NFPA®

731

Standard for the Installation of Premises Security Systems

2020

NFPA®

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING 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 these documents may be superseded at any time by the issuance of a new edition, may be amended with the issuance of Tentative Interim Amendments (TIAs), or be corrected by Errata. It is intended that through regular revisions and amendments, participants in the NFPA standards development process consider the then-current and available information on incidents, materials, technologies, innovations, and methods as these develop over time and that NFPA Standards reflect this consideration. Therefore, any previous edition of this document no longer represents the current NFPA Standard on the subject matter addressed. NFPA encourages the use of the most current edition of any NFPA Standard [as it may be amended by TIA(s) or Errata] to take advantage of current experience and understanding. An official NFPA Standard at any point in time consists of the current edition of the document, including any issued TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, visit the "Codes & Standards" section at www.nfpa.org.

ISBN: 978-145592569-8 (PDF)

ADDITIONAL IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

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 a new edition, may be amended with the issuance of Tentative Interim Amendments (TIAs), or be corrected by Errata. It is intended that through regular revisions and amendments, participants in the NFPA standards development process consider the then-current and available information on incidents, materials, technologies, innovations, and methods as these develop over time and that NFPA Standards reflect this consideration. Therefore, any previous edition of this document no longer represents the current NFPA Standard on the subject matter addressed. NFPA encourages the use of the most current edition of any NFPA Standard [as it may be amended by TIA(s) or Errata] to take advantage of current experience and understanding. An official NFPA Standard at any point in time consists of the current edition of the document, including any issued TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, visit the "Codes & Standards" section at www.nfpa.org.

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® 731

Standard for the

Installation of Premises Security Systems

2020 Edition

This edition of NFPA 731, *Standard for the Installation of Premises Security Systems*, was prepared by the Technical Committee on Premises Security. It was issued by the Standards Council on November 4, 2019, with an effective date of November 24, 2019, and supersedes all previous editions.

This edition of NFPA 731 was approved as an American National Standard on November 24, 2019.

Origin and Development of NFPA 731

The 2006 edition of NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, was the first edition of this standard. The standard, which was developed in parallel with NFPA 730, *Guide for Premises Security*, provided details of how to install electronic premises security equipment. In addition to installation requirements, testing, inspection, and maintenance were addressed to provide a comprehensive document.

The 2008 edition deleted several of the references to Underwriters Laboratories standards. The recharging of batteries was changed from 24 hours to 48 hours, and the secondary power supply requirements were changed from 4 hours to 24 hours. A new Chapter 9 addressed transmission methods for off-premises communication. The standard defined several different verification methods.

The 2011 edition of the document was a total rewrite of the standard. Many of the changes were made to clarify existing requirements.

The 2015 edition was revised to update dates of many referenced publications. The requirements for low-power radio (wireless) systems were also updated. Requirements were clarified relative to the provisions of the security vulnerability assessment versus the risk assessment. Chapter 10 was updated to permit a written performance-based program for inspection, testing, and maintenance as an alternative means of compliance subject to the approval of the AHJ.

The major changes to the 2017 edition included revisions of 4.4.3.5, to clarify that there is not a single value for battery backup; 6.1.5.8 relative to wireless locking hardware interference with other wireless systems; Chapter 7, to address Internet protocol (IP) cameras, camera imaging, and network video recorders (NVR); Annex B, to address megapixel (MP) cameras; and Annex C, to include provisions pertaining to camera resolution, frame rate, compression, and bandwidth.

The 2020 edition saw an alignment of definitions between NFPA 731 and NFPA 730, *Guide for Premises Security*. The definitions of Chapter 3 have been reviewed and many revised to ensure consistency with those of NFPA 730. Definitions that are not used in NFPA 731 have been deleted. The SI/metric conversions have been reviewed throughout the document, and many values have been revised to ensure conversion accuracy.

The word *electronic* has been removed from the title of the document and throughout the document as NFPA 731 is not limited to electronic security but provides requirements for both electronic and mechanical means of protection. Requirements have been added relative to maintenance and prioritization of repairs. New criteria for Power over Ethernet (PoE) equipment and operation have been added.

Four new annexes, extracts from NFPA 730, have been added to provide easier reference and improve clarity: Annex D, Homeland Security Advisory System; Annex E, Critical Infrastructure Protection; Annex F, Special Events; and Annex G, Special Topics.

Technical Committee on Premises Security

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

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

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

Douglas P. Bassett, Xfinity Home, FL [IM]
Rep. Electronic Security Association

George Bish, Amazon/Ring Protect Inc., NC [M]

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. The Monitoring Association

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

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

Joe Gittens, Security Industry Association, MD [U]

Charles E. Hahl, GHD, NC [SE]

Matthew Jakusz, Iverify, NC [IM]

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

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

Scott Lord, Envision Technology Group, KS [U]
Rep. Partner Alliance for Safer Schools

Mark I. Morris, State Farm Insurance Company, IL [I]

Anthony Mucci, Johnson Controls, FL [M]

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

Richard Jay Roberts, Honeywell Fire Safety, IL [M]
Rep. National Electrical Manufacturers 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]
Rep. JENSEN HUGHES

Alternates

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)

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

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

Rick D. Sheets, AT&T Digital Life, TX [IM]
(Alt. to Douglas P. Bassett)

James M. Wenck, GHD, NC [SE]
(Alt. to Charles E. Hahl)

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 731

Standard for the

Installation of Premises Security Systems

2020 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. 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 shall be sent to the technical committee responsible for the source document.

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

Chapter 1 Administration

Δ **1.1 Scope.** This standard covers the application, location, installation, performance, testing, and maintenance of premises security systems and their components.

1.2 Purpose.

Δ **1.2.1** The purpose of this standard is to define the means of signal initiation, transmission, notification, and annunciation; the levels of performance; and the reliability of premises security systems. This standard addresses the integrity and reliability of cyber intrusion protection for equipment or systems network connected to the Internet of Things (IoT).

