C for one- and two-family dwellings.

Building management or the owners' association can have responsibility for common areas, including but not limited to elevators, parking garages, laundry rooms, and recreational facilities.

A.15.1.2.1 An effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.15.1.2.2.1 In performing an SVA of a residential 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

A.15.1.3 A relationship with local law enforcement agencies should be developed to make them familiar with the property. The local police should be requested to include the facility in patrol routes. An open line of communication should be maintained with the local police to obtain information on crime and crime trends in the neighborhood or area.

Management should be active in industry trade groups or owners' associations as a means of sharing common security concerns and solutions.

A.15.2.1.1.1 Background checks, including criminal record checks, are especially important for employees with access to rental units.

A.15.2.1.1.2.2 The crime prevention section of the local police department can usually provide assistance.

A.15.2.1.1.3 Signs of vandalism on the exterior of the building or of homeless people living on or around the property should be reported.

A.15.2.1.2 Investigation of tenant references and employment history are recommended.

A.15.2.1.3 The identity of service personnel should be verified.

A.15.2.1.4.3 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, common areas, and storage, receiving, and trash disposal areas. Public areas, including laundry rooms, exercise rooms, swimming pools, and so forth, and the routes to them should be included in security patrols.

A.15.2.4 A "No Cash Accepted" sign posted in a conspicuous place can cut down on the threat of robbery.

A.15.3.1.2(2) Tenants should be instructed to ascertain the identity of visitors before using the intercom to buzz in callers.

A.15.3.1.2(3) Controlled access to the roof includes that from a fire escape or adjoining building.

A.15.3.2.1 There should be a program to ensure that during nighttime hours all remote or unattended entrances are locked. Video surveillance can be used to monitor these entrances.

A.15.3.3.2 Dwelling unit doors should have no evidence of prior forced-entry attempt. Door glazing and side glass at entrance doors should be protected against breakage.

A.15.4.4 Fencing around the exterior boundary of the property should be maintained. Shrubs and foliage should be trimmed to reduce hiding spaces.

A.15.5.2 Some examples of this type of protection for elevator cars are convex or plain mirrors or video surveillance.

A.16.1.2.2 A security program for restaurants should be designed to control robbery and burglary, the crimes to which they are most susceptible.

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 are 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

A.16.2.1.2 Employee training should include the proper use of security equipment, including prominently displayed surveillance cameras, silent holdup alarm systems, and bullet-resisting vision windows and deal trays for drive-through windows.

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.

A.16.2.1.2.1 Employees should be trained on what to do before, during, and after a robbery.

A.16.2.1.2.2 Delivery personnel should be provided with training on how to evaluate the risks in a given situation.

A.16.2.1.3 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 should 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.

A.16.3.2 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 are to be considered to ensure employee safety.

A.16.3.3.2 The correct type and class of safe or vault must 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 greater the values to be protected, a correspondingly higher level of protection has to be afforded by the safe. Refer to E.5.3 for safes and their various protection classifications to determine the appropriate safe to use.

A.16.3.4.1 Many robberies occur through the back door.

A.16.4 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 locations 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.

A.16.4.1.1 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 must be varied. A sign 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 should be posted.

A.16.4.1.2 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, crow-barring doors or windows, and breaking window glass. Some burglars have resorted 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.

A.16.4.3.2 Adequate outside lighting of the parking area and approaches during nighttime hours of operation enhances employee and customer protection.

A.16.4.5 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.

A.16.5.3.2.1 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. 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 might scare off the burglar.

A.17.1.1 Since there are many different types of shopping centers (e.g., enclosed malls, open-air centers, neighborhood centers, and strip malls), and their locations warrant different security measures, no single set of security measures can apply to all shopping centers.

A.17.1.2.1 Because shopping centers 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 effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.17.1.3(3) The SVA can help determine the need for physical security measures, such as fencing, lighting, video surveillance, and access control systems.

A.17.1.3(4) 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.

A.17.1.3(5) 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.

A.17.2.1.2 One way to provide notification is by monthly newsletter.

A.17.2.1.3.1 Management will regularly review its security needs and provide personnel to respond to emergencies and assist customers and employees as required. If contract security is utilized, the security contractor is responsible for the selection, training, and supervision of personnel and for complying with all state and local laws, rules, and regulations.

A.17.2.1.3.3 Management should consider having some of their security personnel visible, in an effort to deter criminal activity. 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, exit and delivery corridors, and storage, receiving, and trash disposal areas. 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.

A.17.3 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.

A.17.4 The security program for a shopping center often starts at the architect's desk. Every developer and architect must consider security requirements and potential security problems when designing a new shopping center or expanding or renovating an existing facility.

A.17.4.3 Lighting is basic to any security program. Local ordinances and building codes can mandate lighting requirements.

A.17.4.4 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 should consider providing a clear zone between the tops of shrubbery and the bottom branches of the trees, for surveillance purposes.

A.17.5.3.3 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 must 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.

A.17.6 Because of the significant risks they pose, parking facilities are to be afforded special consideration.

A.18.1.2.1 A security program for retail establishments should be designed to control employee theft, robbery, burglary, shoplifting, fraud, and workplace violence. 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 effective security plan cannot stop all crime. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.18.1.2.3 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.

A.18.2.1.1.2.2(1) Having at least two employees on duty during high-risk hours and at opening and closing times will serve as deterrents to robbery.

A.18.2.1.1.3 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. An analysis of the opportunities for theft within a company must be performed so that strategies can be developed to reduce or limit the exposure. In any event, the application of these procedures and devices must be performed with the knowledge and agreement of employees; otherwise, there can be a damaging effect on employee morale and productivity.

A.18.2.1.1.3(2) For example, the person who has the authority to write checks and make deposits cannot be responsible for reconciling the bank statement.

A.18.2.1.2.1 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 retail establishment 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.

Procedural controls are intended to eliminate the opportunity for shoplifting. The physical layout of the store should be such that it discourages shoplifting. High value merchandise cannot be located near doors, and aisles should not be cluttered. 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 but not in violation of life safety and building codes. Customers are not allowed to use fire exits except in an emergency. Prevention methodologies, such as convex mirrors and video surveillance, should also be considered.

Generally, the most important element of a shoplifting prevention program is the arrest and prosecution of shoplifters who will not otherwise be deterred. Prosecution not only serves to impress upon the person arrested that shoplifting will not be tolerated by the store, but it establishes an attitude that becomes known in the community.

Because of ignorance of the law and fear of lawsuits, many retail businesses are reluctant to detain or arrest shoplifters. What begins as the 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.

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.

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 doing all of the following:

(1) Taking the merchandise
(2) Concealing it without having paid for it
(3) Ditching the merchandise

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.

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.

Most 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.

A.18.2.1.2.2.1 Because of the risk of check fraud, some retail businesses have a policy of not accepting checks as payment for goods. The check policy should be posted in a location readily seen by customers.

A.18.2.1.2.2.2(3) Third-party checks such as payroll or government checks can be easily stolen.

A.18.2.1.2.3 Elements of the policy should include requiring 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.

A.18.2.1.3 When outside services (contractors, vendors, or other personnel) are used, management should ask the vendors' or contractors' management about their preemployment screening and drug testing practices.

A.18.2.1.4.1 Performing regular reviews of security procedures keeps management 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 needs to also review all security-related incidents and complaints and how they were resolved.

Management will regularly review its security needs and provide personnel to respond to emergencies and assist customers and employees as required. If contract security is utilized, the security contractor is responsible for the selection, training, and supervision of personnel and for complying with all state and local laws, rules, and regulations.

A.18.2.1.4.3 Management should consider having some of their security personnel visible, in an effort to deter criminal activity. 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, exit and delivery corridors, and storage, receiving, and trash disposal areas. 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.

A.18.2.4 Retail establishments, in particular establishments that operate late at night, will benefit from an examination of their workplaces to determine if workplace violence is a potential hazard for their employees.

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 will 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.

Employee security training should include workplace violence policies. This can be particularly true for employees working at night in retail establishments when higher-level managers are not routinely on duty.

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

Employees in some retail establishments are 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.

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.

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.

Because the major risk of death or serious injury to retail employees is from robbery-related violence, an effective prevention program will 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)

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.

A.18.3.2 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, are to be considered to ensure employee safety.

A.18.4.1.1 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 must be varied. Post a sign 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.

A.18.4.1.2 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, crow-barring doors or windows, and breaking window glass. Some burglars have resorted 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.

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 locations 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.

A.18.4.1.3 The right type and class of safe or vault must 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 the level of protection afforded by the safe should be. UL has listings for safes in various protection classifications. The number of people with access to the combination must be kept to a minimum. The combination number may not be stored in an easily accessible place, such as a desk blotter, and the safe or vault must never be put in "day

mode," in which only one number is needed to complete the combination. The combination must be changed on a regular basis.