1.2.2 This standard defines the features associated with these systems and also provides information necessary to modify or upgrade an existing system to meet the requirements of a particular application.

1.2.3 This standard establishes minimum required levels of performance, extent of redundancy, and quality of installation but does not establish the only methods by which these requirements are to be achieved.

1.2.4 This standard shall not be interpreted to require a level of premises security other than that required by the applicable codes and standards.

1.3 Application.

Δ **1.3.1 Premises Security Systems.** Premises security systems shall include one or more of the following system types:

(1) Intrusion detection systems
(2) Access control systems
(3) Video surveillance systems
(4) Asset protection systems
(5) Environmental detection systems
(6) Holdup and duress systems
(7) Integrated systems

1.3.2 Endorsement. Any reference or implied reference to a particular type of hardware is for the purpose of clarity and shall not be interpreted as an endorsement.

1.3.3 Technical Terms. The intent and meaning of the terms used in this standard shall be, unless otherwise defined herein, the same as those of *NFPA 70*.

1.3.4 The requirements of NFPA 731 shall apply where expressly specified in an agreement or where required by an authority having jurisdiction.

1.3.5 Covered Locations.

Δ **1.3.5.1 Electronic Hardware Components.** This standard applies to new installations of premises security systems or their components installed for protection of building interiors, building perimeters, and surrounding property.

1.3.5.2 Other Hardware Components. This standard applies to nonelectronic building and physical security components where these items interface with, or become part of, a premises security system.

1.3.5.3 Software. In this standard, software includes the system firmware.

1.3.6 Exclusions.

1.3.6.1 One- and Two-Family Dwellings. Premises security systems installed in one- and two-family dwellings are not covered by this standard.

1.3.6.2 Information Technology Systems. The security of data or software in information technology or computer systems is not covered by this standard.

1.3.6.3 Portable Assets. The authorized removal of portable assets is not covered by this standard.

1.4 Retroactivity.

Δ **1.4.1** The provisions of this standard reflect situations and the state of premises security systems at the time the standard was issued.

1.4.2 Unless otherwise noted, it is not intended that the provisions of this standard be applied to facilities, equipment, structures, or installations that were existing or approved for construction or installation prior to the effective date of this standard.

1.5 Equivalency.

1.5.1 Nothing in this standard 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 standard.

1.5.2 Technical documentation shall be submitted to the authority having jurisdiction to demonstrate equivalency.

1.5.3 The system, method, or device shall be approved for the intended purpose by the authority having jurisdiction.

1.6 Units and Formulas.

1.6.1 Units. The units of measure in this standard are presented in the International System (SI) of Units. Where presented, U.S. customary units (inch-pound units) follow the SI units in parentheses.

1.6.2 Where both systems of units are presented, either system shall be acceptable for satisfying the requirements in this standard.

1.6.3 Where both systems of units are presented, users of this standard shall apply one set of units consistently and shall not alternate between units.

1.6.4 The values presented for measurements in this standard are expressed with a degree of precision appropriate for practical application and enforcement. It is not intended that the application or enforcement of these values be more precise than the precision expressed.

1.6.5 Where extracted text contains values expressed in only one system of units, the values in the extracted text have been retained without conversion to preserve the values established by the responsible technical committee in the source document.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document.

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

NFPA 10, *Standard for Portable Fire Extinguishers,* 2018 edition.

NFPA 70®, National Electrical Code®, 2020 edition.

NFPA 72®, National Fire Alarm and Signaling Code®, 2019 edition.

NFPA 80, *Standard for Fire Doors and Other Opening Protectives,* 2019 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2019 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2019 edition.

2.3 Other Publications.

2.3.1 ANSI Publications. American National Standards Institute, Inc., 25 West 43rd Street, 4th Floor, New York, NY 10036.

ANSI/ASA S1.4, *American National Standard Electroacoustics — Sound Level Meters — Part 3: Periodic Tests* (a nationally adopted international standard), 2014.

ANSI/TIA 568.3-D, *Optical Fiber Cabling and Components Standard*, 2016.

Δ **2.3.2 SIA Publications.** Security Industry Association, 8405 Colesville Road, Ste. 500, Silver Spring, MD 20910.

ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, 2014.

ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity*, 2000.

Δ **2.3.3 UL Publications.** Underwriters Laboratories Inc., 333 Pfingsten Road, Northbrook, IL 60062-2096.

UL 50, *Standard for Enclosures for Electrical Equipment, Non-Environmental Considerations*, 2015.

UL 50E, *Standard for Enclosures for Electrical Equipment, Environmental Considerations*, 2015.

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

UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems*, 1999, revised 2006.

UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, 2007, revised 2014.

UL 636, *Standard for Holdup Alarm Units and Systems*, 2013.

UL 639, *Standard for Safety for Intrusion-Detection Units*, 2007, revised 2011.

UL 827, *Standard for Central-Station Alarm Services*, 2014, revised 2016.

UL 1076, *Standard for Proprietary Burglar Alarm Units and Systems*, 2010.

UL 2044, *Standard for Commercial Closed-Circuit Television Equipment*, 2008, revised 2016.

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

UL 2900-2-3, *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems*, 2017.

UL 60065, *Standard for Audio, Video and Similar Electronic Apparatus*, 2015.

UL 60950-1, *Standard for Information Technology Equipment*, 2007, revised 2013.

UL 60950-22, *Standard for Information Technology Equipment — Equipment to Be Installed Outdoors*, 2007.

UL 62368, *Standard for Audio/Video, Information and Communication Technology Equipment*, 2014.

2.3.4 U.S. Government Publications. U.S. Government Publishing Office, 732 North Capitol Street, NW, Washington, DC 20401-0001.

ADA Accessibility Guidelines for Buildings and Facilities (ADAAG).

Title 47, Code of Federal Regulations, Part 15, "Radio Frequency Devices."

2.3.5 Other Publications.

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

2.4 References for Extracts in Mandatory Sections.

NFPA 72®, National Fire Alarm and Signaling Code®, 2019 edition.

Chapter 3 Definitions

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

3.2.4* 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.

3.2.5 Shall. Indicates a mandatory requirement.

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

3.2.7 Standard. An NFPA Standard, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and that is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA Manuals of Style. When used in a generic sense, such as in the phrase "standards development process" or "standards development activities," the term "standards" includes all NFPA Standards, including Codes, Standards, Recommended Practices, and Guides.

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.

3.3.2* Active Lock. An electric locking device that holds a portal closed and cannot be opened for egress by normal operation of the door hardware.

Δ **3.3.3* Ancillary Functions.** Monitored points that are not security points but are incorporated into a premises security system or outputs that are not necessary to the function of the premises security system.

Δ **3.3.4* Annunciator.** A unit containing one or more visible or audible indicators, alphanumeric displays, computer monitors, or other equivalent means in which each indication provides status information about a circuit, condition, system, or location.

3.3.5 Asset Protection System.

3.3.5.1* *Antenna.* The electronic article surveillance (EAS) system component installed at the premises exit point that generates a field to create an exit lane and receives signals from tags that enter the exit lane.

3.3.5.2 *Deactivator.* The EAS system component that is used to deactivate a tag's ability to be detected when in the exit lane.

3.3.5.3 *Detacher.* The EAS system component that is used to remove a tag from the protected item or merchandise.

3.3.5.4* *Electronic Article Surveillance (EAS).* A system used for collecting data, initiating alerts, preventing shoplifting, and like actions.

3.3.5.5 *Tag.* The EAS system component attached to the item or merchandise requiring detection when in the exit lane.

3.3.6* Closed Circuit Television (CCTV). A video system in which an analog or digital video signal travels from the camera to video monitoring stations at the protected premises.

3.3.7 Control Unit. A system component that monitors inputs and controls outputs through various types of circuits. [**72,** 2019]

3.3.8 Controller. A control unit used to provide the logic in an access control system.

3.3.9 Detection.

3.3.9.1 *Intrusion Detection.* The ability to detect the entry or attempted entry of a person or vehicle into a protected area.

3.3.9.2 *Sound Detection.* Recognition of an audio pattern indicative of unauthorized activity.

3.3.10 Device.

3.3.10.1 *Initiating Device.* A system component that originates transmission of a change-of-state condition.

3.3.10.1.1 *Ambush Alarm Initiating Device.* An initiating device or procedure that personnel authorized to disarm the intrusion system at a protected premises can use to transmit a signal indicating a forced disarming of an intrusion detection system.

3.3.10.1.2* *Duress Alarm Initiating Device.* An initiating device intended to enable a person at protected premises to initiate a signal indicating a need for assistance.

3.3.10.1.3* ***Holdup Alarm Initiating Device.*** An initiating device intended to enable an employee of a protected premises to transmit a signal indicating a robbery has transpired.

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

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

•

3.3.12 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.

•

Δ **3.3.13* Monitoring Station.** A facility that receives signals from premises security systems and has personnel in attendance at all times to respond to these signals.

3.3.13.1* ***Central Monitoring Station.*** A monitoring station whose ownership is not the same as that of the properties being monitored.

3.3.13.2* ***Proprietary Monitoring Station.*** A monitoring station having the same ownership as the property(ies) being monitored.

3.3.13.3 ***Public Safety Agency Monitoring Station.*** A monitoring station that is owned by a governmental body that monitors nongovernmental properties.

•

3.3.14 Position Sensor. A device that indicates whether a portal is open or closed.

Δ **3.3.15 Premises Security System.** See 3.3.27.6.

Δ **3.3.16* Premises Security System Provider.** A firm that provides all or some of the services required for the design, installation, testing, and maintenance of premises security systems.

•

3.3.17 Protective Wiring.

3.3.17.1 ***Grooved Striping.*** Soft wooden half-round dowels that are assembled to a surface in parallel runs of opposite polarity.

3.3.17.2 ***Open Wiring.*** A form of protective wiring used across skylights and in areas not subject to damage consisting of bare, hard-drawn solid copper wire not larger than 24 AWG that is arranged in two perpendicular banks of horizontal runs of opposite polarity at intervals not exceeding 101.6 mm (4 in.).

•

3.3.18* Reader. A device used in physical security systems to read a credential that allows access through access control points.

3.3.19 Record of Completion. A document that acknowledges the features of installation, operation (performance), service, and equipment with representation by the property owner, system installer, system supplier, service organization, and the authority having jurisdiction. [**72,** 2019]

3.3.20* Request to Exit (RTE). A device on the protected side of a portal that bypasses the door position switch or locking device to allow travel through the portal without causing an alarm.

3.3.21 Safe. An iron, steel, or equivalent container that has its door(s) equipped with a combination lock.

3.3.22* 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.

3.3.23 Security Personnel. Employees or contract service personnel charged with duties to aid in the protection at a protected premises.

3.3.24 Signal. An indication of a condition communicated by electrical, visible, visual, audible, wireless, or other means.

3.3.24.1* ***Alarm Signal.*** A signal that results from the manual or automatic detection of an alarm condition.

3.3.24.2 ***Supervisory Signal.*** A signal indicating the need for action in connection with the supervision of guard tours or environmental or other nonintrusion monitored point or system.

3.3.24.3 ***Trouble Signal.*** A signal that results from the detection of a trouble condition.

3.3.25 Special Instructions. A written directive between the responsible party for a protected premises and a monitoring station describing disposition and handling of signals.

3.3.26 Strain Relief. Cable termination that provides structural rigidity of conductors under conditions of flexure.

3.3.27 System.

3.3.27.1* ***Combination System (as related to premises security).*** A system that provides premises security as a portion of a single control unit, or multiple control units that work together to provide one integrated control.