A.18.4.3 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. Local ordinances and building codes can mandate lighting requirements.

A.18.4.4 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 should consider providing a clear zone between the tops of shrubbery and the bottom branches of the trees, for surveillance purposes.

A.18.4.5 Clear visibility into the store can serve as a deterrent to robbery because it will enable passersby and police patrols to observe activities inside. It will also enable employees to observe suspicious activities outside the store.

A.18.5.3.2 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. 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 might scare off the burglar.

A.18.5.3.3 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 must 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.

A.18.6 Because of the significant risks they pose, parking facilities are to be afforded special consideration.

A.19.1.1 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' access should be restricted.

A.19.1.1.2 Security for buildings listed in 19.1.1.1 should be designed according to the requirements of the U.S. Department of Justice (DOJ) publication, *Vulnerability Assessment of Federal Facilities*.

A.19.1.2.1 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.

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.

An effective security plan cannot stop all crime. Sales personnel should be advised not to make oral promises regarding the security of the facility. Advertising literature, promotional releases, and so forth, should not make unsupported claims about the safety or security of the facility.

A.19.1.3.2(6) 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 has deteriorated. A history of violent and property crime in the immediate neighborhood and on the premises should be compiled and reviewed.

A relationship with local law enforcement agencies should be developed to make them familiar with the property. The local police should be requested to include the facility in patrol routes. 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.

Management should be active in local security associations or industry trade groups as a means of sharing common security concerns and solutions. Management should consider joining emergency response organizations, including the Department of Homeland Security Information Sharing Network (DHS INFO), which sends members real-time threat information via e-mail, pagers, and cell phones.

A.19.2 Contact information should be posted where it can always be seen. If the reception desk is constantly attended, the information may be posted there, but otherwise contact information should be visible from the exterior of the building.

A.19.2.1.1.2 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.

A.19.2.1.1.3 Security awareness should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

A.19.2.1.1.4 One way to provide notification is by monthly newsletter.

A.19.2.1.2.1 The person requested by the visitor should confirm the appointment. If policy requires it, visitors should be escorted to their destination.

A.19.2.1.2.2 It should be noted that if employees are not required to wear badges, visitors have only to remove theirs to look like employees.

A.19.2.1.3 Contractors, maintenance, housekeeping, and other vendors should display identification badges acceptable to facility management. 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. Maintenance, housekeeping, and other service personnel who operate on all floors or areas of the building should be issued distinctive uniforms and identification badges. The supply of uniforms and badges should be controlled.

A.19.2.2 A messenger center for packages, lunches, and other deliveries should be established. Messengers should not be allowed to roam the building freely.

A.19.3.1.2 A door of solid construction should be used to secure loading openings. 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 machine readable credentials. The freight elevator doors leading into the shipping and receiving area should be secured during periods of nonuse.

A.19.3.1.3 Different business settings or structures, such as high-rise office buildings or campus-style settings of multiple buildings, require different access control approaches.

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.

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.

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.

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.

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.

A.19.3.2.1 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. Visitors should be funneled to the reception desk and not be able to access secure areas without proper authorization.

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 receptionist or guard should be stationed at the desk when the building is open.

If there is an automated access control system for employees, the entrance should be located as close as is practical to the reception desk. If there is no automated access control system, a guard or receptionist should check employee identification.

A.19.3.2.2 Perimeter entrances should be secured during nonbusiness hours. Entry point(s) should be designated for after-hours access. A program exists to ensure that entrances that are not needed for entry or exit are secured.

A.19.3.2.3 Emergency exits should be alarmed and monitored to detect unauthorized use.

A.19.5.2 Some examples of this type of protection for elevator cars are convex or plain mirrors or video surveillance.

A.19.5.3.4 Twenty-four-hour video surveillance and recording are desirable 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.

A.20.1.2.2.1 A facility safety plan and a security plan often address the same or similar concerns. Many 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.

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

Sites that are close to other structures or facilities may be vulnerable from shared perimeters, buildings that are close together, or hazardous processes. Some hazardous materials or processes can be particularly attractive targets because of the potential for greater consequences.

Older buildings might be more vulnerable because they have more windows, while some newer buildings are designed for easy access. 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.

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.

A.20.1.2.2.2 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.

A.20.2.1.1 Maintaining good labor relations will help to protect the facility from actions by employees or contractors. Important labor relations considerations are as follows:

(1) Open negotiations
(2) Workplace policies emphasizing that violence and substance abuse are not tolerated
(3) Adequate training and resources

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.

A.20.2.1.1.2 Security awareness training should be provided. Training should provide up-to-date information covering security practices, employee security awareness, personal safety, and so forth.

A.20.2.1.1.3 Emergency shutdown procedures should be included as part of the written operating procedures. 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.

A.20.2.1.2.2 It should be noted that if employees are not required to wear badges, visitors have only to remove theirs to look like employees.

A.20.2.2.2 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. Another practice to consider is substituting less hazardous substances when possible to make processes inherently safer.

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.

Δ **A.20.3.2** IES G-1, *Guideline for Security Lighting for People, Property, and Public Spaces,* is for design and implementation of security lighting. The guideline is intended for use by property owners and managers, crime prevention specialists, law enforcement and security professionals, risk managers, lighting specifiers, contractors, the legal profession, and homeowners concerned about security and the prevention of crime. It covers basic security principles, illumination requirements for various types of properties, protocol for evaluating current lighting levels for different security applications, and security survey and crime search methodology. Guidelines include exterior and interior security lighting practices for the reasonable protection of persons and property. There are many complexities to exterior lighting design, including but not limited to "dark sky" compliance, light wash through adjacent properties, and energy conservation. Proper illumination should encourage authorized users to occupy spaces and discourage intruders.

Annex B Homeland Security Advisory System

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

B.1 General. A recommended threat response elevation system was originally developed by the United States Department of Homeland Security (DHS). As threat conditions rise, it is recommended that facilities implement an appropriate corresponding set of protective measures to further reduce vulnerability and increase response capability.

The following threat response recommendations are voluntary.

B.2 Threat Conditions and Associated Protective Measures. There is always a threat of a terrorist attack. Each threat condition assigns a recommended level of alert appropriate to the increasing risk of terrorist attacks. Threat conditions contain suggested protective measures that the government and the public can take, recognizing that the heads of federal departments and agencies are responsible for developing and implementing appropriate agency-specific protective measures.

B.2.1 Normal Condition. A normal condition is when there is a low risk of terrorist attacks. The private sector should consider the following protective measures:

(1) Refine and exercise prearranged protective measures.
(2) Ensure that personnel receive proper training on the Homeland Security Advisory System and specific prearranged department or agency protective measures.
(3) Institute a process to ensure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks and that all reasonable measures are taken to mitigate these vulnerabilities. Homeowners and the general public can develop a household disaster plan and assemble a disaster supply kit.
(4) Check communications with designated emergency response or command locations.
(5) Review and update emergency response procedures.
(6) Provide the public with any information that would strengthen its ability to act appropriately.

Homeowners and the general public, in addition to the actions taken for the low threat condition, should take the following steps:

(1) Update their disaster supply kits.
(2) Review their household disaster plans.
(3) Hold household meetings to discuss what members would do and how they would communicate in the event of an incident.
(4) Develop more detailed household communications plans.
(5) If they are apartment residents, discuss with building managers steps to be taken during an emergency.
(6) If they have special needs, discuss their emergency plans with friends, family, or employers.
(7) Increase surveillance of critical locations.
(8) Coordinate emergency plans with nearby jurisdictions as appropriate.
(9) Assess whether the precise characteristics of the threat require the further refinement of prearranged protective measures.
(10) Implement, as appropriate, contingency and emergency response plans.

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Be observant of any suspicious activity and report it to authorities
(2) Contact neighbors to discuss their plans and needs
(3) Check with school officials to determine their plans for an emergency and procedures to reunite children with parents and caregivers
(4) Update household communications plans

B.2.2 Elevated Condition. An elevated condition is declared when there is a credible threat risk. In addition to the measures taken in the previous threat conditions, the private sector should consider the following protective measures:

(1) Coordinate necessary security efforts with federal, state, and local law enforcement agencies, the National Guard, or other security and armed forces.
(2) Take additional precautions at public events, possibly considering alternative venues or even cancellation.
(3) Prepare to execute contingency procedures, such as moving to an alternative site or dispersing the workforce.
(4) Restrict access to a threatened facility to essential personnel only.

Homeowners and the general public, in addition to the actions taken for the normal threat conditions, should take the following steps:

(1) Review preparedness measures (including evacuation and sheltering) for potential terrorist actions, including chemical, biological, and radiological attacks.
(2) Avoid high-profile or symbolic locations.
(3) Exercise caution when traveling.