3.3.27.2* ***Digital Imaging System (DIS).*** A video system in which a digital video signal travels from the camera and can be viewed by any authorized user at or away from the protected premises.

3.3.27.3 ***Duress Alarm System.*** A system or portion thereof that connects to duress alarm initiating devices.

3.3.27.3.1 ***Private Duress Alarm System.*** A system or portion thereof in which the action to activate the duress signal is known only to the person activating the device.

3.3.27.3.2 ***Public Duress Alarm System.*** A system or portion thereof in which the ability to activate a duress signal is available to any person at the protected premises.

3.3.27.4 ***Holdup Alarm System.*** A system or portion thereof that connects to holdup alarm initiating devices.

•

Δ **3.3.27.5*** ***Integrated System.*** A control unit that includes other types of systems in addition to the premises security system.

•

Δ **3.3.27.6** ***Premises Security System.*** A system or portion of a combination system that consists of components and circuits arranged to monitor or control activity at or access to a protected premises.

3.3.28 Trap.

3.3.28.1* ***Ball Trap.*** A device consisting of two spring-tensioned balls that form a connector into which a flat

metal clip that is attached to a conductor can be inserted to complete a circuit.

3.3.28.2 ***Barrier Bar Trap.*** A device consisting of a pressure-sensitive switch that is mounted onto one end of an adjustable bar that is installed across an opening.

3.3.28.3* ***Disconnecting Trap.*** A device intended to supervise the position of an air conditioner, small fan, fixed panel, or similar opening against movement in either direction with the use of a conductor or trip cord extended across the opening.

3.3.29* 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.

3.3.30 Verification.

3.3.30.1 ***Enhanced Call Verification (ECV).*** The attempt by monitoring station personnel to establish that an emergency exists at the protected premises by means of two or more verification calls.

3.3.30.2 ***Multiple Trip Verification (MTV).*** A method to validate an alarm signal by any of the following: (1) connection of sensors in a manner such that more than one sensor must be in alarm before an alarm signal is transmitted to the monitoring station, or (2) verification algorithm in a premises security system that interprets multiple sensor inputs, or (3) procedural methods or programs employed by monitoring station personnel to interpret multiple alarm signals from a protected premises.

3.3.30.3 ***Remote Audio Verification (RAV).*** The attempt by monitoring station personnel to establish that an emergency exists at the protected premises by listening to live audio feed from the protected premises.

3.3.30.4 ***Remote Video Verification (RVV).*** The attempt by monitoring station personnel to establish that an emergency exists at the protected premises by watching video received from the protected premises.

Chapter 4 Fundamentals

4.1 General.

Δ **4.1.1** The basic functions of premises security systems in Chapters 5 through 10 shall meet the requirements of this chapter.

4.1.2 When a premises security system connects to a fire alarm system or other life safety systems, the requirements of other codes and standards pertaining to those systems shall be followed.

Δ **4.1.3** When a premises security system is interconnected with an ancillary system, the ancillary system shall not interfere with the operation of the premises security system.

4.1.4 Priority of other signals over security system alarms shall be permitted where evaluated by the stakeholders through a risk analysis.

4.2 Equipment.

4.2.1 Equipment constructed and installed in conformity with this standard shall be listed for the purpose for which it is used.

Δ **4.2.2*** The premises security system components shall be installed in accordance with the manufacturers' published installation instructions.

4.2.3 Equipment that utilizes initiating, annunciating, and remote control devices that provide signaling by means of low-power radio frequency shall operate in accordance with 47 CFR 15, "Radio Frequency Devices."

4.2.4* Equipment that has the physical appearance of a life safety device or appliance but does not perform its apparent life safety function shall be prohibited.

4.3 Personnel Qualifications.

4.3.1 System Design.

Δ **4.3.1.1*** Persons who develop plans and specifications in accordance with this standard shall be experienced in the design, application, installation, and testing of premises security systems.

4.3.1.2 The system designer shall be identified on the system plans and specifications.

4.3.1.3 Evidence of qualifications shall be provided when requested by the AHJ.

4.3.1.4 Qualified personnel shall include but not be limited to one or more of the following:

(1) Personnel trained and certified by the equipment manufacturer
(2) Personnel licensed and certified by state or local authority
(3) Personnel certified by an accreditation program or industry-recognized program acceptable to the AHJ
(4) Personnel having completed a formal technical training program arranged by the security system provider and acceptable to the AHJ

4.3.2* System Installation.

Δ **4.3.2.1** Installation personnel shall be supervised by persons who are qualified and experienced in the installation, inspection, and testing of premises security systems.

Δ **4.3.2.2** Qualified personnel shall include but not be limited to one or more of the following:

(1) Personnel trained and certified by the equipment manufacturer
(2) Personnel licensed or certified by federal, state, or local authority
(3) Personnel certified by an accreditation program or industry-recognized program acceptable to the AHJ
(4)* Trained and qualified personnel employed by an organization listed by a national testing laboratory for the servicing of premises security systems

4.4 Power.

4.4.1 Power Supplies.

4.4.1.1 Power supplies shall be installed in conformity with the requirements of *NFPA 70*.

4.4.1.2 Power supplies shall be reliable and have the capacity to service the intended load.

Δ **4.4.1.3*** At least two independent power supplies shall be required, one primary and one secondary, for the following premises security systems:

(1) Intrusion detection systems
(2) Holdup, duress, and ambush systems
(3) Power over Ethernet (PoE) power source equipment (PSE)

4.4.1.4 When installed, secondary power supplies that are not required by 4.4.1.3 shall conform to the requirements of this standard.