B.2.3 Imminent Condition. An imminent condition reflects a credible, specific, and imminent threat risk. Under most circumstances, the protective measures for an imminent condition are not intended to be sustained for substantial periods of time. In addition to the protective measures in normal and elevated threat conditions, the private sector should consider the following general measures:

(1) Increase or redirect personnel to address critical emergency needs.
(2) Assign emergency response personnel and pre-position and mobilize specially trained teams or resources.
(3) Monitor, redirect, or constrain transportation systems.
(4) Close public and government facilities not critical for continuity of essential operations, especially public safety.

Homeowners and the general public, in addition to the actions taken for the previous threat conditions, should take the following steps:

(1) Avoid public gathering places such as sports arenas, holiday gatherings, or other high-risk locations.
(2) Follow official instructions about restrictions to normal activities.
(3) Contact employers to determine status of work.
(4) Listen to the radio and TV for possible advisories or warnings.
(5) Prepare to take protective actions such as sheltering-in-place or evacuation if instructed to do so by public officials.

B.3 Preparing for Terrorism. Wherever they are, individuals should be aware of their surroundings. The very nature of terrorism suggests there might be little or no warning.

B.3.1 Individuals should take the following steps:

(1) Take precautions when traveling.
(2) Be aware of conspicuous or unusual behavior.
(3) Do not accept packages from strangers.
(4) Do not leave luggage unattended.
(5) Promptly report to police or security personnel unusual behavior, suspicious packages, and strange devices.
(6) Do not be afraid to move or leave if you feel uncomfortable or if something does not seem right.
(7) Learn where emergency exits are located in buildings you frequent. Notice where exits are when you enter unfamiliar buildings. Plan how to get out of a building, subway, or congested public area or traffic. Note where staircases are located. Notice heavy or breakable objects that could move, fall, or break in an explosion.
(8) Assemble a disaster supply kit at home and learn first aid. Separate the supplies to take if evacuation is necessary, and put them in a backpack or container, ready to go.
(9) Be familiar with different types of fire extinguishers and how to locate and use them. Know the location and availability of hard hats in buildings in which you spend a lot of time.

B.3.2 Private sector facilities should take the following steps:

(1) Consider all the precautions prescribed for individuals.
(2) Develop written policies and procedures for terrorist events, train all personnel to them, and test their effectiveness.
(3) Provide a prepared on-site area of refuge for guests and employees should an off-site consequence prevent travel from the facility. Preparations should include provision of nonperishable food and drinking water, battery-powered commercial radio or television, first aid supplies, sanitation supplies, flashlights, and so forth.

B.4 Protection Against Cyber Attacks. Cyber attacks target computer or telecommunication networks of critical infrastructures such as power systems, traffic control systems, or financial systems. Cyber attacks target information technologies (IT) in three different ways. The first type of attack is a direct attack against an information system through the wires alone (hacking). The second type of attack takes the form of a physical assault against a critical IT element. The third type of attack originates from the inside as a result of a trusted party with access to the system compromising information.

Both individuals and private sector facilities should be prepared for the following situations:

(1) To be without services that people normally depend on and that could be disrupted — electricity, telephone service, natural gas, gasoline pumps, cash registers, ATM machines, and Internet transactions
(2) To respond to official instructions (such as general evacuation, evacuation to shelter, or shelter-in-place) if a cyber attack triggers other hazards, for example, hazardous materials releases, nuclear power plant incident, dam or flood control system failures

B.5 Preparing for a Building Explosion. Explosions can collapse buildings and cause fires. Both individuals and private sector facilities can do the following:

(1) Regularly review and practice emergency evacuation procedures.
(2) Know where emergency exits are located.
(3) Keep fire extinguishers in proper working order. Know where they are located and learn how to use them.
(4) Learn first aid.

Additionally, private sector facilities should keep the following items in a designated place on each floor of the building:

(1) Portable, battery-operated radio and extra batteries
(2) Several flashlights and extra batteries

(3) First aid kit and manual
(4) Several hard hats
(5) Fluorescent tape to rope off dangerous areas

B.6 Bomb Threats. If a bomb threat is received, get as much information from the caller as possible. Keep the caller on the line and record everything that is said. Then notify the police and facility security.

Following notification of a bomb threat, do not touch or handle any suspicious packages. Clear the area around suspicious packages and notify the police immediately. In evacuating a building, avoid windows, glass doors, and other potentially hazardous areas. Building evacuation procedures should keep sidewalks and streets to be used by emergency officials or others still exiting the building clear and unobstructed.

B.6.1 Suspicious Parcels and Letters. Be wary of suspicious packages and letters. They can contain explosives or chemical or biological agents. Be particularly cautious at high-profile facilities.

Over the years, postal inspectors have identified certain characteristics that ought to trigger suspicion about a parcel, including the following:

(1) An unexpected delivery or from someone unfamiliar
(2) No return address or one that cannot be verified as legitimate
(3) Marked with restrictive endorsements, such as "Personal," "Confidential," or "Do Not X-Ray"
(4) Protruding wires or aluminum foil, strange odors, or stains
(5) City or state in the postmark that does not match the return address
(6) Unusual weight given its size, lopsidedness, or odd shape
(7) Marked with threatening language
(8) Inappropriate or unusual labeling
(9) Excessive postage or excessive packaging material such as masking tape and string
(10) Misspellings of common words
(11) Addressed to someone no longer with the organization or otherwise outdated
(12) Incorrect titles or title without a name
(13) Not addressed to a specific person
(14) Handwritten or poorly typed addresses

With suspicious envelopes and packages other than those that might contain explosives, take the following additional steps against possible biological and chemical agents:

(1) Refrain from eating or drinking in a designated mail-handling area.
(2) Place suspicious envelopes or packages in a plastic bag or some other type of container to prevent leakage of contents. Never sniff or smell suspect mail.
(3) If you do not have a container, then cover the envelope or package with anything available (e.g., clothing, paper, trash can) and do not remove the cover.
(4) Leave the room and close the door or section off the area to prevent others from entering.
(5) Wash your hands with soap and water to prevent spreading any hazardous substance to your face.
(6) If you are at work, report the incident to facility security officials, who should notify police and other authorities without delay.
(7) List all people who were in the room or area when the suspicious letter or package was recognized. Give a copy of this list to both local public health authorities and law enforcement officials for follow-up investigations and advice.
(8) If you are at home, report the incident to local police without delay.

B.6.2 Explosion. In the event of an explosion, the following actions should be taken:

(1) Evacuate the building as quickly as possible.
(2) Instruct personnel to do the following:
    (a) Do not stop to retrieve personal possessions or make phone calls.
    (b) Get under a sturdy table or desk if debris and other objects are falling.
    (c) Leave quickly after debris has stopped falling; watch for weakened floors, stairs, and additional falling debris as you exit.

B.6.3 Fire. In the event of a fire, the following actions should be taken:

(1) Stay low to the floor and exit the building as quickly as possible.
(2) Cover nose and mouth with a wet cloth.
(3) When approaching a closed door, use the back of the hand to feel the lower, middle, and upper parts of the door. Never use the palm or fingers to test for heat: burning those areas could impair your ability to escape a fire (i.e., using a ladder and crawling).
(4) If the door is NOT hot, open it slowly and make sure that fire or smoke is not blocking the escape route. If the escape route is blocked, shut the door immediately and use an alternative escape route, such as a window. If the escape route is clear, leave immediately through the door. Be prepared to crawl — smoke and heat rise, causing the air near the floor to be cleaner and cooler.
(5) If the door is hot, do NOT open it. Escape through a window. If you cannot escape, hang a white or light-colored sheet outside the window, alerting fire fighters to your presence.
(6) Thick smoke and poisonous gases collect first along the ceiling. Stay below the smoke at all times.

B.6.4 Trapped in Debris. In the event you are trapped by debris, the following actions should be taken:

(1) Do not light a match or lighter.
(2) Do not move about or kick up dust. Cover your mouth with a handkerchief or clothing.
(3) Rhythmically tap on a pipe or wall so that rescuers can hear where you are. Use a whistle if one is available. Shout only as a last resort when you hear sounds and think someone will hear you — shouting can cause inhalation of dangerous amounts of dust.

B.7 Chemical and Biological Weapons. In the event of a chemical or biological weapon attack, authorities will provide instructions on the best course of action. This can be to evacuate the area immediately, to seek shelter at a designated location, or to take immediate shelter where you are and seal the premises. The best way to protect yourself is to take emergency preparedness measures ahead of time and to get medical attention, if needed, as soon as possible.

B.7.1 Chemical Weapons. Chemical warfare agents are poisonous vapors, aerosols, liquids, or solids that have toxic effects on people, animals, or plants. They can be released by bombs; sprayed from aircraft, boats, or vehicles; or used as a liquid to create a hazard to people and the environment. Some chemical agents are odorless and tasteless. They can have an immediate effect (a few seconds to a few minutes) or a delayed effect (several hours to several days). While potentially lethal, chemical agents are difficult to deliver in lethal concentrations. Outdoors, the agents often dissipate rapidly. Chemical agents are also difficult to produce.

The six types of agents are as follows:

(1) Lung-damaging (pulmonary) agents such as phosgene
(2) Cyanide
(3) Vesicants or blister agents such as mustard
(4) Nerve agents such as GA (tabun), GB (sarin), GD (soman), GF (cyclosarin), and VX
(5) Incapacitating agents such as BZ
(6) Riot-control agents (similar to Mace)

B.7.2 Biological Weapons. Biological agents are organisms or toxins that can kill or incapacitate people, livestock, and crops. The three basic groups of biological agents that would be likely to be used as weapons are bacteria, viruses, and toxins.

Bacteria are small free-living organisms that reproduce by simple division and are easy to grow. The diseases they produce often respond to treatment with antibiotics.

Viruses are organisms requiring living cells in which to reproduce and are intimately dependent on the body they infect. Viruses produce diseases that generally do not respond to antibiotics. However, antiviral drugs are sometimes effective.

Toxins are poisonous substances typically found in, and extracted from, living plants, animals, or microorganisms; some toxins, however, can be produced or altered by chemical means. Select toxins can be treated with specific antitoxins and selected drugs.

Most biological agents are difficult to grow and maintain. Many break down quickly when exposed to sunlight and other environmental factors, while others, such as anthrax spores, are very long-lived. They can be dispersed by spraying them in the air, by infecting animals that carry the disease to humans, or through food and water contamination, as follows:

(1) Aerosols — Biological agents are dispersed into the air, forming a fine mist that can drift for miles. Inhaling the agent can cause disease in people or animals.
(2) Animals — Some diseases are spread by insects and animals such as fleas, mice, flies, and mosquitoes. Deliberately spreading diseases through livestock is also referred to as agroterrorism.
(3) Food and water contamination — Some pathogenic organisms and toxins can persist in food and water supplies. Cooking food and boiling water will kill most microbes and deactivate most toxins.
(4) Person-to-person — Person-to-person spread of infectious agents is also possible. Humans have been the source of infection for smallpox, plague, and the Lassa viruses.

B.7.3 What to Do to Prepare for a Chemical or Biological Attack. A disaster supply kit should be assembled to include the following:

(1) Battery-powered commercial radio with extra batteries.
(2) Nonperishable food and drinking water.
(3) Roll of duct tape and scissors.
(4) Plastic for doors, windows, and vents for the room in which you will take shelter — this should be an internal room where air that can contain hazardous chemical or biological agents can be blocked out. To save critical time during an emergency, sheeting should be premeasured and cut for each opening.
(5) First aid kit.
(6) Sanitation supplies, including soap, water, and bleach.

B.7.4 What to Do During a Chemical or Biological Attack. The following safeguards should be observed:

(1) Listen to the radio for instructions from authorities, such as whether to remain inside or to evacuate.
(2) If you are instructed to remain in your home, the building where you are, or other shelter during a chemical or biological attack, do the following:
    (a) Turn off all ventilation, including furnaces, air conditioners, vents, and fans.
    (b) Seek shelter in an internal room, preferably one without windows.
    (c) Seal the room with duct tape and plastic sheeting. Ten square feet of floor space per person will provide sufficient air to prevent carbon dioxide buildup for up to 5 hours.
(3) Remain in protected areas where toxic vapors are reduced or eliminated; be sure to have a battery-operated radio at hand.
(4) If you are caught in an unprotected area, do the following:
    (a) Attempt to get upwind of the contaminated area.
    (b) Attempt to find shelter as quickly as possible.
    (c) Listen to your radio for official instructions.

B.7.5 What to Do After a Chemical Attack. Immediate symptoms of exposure to chemical agents can include blurred vision, eye irritation, difficulty breathing, and nausea. A person affected by a chemical or biological agent requires immediate attention by professional medical personnel. If medical help is not immediately available, decontaminate yourself and assist in decontaminating others. Decontamination is needed within minutes of exposure to minimize health consequences. (However, you should not leave the safety of a shelter to go outdoors to help others until authorities announce it is safe to do so.) The following steps should be taken:

(1) Use extreme caution when helping others who have been exposed to chemical agents.
(2) Remove all clothing and other items in contact with the body. Contaminated clothing normally removed over the head should be cut off to avoid contact with the eyes, nose, and mouth. Put the clothing into a plastic bag if possible. Decontaminate hands using soap and water. Remove eyeglasses or contact lenses. Put glasses in a pan of household bleach to decontaminate.
(3) Remove all items in contact with the body.
(4) Flush eyes with lots of water.
(5) Gently wash face and hair with soap and water; then thoroughly rinse with water.
(6) Decontaminate other body areas likely to have been contaminated. Blot (do not swab or scrape) with a cloth soaked in soapy water and rinse with clear water.

(7) Change into uncontaminated clothes. Clothing stored in drawers or closets is likely to be uncontaminated.
(8) If possible, proceed to a medical facility for screening.

B.7.6 What to Do After a Biological Attack. In many biological attacks, people will not know they have been exposed to an agent. In such situations, the first evidence of an attack can be when you notice symptoms of the disease caused by exposure to an agent — seek immediate medical attention for treatment.

In some situations, like the anthrax letters sent in 2001, people can be alerted to a potential exposure. Pay close attention to all official warnings and instructions on how to proceed. The delivery of medical services for a biological event might be handled differently to respond to increased demand. Again, it will be important to pay attention to official instructions via radio, television, and emergency alert systems.

If your skin or clothing comes in contact with a visible, potentially infectious substance, remove and bag the clothes and personal items and wash yourself with warm soapy water immediately. Put on clean clothes and seek medical assistance.

For more information, visit the web site for the Centers for Disease Control and Prevention, *www.bt.cdc.gov*.

B.8 Nuclear and Radiological Attack. Nuclear explosions can cause deadly effects — blinding light, intense heat (thermal radiation), initial nuclear radiation, blast, fires started by the heat pulse, and secondary fires caused by the destruction. They also produce radioactive particles, called *fallout*, that can be carried by wind for hundreds of miles.

Terrorist use of a radiological dispersion device (RDD) — often called a "dirty nuke" or "dirty bomb" — is considered far more likely than use of a nuclear device. These radiological weapons are a combination of conventional explosives and radioactive material designed to scatter dangerous and sublethal amounts of radioactive material over a general area. Such radiological weapons appeal to terrorists because they require very little technical knowledge to build and deploy compared to that for a nuclear device. Also, these radioactive materials are used widely in medicine, agriculture, industry, and research and thus are much more readily available and easy to obtain than weapons-grade uranium or plutonium.

Terrorist use of a nuclear device would probably be limited to a single smaller "suitcase" weapon. The strength of such a weapon would be in the range of the bombs used during World War II. The nature of the effects would be the same as a weapon delivered by an intercontinental missile, but the area and severity of the effects would be significantly more limited.

There is no way of knowing how much warning time there would be before an attack by a terrorist using a nuclear or radiological weapon. A surprise attack remains a possibility.

The danger of a massive strategic nuclear attack on the United States involving many weapons receded with the end of the Cold War. However, some terrorists have been supported by nations that have nuclear weapons programs.

If there were threat of an attack from a hostile nation, people living near potential targets could be advised to evacuate, or they could decide on their own to evacuate to an area not considered a likely target. Protection from radioactive fallout would require taking shelter in an underground area or in the middle of a large building.

In general, potential targets include the following:

(1) Strategic missile sites and military bases
(2) Centers of government, such as Washington, D.C., and state capitals
(3) Important transportation and communication centers
(4) Manufacturing, industrial, technology, and financial centers
(5) Petroleum refineries, electrical power plants, and chemical plants
(6) Major ports and airfields

Taking shelter during a nuclear attack is absolutely necessary. There are two kinds of shelters — blast and fallout. Blast shelters offer some protection against blast pressure, initial radiation, heat, and fire, but even a blast shelter could not withstand a direct hit from a nuclear detonation. Fallout shelters do not need to be specially constructed for that purpose. They can be any protected space, provided that the walls and roof are thick and dense enough to absorb the radiation given off by fallout particles. The three protective factors of a fallout shelter are as follows:

(1) *Shielding*. The more heavy, dense materials — thick walls, concrete, bricks, books, and earth — between you and the fallout particles, the better.
(2) *Distance*. The more distance between you and the fallout particles, the better. An underground area, such as a home or office building basement, offers more protection than the first floor of a building. A floor near the middle of a high-rise can be better, depending on what is nearby at that level on which significant fallout particles would collect. Flat roofs collect fallout particles so the top floor is not a good choice, nor is a floor adjacent to a neighboring flat roof.
(3) *Time*. Fallout radiation loses its intensity fairly rapidly. In time, you will be able to leave the fallout shelter. Radioactive fallout poses the greatest threat to people during the first 2 weeks, by the end of which time it will have declined to about 1 percent of its initial radiation level.