4.4.2 Primary Supply.

4.4.2.1 Primary (main) power shall be supplied from either a dedicated branch circuit or the unswitched portion of a branch circuit by one of the following means:

(1) Commercial light and power
(2) An engine-driven generator or equivalent in accordance with 4.4.5, where a person specifically trained in its operation is on duty at all times
(3) An engine-driven generator or equivalent arranged for cogeneration with commercial light and power in accordance with 4.4.5, where a person specifically trained in its operation is on duty at all times
(4)* An alternative energy source with capacity required by the security vulnerability assessment (SVA)

4.4.2.2 Circuit disconnecting means shall have a distinctive marking, be accessible only to authorized personnel, and be identified as "PREMISES SECURITY CIRCUIT."

4.4.2.3 The location of the circuit disconnecting means shall be permanently identified at the premises security control unit.

4.4.2.4 Primary (main) power supplies to equipment that include Class 2 or Class 3 plug-in transformers utilizing receptacles shall be mechanically secured to prevent inadvertent disconnection.

4.4.2.5 An overcurrent protective device of the correct current-carrying capacity and capable of interrupting the maximum short-circuit current to which it could be subjected shall be provided in each ungrounded conductor.

4.4.2.6 A transient voltage surge protection device or circuit shall be installed at or incorporated into the primary power supply for the following:

(1) Microprocessor-based control units
(2) Microprocessor-based subpanels
(3) Microprocessor-based annunciators
(4) Other microprocessor-based equipment

4.4.2.7 Circuit breakers or engine stops shall not be installed in such a manner as to cut off the power for lighting or for operation of elevators.

4.4.3 Secondary Supply.

4.4.3.1 The secondary (standby) power supply shall supply energy to the system in the event of total failure of the primary (main) power supply or when the primary voltage drops to a level insufficient to maintain functionality of the control equipment and system components.

4.4.3.2 When primary power is lost or incapable of providing the minimum voltage required for normal operation, the secondary supply shall automatically supply the power to the system without loss of signals or causing transmission of an alarm.

4.4.3.3 For an integrated system, the secondary supply capacity required by 4.4.1.4 shall include the load of all premises security–related equipment, functions, or features that are not automatically disconnected upon transfer of operating power to the secondary supply.

Δ **4.4.3.4** The secondary supply shall consist of one of the following:

(1) A storage battery dedicated to the premises security system arranged in accordance with 4.4.4
(2) An individual branch circuit of an automatic-starting engine-driven generator arranged in accordance with 4.4.5 and storage batteries dedicated to the premises security system with 15 minutes of capacity under maximum alarm load
(3) An emergency generating system as defined in *NFPA 70*, Article 700

4.4.3.5* The secondary supply shall have the capacity to operate a premises security system for the longest time required by any of the following:

(1) SVA (satisfies the needs determined)
(2) System design
(3) Manufacturer's published instructions
(4) Other applicable standards

4.4.3.6 Operation of secondary power shall not affect the required performance of a premises security system.

4.4.3.7 The system shall produce the same alarm and trouble signals and indications, excluding the ac power indicator, when operating from the standby power source as are produced when the unit is operating from the primary power source.

Δ **4.4.3.8** The secondary power supply shall automatically provide power to the premises security system within 10 seconds whenever the primary power supply fails to provide the minimum voltage required for operation.

4.4.3.9 Required signals shall not be lost, interrupted, or delayed for more than 10 seconds as a result of the primary power failure.

Δ **4.4.3.10** Storage batteries dedicated to the premises security system or an uninterruptible power supply (UPS) arranged in accordance with the provisions of NFPA 111 shall be permitted to supplement the secondary power supply to ensure required operation during the transfer period.

4.4.3.11 Where a UPS is employed in 4.4.3.10, a positive means for disconnecting the input and output of the UPS system while maintaining continuity of the power supply to the load shall be provided.

N **4.4.3.12** If the surveillance system, access control system, or any other premises security system utilizes Power over Ethernet (PoE) technology comprised of power source equipment (PSE) and powered devices (PD), the PSE shall have a secondary power source listed for the purpose and installed in accordance with *NFPA 70*.

4.4.4 Storage Batteries.

4.4.4.1 Batteries shall be permanently marked using the month/year format with all of the following information:

(1) Date of manufacture
(2) Date of installation

4.4.4.2 Batteries shall be replaced in accordance with the earlier of the following:

(1) Recommendations of the electronic premises security equipment manufacturer
(2) Within 5 years of manufacture for sealed lead-acid batteries

4.4.4.3 Storage batteries shall be located so that the premises security equipment, including overcurrent devices, are as follows:

(1) Readily accessible as defined by *NFPA 70*
(2) Not adversely affected by battery gases
(3) In accordance with the requirements of *NFPA 70*, Article 480

4.4.4.4 Cells shall be insulated against grounds and crosses.

4.4.4.5* Batteries shall be mounted as follows:

(1) In an enclosure approved for the application
(2) In accordance with 4.6.2.2

4.4.4.6 Battery racks shall be protected against corrosion.

Δ **4.4.4.7** If not located in or adjacent to the premises security system control unit, the batteries and their charger location shall be permanently identified at the premises security control unit.

4.4.4.8 In-line overcurrent protection shall be between the secondary power supply batteries and the secondary power supply.

4.4.4.9 Battery charging rates shall comply with all of the following:

(1) Maintain the battery fully charged under all conditions of normal operation
(2) Provide capacity to recharge batteries within 48 hours if fully discharged
(3) Not cause battery damage when fully charged

4.4.4.10 The batteries shall be protected against excessive load current by overcurrent devices.

4.4.4.11 The batteries shall be protected from excessive charging current by overcurrent devices or by automatic current-limiting design of the charging source or similar technology.

4.4.4.11.1 A means for monitoring the integrity of the batteries and charger shall be provided to detect a battery charger failure.

4.4.4.11.2 Failure of the battery charger shall result in the initiation of a trouble signal.

4.4.5 Engine-Driven Generator Installation. The installation of engine-driven generators shall conform to the provisions of *NFPA 70*, Article 700, and NFPA 110.