It is important to remember that any protection, however temporary, is better than none at all, and the more shielding, distance, and time that can be taken advantage of, the better.

B.8.1 Electromagnetic Pulse. In addition to other effects, a nuclear weapon detonated in or above the earth's atmosphere can create an electromagnetic pulse (EMP), which is a high-density electrical field. An EMP acts like a bolt of lightning but is stronger, faster, and briefer. An EMP can seriously damage electronic devices connected to power sources or antennas, such as communications systems, computers, electrical appliances, and automobile or aircraft ignition systems. The damage could range from a minor interruption to actual burnout of components. Most electronic equipment within 1000 miles (1609 km) of a high-altitude nuclear detonation could be affected. Battery-powered radios with short antennas generally would not be affected.

Although an EMP is unlikely to harm most people, it could harm those with pacemakers or other implanted electronic devices.

B.8.2 What to Do Before a Nuclear or Radiological Attack. The following preparations should be made:

(1) Learn the warning signals and all sources of warning used in your community. Make sure you know what the signals are, what they mean, how they will be used, and what you should do if you hear them.
(2) Assemble and maintain a disaster supply kit with food, water, medications, fuel, and personal items adequate for up to 2 weeks — the more the better.
(3) Find out what public buildings in your community have been designated as fallout shelters. They might have been designated years ago, but start there and learn which buildings are still in use and could be designated as shelters again.
(4) Look for yellow and black fallout shelter signs on public buildings. Note: With the end of the Cold War, many of the signs have been removed from the buildings previously designated as fallout shelters.
(5) If there are no noticeable or official designations, make a list of potential shelters near your home, workplace, and school — such as basements, windowless center areas of middle floors in high-rise buildings, subways, and tunnels.
(6) Give your household clear instructions about where fallout shelters are located and what actions to take in case of attack.
(7) If you live in an apartment building or high-rise, talk to the manager about the safest place in the building for sheltering and about providing for building occupants until it is safe to go out.
(8) There are few public shelters in many suburban and rural areas. If you are considering building a fallout shelter at home, keep the following in mind:
    (a) A basement or any other underground area is the best place to shelter from fallout. Often, few major changes are needed, especially if the structure has two or more stories and its basement — or one corner of it — is below ground.
    (b) Fallout shelters can be used for storage during nonemergency periods, but only store things there that can be very quickly removed. (Dense, heavy items, however, can be used to add to the shielding.)
    (c) Shelters designated for tornadoes or other severe weather conditions could be used as shelter in the event of a nuclear detonation or for fallout protection. These shelters are especially valuable for people with homes that have no basement.
    (d) All the items necessary for your stay need not be stocked inside the shelter itself but can be stored elsewhere, as long as you can move them quickly to the shelter.
    (e) Learn about your community's evacuation plans. Such plans can include evacuation routes, relocation sites, how the public will be notified, and transportation options for people who do not own cars and those who have special needs.
(9) Call your local emergency management office for more information.

B.8.3 What to Do During a Nuclear or Radiological Attack. The following safeguards should be observed:

(1) Do not look at the flash or fireball — it can blind you.
(2) If you hear an attack warning:
    (a) Take cover as quickly as you can, BELOW GROUND IF POSSIBLE, and stay there unless instructed to do otherwise.
    (b) If you are caught outside, unable to get inside immediately, take cover behind anything that might offer protection. Lie flat on the ground and cover your head.
    (c) If the explosion is some distance away, it could take 30 seconds or more for the blast wave to hit.
    (d) Protect yourself from radioactive fallout. If you are close enough to see the brilliant flash of a nuclear explosion, the fallout will arrive in about 20 minutes. Take shelter, even if you are many miles from ground zero — radioactive fallout can be carried by the winds for hundreds of miles. Remember the three protective factors: shielding, distance, and time.
    (e) Keep a battery-powered radio with you and listen for official information. Follow the instructions given. Local instructions should always take precedence: officials on the ground know the local situation best.

B.8.4 What to Do After a Nuclear or Radiological Attack. In a public or home shelter, the following should be done:

(1) Although it can be difficult, make every effort to maintain sanitary conditions in the shelter space.
(2) Water and food can be scarce. Use them prudently but do not impose severe rationing, especially for children, the ill, or the elderly.
(3) Cooperate with shelter managers. Living with many people in confined space can be difficult and unpleasant.
(4) Do not leave the shelter until officials say it is safe. The length of your stay can range from a day to 2 to 4 weeks. Follow their instructions when leaving.

You can expect the following conditions:

(1) Contamination from a radiological dispersion device could affect a wide area, depending on the amount of conventional explosives used, the quantity of radioactive material, and atmospheric conditions.
(2) A "suitcase" terrorist nuclear device detonated at or near ground level would produce heavy fallout from the dirt and debris sucked up into the mushroom cloud.
(3) A missile-delivered nuclear weapon from a hostile nation would probably cause an explosion many times more powerful than a suitcase bomb and provide a greater cloud of radioactive fallout.
(4) The decay rate of the radioactive fallout would be uniform, making it necessary for those in the areas with highest radiation levels to remain in shelters for up to a month.
(5) The heaviest fallout would be limited to the area at or downwind from the explosion, and 80 percent of the fallout would occur during the first 24 hours.
(6) Because of these facts and the very limited number of weapons terrorists could detonate, most of the country would not be affected by fallout.
(7) People in most of the areas that would be affected could be allowed to come out of shelter and, if necessary, evacuate to unaffected areas within a few days.

B.9 Returning to Normal. After an attack, you should do the following:

(1) Keep listening to the radio for news about what to do, where to go, and places to avoid.
(2) If you were within the range of a bomb's shock wave, or you are in a high-rise building that experienced a nonnuclear explosion, check first for any sign of collapse or damage, such as the following:
    (a) Toppling chimneys, falling bricks, collapsing walls, plaster falling from ceilings
    (b) Fallen light fixtures, pictures, and mirrors
    (c) Broken glass from windows
    (d) Overturned bookcases, wall units, or other fixtures
    (e) Fires from broken chimneys
    (f) Ruptured gas and electric lines
(3) Immediately clean up spilled medicines, drugs, flammable liquids, and other potentially hazardous materials.
(4) Listen to a battery-powered radio for instructions and information about community services.
(5) Monitor the radio and television for information on assistance that can be provided. Local, state, and federal governments and other organizations will help meet emergency needs and aid in the recovery from damage and losses.

The danger can be aggravated by broken water mains and fallen power lines. If gas, water, and electricity were turned off at the main valves/switch before you went to shelter, observe the following precautions:

(1) Do not turn the gas back on. The gas company will turn it back on, or you will receive other instructions.
(2) Turn the water back on at the main valve only after you know the water system is working and water is not contaminated.
(3) Turn electricity back on at the main switch only after you know the wiring is undamaged and the community electrical system is functioning.
(4) Check to see that sewage lines are intact before using sanitary facilities.
(5) Stay away from damaged areas.
(6) Stay away from areas marked “Radiation Hazard” or “HAZMAT.”

Private sector facilities should be alert, not alarmed. Have a written vulnerability assessment plan and implement it at times of terrorist threat. Such a plan should require the following:

(1) Lock down “back-of-the-house,” nonpublic areas to essential personnel only. These areas can include kitchens where food handling and storage could be compromised, mechanical spaces where HVAC equipment and water supply sources are located, and electrical distribution rooms.
(2) Increase the presence of security officers in public spaces to observe off-normal activity, unattended articles, suspicious parcels and letters, and individuals who act strangely or just do not seem to belong.
(3) Provide a prepared on-site area of refuge for visitors and employees should an off-site consequence prevent travel from the facility. Nonperishable food, drinking water, battery-powered commercial radio, first aid supplies, sanitation supplies, flashlights, and so forth, should be stored in the area.
(4) Insist on government-issued photo IDs for facility entry.

Car parks might restrict public parking, limiting access to automobiles of known visitors and employees only. Additionally, access of vans or trucks might be prohibited. Vehicles of any kind can be restricted from parking in the immediate proximity of the facility perimeter.

Some protection features are better nondisclosed, so as not to compromise security. Follow the need-to-know doctrine. Be careful not to compromise security by disclosure of covert or highly sensitive security measures to other than internal security, law enforcement, and other essential personnel.