4.5 System Functions.

4.5.1 Premises security system functions shall be permitted to be performed automatically.

Δ **4.5.2*** The performance of premises security system functions shall not interfere with power for fire alarms, for lighting, or for operation of elevators, building control, or other life safety systems.

Δ **4.5.3** The performance of premises security system functions shall not preclude the combination of other services requiring monitoring of operations.

4.5.4 Premises security system alarms, supervisory signals, and trouble signals shall be distinctively and descriptively annunciated.

4.5.5 Equipment shall be designed so that it is capable of performing its intended functions under the following conditions:

(1) At 85 percent and at 110 percent of the nameplate primary (main) and secondary (standby) input voltage(s)
(2) At ambient temperatures of 0°C (32°F) and 49°C (120°F)
(3) At a relative humidity of 85 percent and an ambient temperature of 30°C (86°F)

4.5.6 Equipment intended for use in damp, wet, or exterior environments shall be listed for the use.

4.6 Installation and Design.

4.6.1 General.

4.6.1.1 Where required, the AHJ shall approve system design and installation.

Δ **4.6.1.2*** The site shall be inspected for environmental factors that affect the operation of the premises security system.

4.6.1.3 The devices installed shall perform their intended functions in the environmental conditions at the protected premises.

4.6.2 Equipment.

4.6.2.1 Devices, appliances, and control units shall be located and mounted so that accidental operation or failure is not caused by vibration or jarring.

4.6.2.2 Unless otherwise permitted by the manufacturer, control units, power supplies, and batteries shall be mounted in the vertical, upright position.

4.6.2.3* All equipment requiring manual resetting to maintain normal operation shall have an indication to the user that the device has not been restored.

4.6.2.4 Equipment shall be installed in locations where conditions do not exceed the voltage, temperature, and humidity limits specified in 4.5.5 unless listed for the application.

4.6.2.5* Control units and subcontrols shall be accessible to service personnel.

4.6.2.6* To reduce the possibility of damage by induced transients, circuits and equipment shall be protected in accordance with the requirements of *NFPA 70*.

4.6.3 Wiring.

4.6.3.1 The installation of all wiring, cable, and equipment shall be performed in accordance with *NFPA 70*, Article 725 or Article 800, where applicable.

4.6.3.2 Optical fiber cables shall be protected against mechanical injury in accordance with *NFPA 70*, Article 770.

4.6.3.3* A conductor shall be spliced or joined with a mechanical splicing device listed for this purpose.

Δ **4.6.3.4*** Unless specifically allowed by the manufacturer's wiring specifications, low-voltage premises security system wiring shall be spaced at least 50.8 mm (2 in.) from conductors of any light and power circuits, unless one of the circuits is in raceway listed for the purpose.

4.6.3.5* Premises security system wiring and cables shall be of the gauge, strands, insulation, and electrical properties specified by the equipment manufacturer.

4.6.3.6 Connections of conductors to terminal parts shall ensure a tight, conductive connection without damaging the conductors and be made by means of pressure connectors, wire binding screws, or splices to flexible leads.

4.6.3.7 Conductors shall be connected to devices and to fittings so that tension is not transmitted to joints or terminals.

4.6.3.8 Wires and cables shall not be placed in such a manner as to prevent access to equipment.

4.6.3.9 Terminals for more than one conductor shall be identified and intended for the purpose.

4.6.3.10 Conductors under a single terminal shall be of the same gauge and composition.

4.6.3.11* Terminals shall be marked or color coded where necessary to indicate the correct connections.

4.6.3.12* At raceway connections to junction boxes and open ends of raceways, the following shall apply:

(1) Conductors shall be protected from abrasion.
(2) Raceway shall be sized and installed in accordance with *NFPA 70*.

4.6.3.13 Circuit identification shall be within the control panel and enclosures used for wiring connections.

4.6.3.14 Circuit identification shall not be visible to the public.

4.6.3.15 Strain relief shall be provided for wiring leaving control panels and junction boxes not utilizing raceway.

4.6.4 Service Loops — Metallic Conductors.

4.6.4.1 A minimum 152.4 mm (6 in.) service loop shall be at control panels and enclosures used for wiring terminations.

4.6.4.2 A minimum 152.4 mm (6 in.) service loop shall be at field terminations.

4.6.4.3 Where exposed or subject to damage, service loops shall be mechanically secured.

4.6.5 Service Loops — Optical Fiber Cables.

4.6.5.1 A service loop shall be at control panels and enclosures and field terminations.

4.6.5.2 The radius of the service loop shall meet the manufacturer's specifications.

4.6.5.3 If no manufacturer's specifications exist, the radius shall not be less than 10 times the cable diameter.

4.6.5.4 Where exposed or subject to damage, service loops shall be mechanically protected.

4.7* Special Requirements for Low-Power Radio (Wireless) Systems.

4.7.1* Listing Requirements. Low-power radio equipment shall be specifically listed for the purpose.

4.7.2 Power Supplies. A primary battery (dry cell) shall be permitted to be used as the sole power source of a low-power radio transmitter where all of the following conditions are met:

(1) Each transmitter serves only one device.
(2) Each transmitter is individually identified at the receiver/control unit.
(3) The battery is capable of operating the low-power radio transmitter for not less than 1 year before the battery depletion threshold is reached.
(4) A battery depletion signal is transmitted before the battery has been depleted to a level below that required to support alarm transmission for 7 additional days of nonalarm operation and incorporates the following:
    (a) This signal is distinctive from alarm, supervisory, tamper, and trouble signals.
    (b) This signal visibly identifies the affected low-power radio transmitter.
    (c) This signal, when silenced, automatically re-sounds at least once every 4 hours.
(5) Catastrophic (open or short) battery failure causes the following conditions:
    (a) A trouble signal identifies the affected low-power radio transmitter at its receiver/control unit.
    (b) When silenced, the trouble signal automatically re-sounds at least once every 4 hours.
(6) Any mode of failure of a primary battery in a low-power radio transmitter does not affect any other low-power radio transmitter.