Publish and distribute specialized instructions to visitors and employees relating to the current security level. Inform them of the fact that the facility has taken active security measures and that many will not be evident to them. Tell them that they can experience some visible security measures such as the following:

(1) Increased presence of security officers
(2) Closer scrutiny of carried items like large purses, briefcases, and backpacks
(3) Requests for proof of identity, usually a government-issued photo ID
(4) More stringent rules regarding bags and parcels
(5) Limitation on parking in the immediate proximity of the facility perimeter, access to car parks to known visitors and employees only, and no vans, trucks, or other large vehicles in car parks.

Annex C Critical Infrastructure Protection

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

C.1 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.

C.2 Chemical Facilities.

C.2.1 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.

C.2.2 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.

C.2.3 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.

C.2.4 Some chemicals can be particularly attractive targets because of the potential for greater consequences.

C.2.5 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.

C.2.6 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.

C.2.6.1 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.

C.2.6.2 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.

C.2.6.3 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

C.2.6.4 Consideration should be given to protecting equipment containing hazardous chemicals against sabotage and accidents.

C.2.6.5 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.

C.2.6.6 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.

C.2.6.7 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.

C.2.6.8 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.

C.2.7 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.

C.3 Water Treatment Facilities.

C.3.1 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.

C.3.1.1 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.

C.3.1.2 Supply interruptions can also occur as an indirect result of contamination.

C.3.2 Water treatment facilities should comply with the procedures in C.3.2.1 through C.3.2.3.

C.3.2.1 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.

C.3.2.2 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.

C.3.2.3 Water authorities should reasonably ensure that fire hydrants and other entry points to the distribution system are tamper resistant.

C.4 Power Distribution Facilities. See *NFPA 70*.

Annex D Special Events

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

D.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.

D.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.

D.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.

D.3.1 Security Committee.

D.3.1.1 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 person.

D.3.1.2 The committee meets 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.

D.3.1.3 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.

D.3.2 Statement of Purpose. The committee develops 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."

D.3.3 Event Planning Measures.

D.3.3.1 Personnel.

D.3.3.1.1 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 6 for guidance on security personnel).

D.3.3.1.2 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.

D.3.3.1.3 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.3.3.1.4 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.

D.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.

D.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.

D.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.

D.3.3.5 Parking and Traffic Control.

D.3.3.5.1 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.

D.3.3.5.2 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 transportation to and from the satellite parking, as well as safety, security, and traffic control at the satellite parking, also should be addressed.

D.3.3.5.3 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.

D.3.4 Ingress and Egress.

D.3.4.1 General.

D.3.4.1.1 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.

D.3.4.1.2 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.

D.3.4.1.3 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.

D.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.

D.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 check in on a regular basis to the communications center.

D.3.6 Other Considerations.

D.3.6.1 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, and procedures should be in place for evacuating a facility and conducting bomb searches.

D.3.6.2 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.

D.4 Handling Disturbances, Ejections, and Arrests. Event planners develop policies and procedures as a means of providing staff with guidelines on how to handle disturbances. Staff also should 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 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 members should stay calm and speak clearly when dealing with those involved in the disturbance. They also should 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 waits until help arrives before attempting to quell the disturbance. If possible, staff remains in contact with the control center throughout the disturbance.
(5) One action staff can take in handling any disturbance is to ask the people 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 handles all ejections and arrests, since they are usually more experienced in the proper procedures to follow.

D.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 people with access to critical assets.
(2) When outside services (contractors, vendors, or other personnel) are used, management asks the vendors'/contractors' management about their pre-employment screening and drug testing practices.
(3) A drug testing program should be established.

The increase in the number of lawsuits based on the tort of negligent hiring has resulted in employers being under a greater responsibility to use due care in selecting employees. At the same time, federal and state laws impose restrictions on employers that are intended to protect the privacy of applicants. Since many employees have access to critical assets (people, property, and information), the need for preemployment screening cannot be overemphasized.

Annex E Special Topics

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

E.1 General. Annex E is a collection of information that appeared in the first edition of NFPA 730 and is provided here for informational purposes only.

E.2 Exterior.

E.2.1 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.

E.2.1.1 Concrete Planters. Concrete planters and bollards (discussed in E.2.1.2) are being used to protect the White House and other federal government buildings in Washington, D.C.

E.2.1.1.1 In testing performed by the U.S. Army Corps of Engineers, a concrete planter, designed as shown in Figure E.2.1.1.1, was capable of stopping a 15,000 lb (6804 kg) vehicle traveling at 50 mph (22.4 m/sec). This planter should also stop a 4500 lb (2041.2 kg) vehicle traveling at 30 mph (13.4 m/sec), 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).

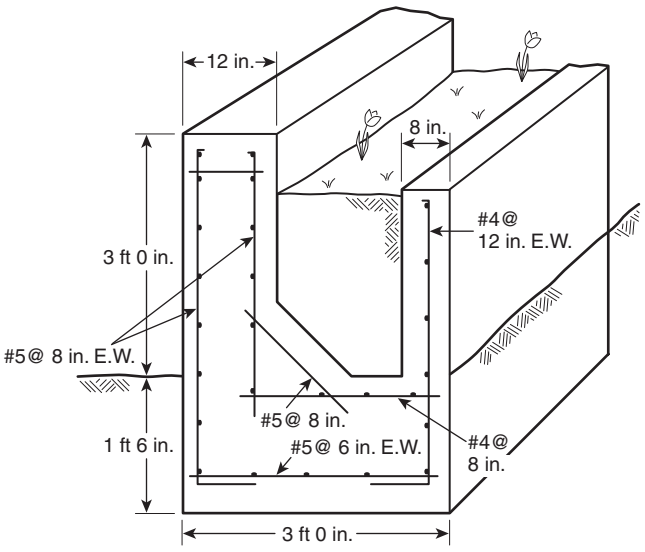


FIGURE E.2.1.1.1 Concrete Planter. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)***

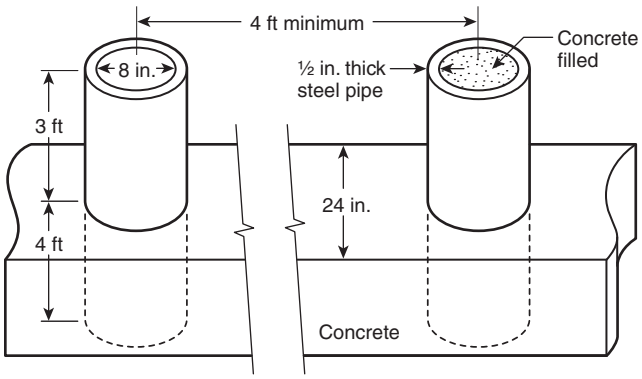
E.2.1.1.2 If local building or street codes permit their use, and the sidewalk in front of the store is wide enough, a decorative concrete planter placed between the pedestrian walkway and the curb can be used. If more than one planter is required to provide coverage for the front of the store, they should be spaced a maximum of 4 ft (1.22 m) apart.

E.2.1.2 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.

E.2.1.2.1 In testing performed by the U.S. Army Corps of Engineers, concrete-filled steel bollards *(see Figure E.2.1.2.1)* 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 (2041 kg) vehicle traveling at 30 mph (13.4 m/sec). The concrete portion of the bollard had a diameter of 8 in. (200 mm), and the steel pipe was ½ in. (13 mm) thick.

E.2.1.2.2 When the bollards were reinforced with a 12 in. (0.31 m) "C" channel *(see Figure E.2.1.2.2)*, the design was capable of stopping a 15,000 lb (6804 kg) vehicle traveling at 50 mph (22.4 m/sec).

E.2.1.3 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 E.2.1.3)*, was capable of stopping a 4000 lb (1814 kg) vehicle traveling at 50 mph (22.4 m/sec). Jersey barriers can be used in place of planters and bollards where aesthetics are not of concern.



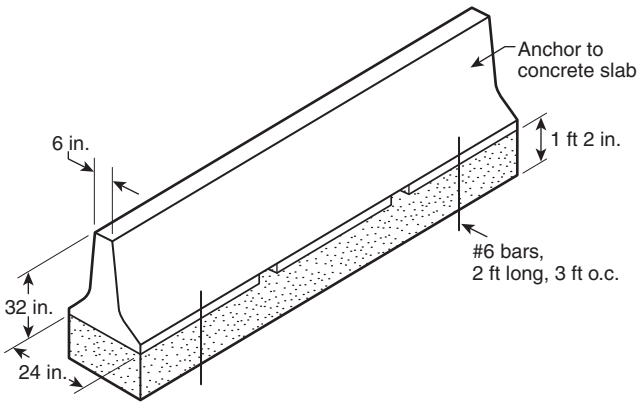
For SI units, 1 in. = 2.54 cm.