4.7.3 Alarm Signals.

4.7.3.1* When actuated, each low-power radio transmitter shall automatically transmit an alarm signal.

4.7.3.2* Each low-power radio transmitter shall automatically repeat alarm transmission at intervals not exceeding 60 seconds until the initiating device is returned to its nonalarm condition.

4.7.3.3 Fire alarm signals shall have priority over all other signals.

4.7.3.4 The maximum allowable response delay from activation of an initiating device to receipt and display by the receiver/control unit shall be 10 seconds.

Δ **4.7.3.5** An alarm signal from a low-power radio transmitter shall identify the particular initiating device in alarm at its receiver/fire alarm control unit until manually reset.

4.7.4 Monitoring for Integrity.

4.7.4.1* The low-power radio transmitter shall be specifically listed as using a transmission method that is highly resistant to misinterpretation of simultaneous transmissions and to interference.

Δ **4.7.4.2** The occurrence of any single fault that disables transmission between any low-power radio transmitter and the receiver/fire alarm control unit shall cause a latching trouble signal within 200 seconds.

4.7.4.3 A single fault on the signaling channel shall not cause an alarm signal.

4.7.4.4 The periodic transmission required to comply with 4.7.4.2 from a low-power radio transmitter shall ensure successful alarm transmission capability.

4.7.4.5 Removal of a low-power radio transmitter from its installed location shall cause immediate transmission of a distinctive supervisory signal that indicates its removal and individually identifies the affected device.

4.7.4.6 Reception of any unwanted (interfering) transmission by a retransmission device (repeater) or by the main receiver/control unit for a continuous period of 20 seconds or more shall do the following:

(1) Cause an audible and visible trouble indication at the main receiver/control unit
(2) Identify the specific trouble condition as an interfering signal

4.7.5 Output Signals from Receiver/Control. When the receiver/control is used to actuate remote appliances, such as notification appliances and relays, by wireless means, the remote appliances shall meet the following:

(1) Power supplies comply with Chapter 4 or the requirements of 4.7.2.
(2) Monitoring for integrity complies with requirements in Chapter 4 or 4.7.4.
(3) Maximum allowable response delay from activation of an initiating device to activation of required alarm functions is not more than 10 seconds.
(4) Each receiver/control automatically repeats alarm transmission at intervals not exceeding 60 seconds or until confirmation that the output appliance has received the alarm signal.
(5) Appliances continue to operate (latch-in) until manually reset at the receiver/control.

4.8 Grounding.

4.8.1 All grounding shall be in accordance with *NFPA 70*.

4.8.2 Additional grounding shall be in accordance with manufacturer's requirements.

4.8.3 All other circuits shall test free of grounds.

4.9 Zoning and Annunciation.

4.9.1* Required annunciation shall comply with the following:

(1) Readily accessible to responding personnel
(2) Located as required by the AHJ

4.9.2* Where required, the location of an operated initiating device shall be visibly indicated by building, floor, or other approved subdivision by annunciation, printout, or other approved means.

4.9.3 Where required, the visible indication shall not be canceled by the operation of an audible alarm silencing means.

4.9.4* Visual annunciators shall be capable of displaying all locations in alarm.

4.9.5 If all locations in alarm are not displayed simultaneously, visual indication shall show that other locations are in alarm.

4.10 Software Control.

4.10.1 Where required, software provided with a premises security system shall be listed for use with the equipment on which it is installed.

4.10.2* A record of installed software version numbers shall be maintained at a location approved by the AHJ.

4.10.3* Software shall be protected from unauthorized changes.

4.10.4 All software changes shall be tested in accordance with 10.4.2.

N **4.10.5** Where required by the AHJ or SVA, equipment that is network connected shall be in compliance with applicable standards such as UL 2900-2-3, *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems.*

4.11 Interconnected and Combination Systems.

4.11.1 General.

4.11.1.1 Premises security systems shall be permitted to be either integrated systems combining detection, notification, and auxiliary functions in a single system or a combination of component subsystems.

4.11.1.2 Premises security system components shall be permitted to share control equipment or be able to operate as standalone subsystems arranged to function as a single system.

4.11.1.3 All component subsystems shall be capable of simultaneous, full-load operation without degradation of the required overall system performance.

4.11.1.4 Where required by other sections of this standard, additional power supplies provided for control units, circuit interfaces, or other equipment essential to system operation, located remote from the main control unit, shall comprise a primary power supply and a secondary power supply meeting the requirements of 4.4.1 through 4.4.4.

4.11.2 Interconnections.

4.11.2.1 Where required, the method of interconnection of control units shall meet the conductor integrity monitoring requirements of 5.1.4.

4.11.2.2 Interconnections shall be achieved by one of the following recognized means:

(1) Electrical contacts listed for the connected load
(2)* Listed digital data interfaces
(3) Other listed methods

4.11.2.3 If approved by the AHJ, interconnected control units providing localized detection, signaling, and ancillary functions shall be permitted to be monitored by a premises security system as initiating devices.

4.11.2.4 Each interconnected control unit shall be separately monitored for alarm, trouble, and supervisory conditions.

4.11.2.5 Interconnected control unit alarm signals shall be permitted to be monitored by zone or combined common signals.

4.11.3 Combination Systems.

Δ **4.11.3.1** Systems other than premises security systems shall be permitted to share components, equipment, circuitry, and installation wiring with premises security systems.

Δ **4.11.3.2** To maintain the integrity of premises security system functions, the provision for removal, replacement, failure, or maintenance procedure on any supplementary hardware, software, or circuit(s) shall not impair the required operation of the premises security system.

Δ **4.11.3.3** If the AHJ determines that the information being displayed or annunciated on a combination system is excessive, causing confusion and delayed response to an emergency, the AHJ shall be permitted to require a separate display or annunciation of information for the premises security system.