FIGURE E.2.1.2.1 Concrete-Filled Bollard. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)***

E.2.2 Fencing. Fences are a 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.

E.2.2.1 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 can be 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 F567, *Standard Practice for the Installation of Chain-Link Fence*, provides materials specifications, design requirements, and installation procedures for chain-link fencing.

E.2.2.2 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 F567, *Standard Practice for the Installation of Chain-Link Fence*, requirements.

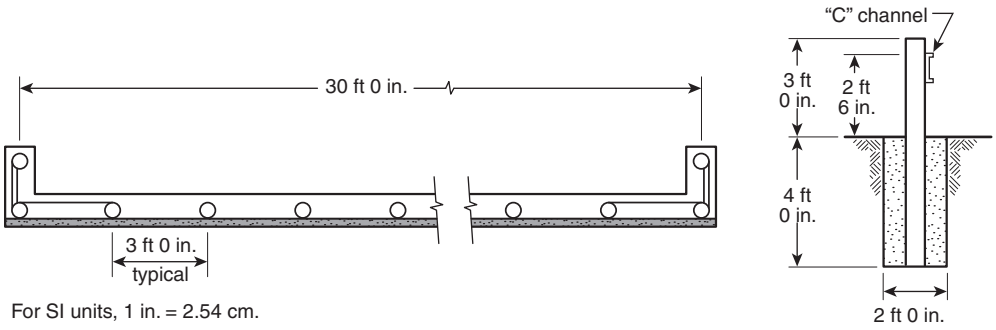


For SI units, 1 in. = 2.54 cm.

FIGURE E.2.1.3 Jersey Barrier. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)***

E.2.2.2.1 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.

E.2.2.2.2 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. (305 mm) and 9 in. (229 mm) 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. (51 mm) of building walls.



For SI units, 1 in. = 2.54 cm.

FIGURE E.2.1.2.2 Concrete-Filled Steel Bollard with 12 in. "C" Channel. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)***

E.2.2.2.3 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 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.

E.2.2.3 Rails and Tension Wires.

E.2.2.3.1 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.

E.2.2.3.2 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. (152 mm) of the fabric should also be provided. Some fences have a bottom rail in place of the bottom tension wire.

E.2.2.4 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. (51 mm) per side.

E.2.2.4.1 "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.

E.2.2.4.2 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.

E.2.2.4.3 The fabric should be stretched taut and securely fastened to the posts at 15 in. (381 mm) 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).

E.2.2.4.4 The bottom of the fabric should extend to within 2 in. (51 mm) 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.

E.2.2.5 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. (457 mm) in length, attached to the fence posts either vertically or at an angle of approximately 45 degrees.

E.2.2.5.1 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.

E.2.2.5.2 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.

E.2.2.5.3 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.

E.2.2.5.4 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. (25.4 mm) or 1¼ in. (32 mm) wide, with needle-sharp barbs that are spaced on 4 in. (102 mm) 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).

E.2.2.6 Gates.

E.2.2.6.1 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.

E.2.2.6.2 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. (381 mm) 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. (51 mm) of the ground.

E.2.2.6.3 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 people 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.

E.2.2.6.4 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.

E.2.2.7 Locks.

E.2.2.7.1 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.

E.2.2.7.2 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.

E.2.3 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*.

E.2.3.1 General.

E.2.3.1.1 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.

E.2.3.1.2 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.

E.2.3.2 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 F567. 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.

E.2.3.2.1 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).

E.2.3.2.2 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.

E.2.3.3 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.

E.2.3.3.1 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.

E.2.3.3.2 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.

E.2.3.3.3 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.

E.2.3.4 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.

E.2.3.4.1 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.

E.2.3.4.1.1 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).

E.2.3.4.1.2 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.

E.2.3.4.2 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 the 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.

E.2.4 Lighting.

E.2.4.1 Lighting Terms.

E.2.4.1.1 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).

E.2.4.1.2 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.

E.2.4.1.3 Illuminance is the intensity of incident luminous flux on a surface. Illuminance is the measure for lighting levels and is measured in footcandles (fc) (1 lm/ft^2) or lux (lx) (1 lm/m^2).

E.2.4.1.4 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 foot (cd/ft^2) [candela per square meter (cd/m^2)].

E.2.4.2 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.

E.2.4.2.1 Incandescent Lamps.

E.2.4.2.1.1 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.

E.2.4.2.1.2 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 an 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, which is common with incandescent lamps and which causes blackening of the bulb. The design helps these particles redeposit on the filament, increasing lamp life. Efficiency and color rendition of tungsten halogen and incandescent lamps are approximately the same.

E.2.4.2.2 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.

E.2.4.2.3 High-Intensity Discharge (HID) Lamps. HID lamps include mercury vapor, metal halide, and high-pressure sodium.

E.2.4.2.3.1 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.

E.2.4.2.3.2 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.

E.2.4.2.3.3 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.

E.2.4.2.3.4 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.

Δ **E.2.4.3 Warm-Up and Restrike Times.** Table E.2.4.3 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.

E.2.4.4 Floodlight Luminaires.

E.2.4.4.1 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.

E.2.4.4.2 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.

Δ **Table E.2.4.3 Time Required for Various Lighting Sources to Reach Full Illumination**

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

E.2.4.4.3 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.

E.2.4.4.4 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.

E.2.4.4.5 Street Light Luminaires.

E.2.4.4.5.1 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 through V. The distribution of the light can be symmetrical or asymmetrical.

E.2.4.4.5.2 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.

E.2.4.4.5.3 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.

E.2.4.4.6 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.

E.2.4.4.7 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. (305 mm) to 24 in. (610 mm), and the wattage of the lamp, which can range from 250 watts to 3000 watts.

E.3 Portals.

E.3.1 Doors.

E.3.1.1 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, *Recommended Specifications for Standard Steel Door Frames*, and tested to ANSI/SDI A250.4, *Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors and Hardware Reinforcing*, and wood doors are tested for security. Door strength and reinforcement should be compatible with the locks used.

E.3.1.2 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.

E.3.1.3 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 grilles.

E.3.1.4 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.

E.3.1.5 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.

E.3.1.6 Other security measures that should be considered for doors are described in E.3.1.6.1 through E.3.1.6.9.

E.3.1.6.1 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.

E.3.1.6.2 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.

E.3.1.6.3 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.

E.3.1.6.4 If an exterior door has a glass panel within 40 in. (1016 mm) 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.

E.3.1.6.5 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 grille.

E.3.1.6.6 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.

E.3.1.6.7 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.

E.3.1.6.8 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.

E.3.1.6.9 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/BHMA A156.16, *Auxiliary Hardware*, are available in three viewing angles to suit the application: Grade 1, 185 degrees; Grade 2, 145 degrees; and Grade 3, 115 degrees.

E.3.1.7 Specialty doors include those described in E.3.1.7.1 through E.3.1.7.4.

E.3.1.7.1 Coiling doors should be protected with slide bolts on the bottom bar unless they are controlled or locked by electric power.

E.3.1.7.2 An iron keeper for securing the hand chain or an iron pin for the shaft on the crank should be provided.

E.3.1.7.3 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.

E.3.1.7.4 Metal accordion grate or grille-type doors should have a secured metal guide track at the top and bottom and be secured with a cylinder lock or padlock.

E.3.2 Windows.

E.3.2.1 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.

E.3.2.2 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.

E.3.2.3 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 grilles must be securely fastened to the window frame so they cannot be pried loose.

E.3.2.4 Outside hinges on windows should have nonremovable pins. The hinge pins should be welded, flanged, or otherwise secured so they cannot be removed.

E.3.3 Ironwork. Ironwork, such as crossbars, gates, and screens, are used on doors and windows to protect against unauthorized intrusion.

E.3.3.1 Crossbars.

E.3.3.1.1 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.

E.3.3.1.2 A steel crossbar should have cross-sectional dimensions of at least 1¾ in. × ½ in. (44 mm × 13 mm). 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.

E.3.3.2 Flat or Round Iron Bars.

E.3.3.2.1 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. (19 mm) diameter, while flat bars are usually 1½ in. × ⅜ in. (38 mm × 10 mm). 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. (127 mm) apart and horizontal bars 24 in. (610 mm) or less.

E.3.3.2.2 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.

E.3.3.2.3 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.

E.3.3.2.4 Iron gates are used as security devices on entrances to stores and mercantile occupancies. Round bars should be at least 1½ in. (38 mm) diameter, while flat bars should be at least 1½ in. × ⅜ in. (38 mm × 10 mm); vertical bars should be spaced not more than 5 in. (127 mm) apart. The lock used to secure the gate should be of the deadbolt type, with a minimum bolt throw of 1 in. (25 mm) 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 the frame. If the hinge pin is removable, then provision should be made to secure it.

E.3.3.3 No. 18 Gauge Sheet Steel Panel.

E.3.3.3.1 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.

E.3.3.3.2 The panel should be attached to the inside surface of the door, covering its length and width, with screws on maximum 6 in. (152 mm) 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.

E.3.3.4 No. 8 Gauge Wire Mesh Screening.

E.3.3.4.1 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.

E.3.3.4.2 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.

E.3.3.5 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.

E.3.4 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.

E.3.4.1 Burglary-Resistant Glazing Materials. ANSI/UL 972, *Standard for Burglary Resisting Glazing Material*, 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.

E.3.4.1.1 UL-Listed Burglary-Resisting Glazing Materials. The three types of materials currently 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.

E.3.4.1.1.1 Laminated Glass. This material consists of two sections of $\frac{1}{8}$ 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 $\frac{9}{32}$ in. (7.1 mm) and is designed to fit the nominal $\frac{1}{4}$ in. (6.4 mm) frame of a show window.

E.3.4.1.1.2 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 $\frac{7}{8}$ in. (22.2 mm) thickness.

E.3.4.1.1.3 Polycarbonate. This material is also a plastic sheet of monolithic construction made by the extrusion or injection molding of polycarbonate resin. It is $\frac{1}{8}$ in. (3.2 mm) thick, making it suitable for use in window frames. Polycarbonate has 300 times the impact resistance of plate glass and 20 to 30 times the impact strength of acrylic.

E.3.4.1.2 Application of UL-Listed Burglary-Resisting Glazing Materials.

E.3.4.1.2.1 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.

E.3.4.1.2.2 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.

E.3.4.1.2.3 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.

E.3.4.1.2.4 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.

E.3.4.1.2.5 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.

E.3.4.1.2.6 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 (i.e., 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.

E.3.4.1.2.7 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.

E.3.4.1.2.8 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 rabbeted dimensions is preferred.

E.3.4.1.2.9 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.

E.3.4.1.2.10 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 $\frac{3}{8}$ in. (10 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.

E.3.4.2 Bullet-Resisting Glazing Materials. ANSI/UL 752, *Standard for Bullet-ResistingEquipment*, 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 F1233, *Standard Test Method for Security Glazing Materials and Systems*, provides test criteria to evaluate the level of resistance of security glazing materials and systems to forced entry due to ballistic impact.

E.3.4.2.1 UL-Listed Bullet-Resisting Glazing Materials.

E.3.4.2.1.1 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.

(A) 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 $1\frac{3}{16}$ in. (30.2 mm) upward to provide protection at all ballistic levels.

(B) Acrylics. These materials are usually monolithic in structure and available in thicknesses ranging from $1\frac{1}{4}$ in. to $1\frac{3}{4}$ in. (31.8 mm to 44.5 mm). They provide protection only at the handgun levels and not in the high-power rifle category.

(C) Polycarbonates. Usually of laminated construction, polycarbonates consist of multiple polycarbonate sheets bonded to an interlayer of PVB. They are available in thicknesses ranging from $\frac{3}{4}$ in. to $1\frac{3}{4}$ in. (19.1 mm to 44.5 mm). They provide protection only at the handgun levels.

(D) Composites. These materials 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.

E.3.4.2.1.2 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.

E.3.4.2.2 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.

E.3.4.2.2.1 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.

E.3.4.2.2.2 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.

E.3.4.2.2.3 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.

E.3.4.2.3 ASTM Testing. ASTM F1233, *Standard Test Method for Security Glazing Materials and Systems*, 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.

E.3.4.2.3.1 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.

E.3.4.2.3.2 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 F1233, *Standard Test Method for Security Glazing Materials and Systems*. Three rounds are fired at the specimen at 120 degree intervals around an 8 in. (203 mm) diameter circle and at 0 degree angle of obliquity.

E.3.4.2.3.3 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.

E.3.4.2.3.4 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.

E.3.4.2.4 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.

E.3.4.2.4.1 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.

E.3.4.2.4.2 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.

(A) 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 a person 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.

(B) 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.

(C) 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.

(D) 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 $\frac{5}{8}$ 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.

(E) 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.

(F) 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.

(G) 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.

E.3.5 Locking Hardware.

E.3.5.1 Locks are commonly employed security devices. They are found on anything to which access must be controlled, such as vehicles, storage containers, doors, gates, and windows. The security of any property or facility relies heavily on locking devices. An assessment of all hardware, including door frames and jambs, should be included in any physical security survey. Locking devices vary greatly in appearance as well as function and application.

E.3.5.2 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 limits both key duplication and distribution. Refer to ANSI/BHMA A156.28, *Recommended Practice for Keying Systems*. Keys should comply with ANSI/BHMA A156.5, *Auxiliary Locks and*

Associated Products (section on cylinders), and ANSI/BHMA A156.30, *High Security Cylinders*, in the appropriate grade for the application.

E.3.5.3 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, 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.

E.3.5.4 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, *High Security Cylinders*, in the appropriate grade for the application. Electronic cylinders for burglary resistance should be listed to ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

E.3.5.5 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.

E.3.5.6 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.

E.3.5.7 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.

E.3.5.8 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.

E.3.5.9 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 should also be followed for combination padlocks.

E.3.5.10 Exit Devices.

E.3.5.10.1 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.

E.3.5.10.2 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.

E.3.5.10.3 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 a vertical-by-vertical or a 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.

E.3.5.10.4 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.

E.3.5.11 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. Bored/cylindrical locks should meet ANSI/BHMA A156.2, *Bored and Preassembled Locks and Latches*, and ANSI/UL 437, *Standard for Key Locks*, in the appropriate grade for the application.

E.3.5.12 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. Interconnected locks combine the security and safety of a latching device with the security of a deadbolt. These locks should meet ANSI/BHMA A156.12, *Interconnected Locks and Latches*, and ANSI/UL 437, *Standard for Key Locks*, in the appropriate grade for the application.

E.3.5.13 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 the 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, *Mortise Locks and Latches Series 1000*, and ANSI/UL 437, *Standard for Key Locks*, in the appropriate grade for the application.

E.3.5.14 Electromechanical Locks. Electromechanical door locks are used primarily 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 comply with ANSI/BHMA A156.25, *Electrified Locking Devices*, 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 ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

E.3.5.15 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 comply with ANSI/BHMA A156.23, *Electromagnetic Locks*, in the appropriate grade for the application and be listed to ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*, for burglary-resistant electric locks.

Δ **E.3.5.16 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 comply with ANSI/BHMA A156.24, *Delayed Egress Locking Systems*, in the appropriate grade for the application and be listed as "Special Locking Arrangements" per ANSI/UL 294, *Standard for Access Control System Units*, and NFPA *101*.

E.3.5.17 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 comply with ANSI/BHMA A156.31, *Electric Strikes and Frame Mounted Actuators*, in the appropriate grade for the application and should be listed to ANSI/UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*, for burglary-resistant electric door strikes.

E.3.5.18 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.

E.3.5.19 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 where 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 comply with the deadbolt section of ANSI/BHMA A156.5, *Auxiliary Locks and Associated Products*, and the door

locks section of ANSI/UL 437, *Standard for Key Locks*, in the appropriate grade for the application.

E.3.5.20 Hinges. Hinges or pivots are required for all swinging doors. Hinges other than continuous hinges should be installed at intervals of 30 in. (762 mm). Nonremovable pins (NRPs) should be used on hinges accessible from the outside (out-swinging doors). Various types of security studs are available to prevent attack. They should meet the requirements of ANSI/BHMA A156.1, *Butts and Hinges*, or ANSI/BHMA A156.26, *Continuous Hinges*, in the appropriate grade for the application. Hinges for use in burglar alarm systems should be listed to ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*.

E.3.5.21 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 the requirements of ANSI/BHMA A156.4, *Door Controls — Closers*, or ANSI/BHMA A156.17, *Self-Closing Hinges and Pivots*, in the appropriate grade for the application.

E.4 Electronic Premises Security Systems.

E.4.1 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 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.

E.4.1.1 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

E.4.1.2 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.

E.4.1.2.1 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.

E.4.1.2.2 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.

E.4.1.2.3 The installation of intrusion detection system components is very important, and attention should be given to NFPA 731 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.

E.4.1.2.4 Sensors. The three basic types of sensors are perimeter, volumetric, and proximity.

E.4.1.2.4.1 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. Perimeter sensors should be listed to ANSI/UL 639, *Standard for Intrusion-Detection Units*.

(A) 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. Connectors and switches used in burglar alarm systems should be listed to ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*.

(B) 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.

(C) Screens. 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. Linings and screens for use with burglar alarm systems should be listed to ANSI/UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems*.

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

(E) 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 that specific frequencies be 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. Glass