4.12 Documentation and Training.

4.12.1 General.

4.12.1.1 The AHJ shall be notified prior to the start of installation, if required.

4.12.1.2 Notification of alteration of equipment or wiring shall be provided to the AHJ, if requested.

4.12.1.3 At the AHJ's request, complete information regarding the system or system alterations, including specifications and battery calculations, shall be provided.

4.12.1.4 Before requesting final approval of the installation, if required by the AHJ, the installing contractor shall verify that the system has been installed in accordance with the system design and tested in accordance with the manufacturer's published instructions.

Δ **4.12.2* Documentation.**

Δ **4.12.2.1** Every system installation shall include the following documentation:

(1)* Owner's manual
(2) User's instructions
(3)* A record of completion by the system installer
(4) Name and contact telephone number of the organization maintaining the premises security system
(5) Name and contact telephone number of the organization monitoring the premises security system displayed at the control unit
(6) Any other documentation required by law or the AHJ

4.12.2.2 Upon final acceptance of the system, documentation shall be delivered to the responsible party for the protected premises.

4.12.3 Training.

4.12.3.1* The owner or the leasee of the system serving the protected premises shall arrange for training of the system users.

4.12.3.2 The service provider shall provide this training.

4.12.3.3* User training shall be documented.

4.12.3.3.1 Training documentation shall be maintained for 1 year as part of the system documentation.

4.12.3.3.2 Training documentation shall be provided, when requested, to the AHJ.

Chapter 5 Intrusion Detection Systems

5.1 General.

N **5.1.1 Intrusion Detection Systems.** Intrusion detection systems shall be installed in accordance with this section.

N **5.1.2 Installation and Design.** Intrusion detection systems shall be designed to detect vulnerabilities identified by one or more of the following:

(1) Security vulnerability assessment
(2) AHJ
(3) Qualified security professional per 4.3.1.4

5.1.3 Interconnecting Control Units.

5.1.3.1 Control units, subcontrols, and devices that are used to interconnect the control unit to protection devices shall be located within the area being protected by the system.

5.1.3.2 If the enclosures for such equipment are not located in such an area, the enclosures shall be protected by one of the following methods:

(1) Continuously under the notice of assigned security personnel
(2) Located in an area that is accessible only to authorized personnel
(3) Supervised to annunciate tampering

5.1.4 Monitoring Integrity of Conductors.

5.1.4.1 All means of connection between a control unit and its primary and secondary power supplies, including accessories essential to the operation of the premises security system control unit, shall be monitored for integrity.

5.1.4.1.1 The occurrence of a single fault shall be indicated within 200 seconds.

5.1.4.1.2 The restoration to normal operation shall be automatically indicated within 200 seconds.

5.1.4.2* Wiring to all initiating devices of an intrusion detection system shall be monitored for integrity so that the presence of an off-normal condition is automatically indicated to the user upon arming of the system.

5.1.4.3 Interconnecting wiring between the protected premises control unit and the separate signal transmission equipment shall be monitored for integrity or physically protected.

5.1.4.4 A fault on wiring to initiating devices shall not restore or clear an unacknowledged alarm signal at the control unit.

5.1.5 Intrusion Detection Alarm Signals. Alarm signals from an intrusion detection system shall cause one or more of the following:

(1) A signal sent to a monitoring station
(2) Activation of a signaling device at the protected premises

5.1.6 Entry/Exit Delay.

5.1.6.1 A delay circuit that allows entry into protected premises shall be limited to only those initiating devices, such as door contacts installed on entry doors and interior sensors, that must be bypassed to allow access to the mechanism that is used to place the system in a disarmed state.

5.1.6.2* The mechanism that is used to disarm the system shall be reachable within 15 seconds of the entry portal.

5.1.6.3 The entry time shall not exceed 240 seconds.

5.1.6.4 The exit delay shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, Section 4.2.2.

5.1.6.5 The entry delay shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, Section 4.2.3.

5.1.7* Installation Requirements.

5.1.7.1 Devices shall be installed in accordance with the manufacturer's published installation instructions.

5.1.7.2 Selection and placement of devices shall be based on the intended threat and environmental conditions as specified by the designer in consultation with the end user.

5.2 Exterior Space Detection Systems. Signals from exterior space detection systems shall not be dispatched as an alarm unless alarm verification in accordance with 9.6.1.1 is used.

5.2.1 Photoelectric Detector.

Δ **5.2.1.1** Photoelectric detector units shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.1.2 An alarm signal shall be initiated when a minimum of two of the following parallel units mounted on the same vertical plane are activated:

(1)* Two photoelectric detector units
(2) One photoelectric detector unit and one unit of another technology as described in this standard

5.2.2* Motion Detection.

Δ **5.2.2.1** Motion detection units shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.2.2 Passive infrared (PIR) units shall meet the requirements of ANSI/SIA PIR-01, *Passive Infrared Motion Detector Standard — Features for Enhancing False Alarm Immunity*.

5.2.3 Exterior Structure Detectors.

Δ **5.2.3.1** Exterior structure detectors shall be in compliance with applicable standards, such as UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, and UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.3.2* Exterior structure detectors shall include but not be limited to the following types:

(1) Audio
(2) Contacts
(3) Fiber optic
(4) Protective cabling
(5) Proximity
(6) Shock sensors
(7) Stress sensors

5.2.4 Exterior Buried Detectors.

Δ **5.2.4.1** Exterior buried detectors shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.2.4.2 Exterior buried detectors shall include, but not be limited to, the following types:

(1) Electromagnetic
(2) Fiber-optic
(3) Leaky coaxial
(4) Seismic

5.2.4.3* Video Motion Detection (VMD). When activated, video motion detectors shall annunciate at one or more of the following and display the captured image:

(1) The protected premises
(2) The monitoring station

5.3 Interior Detection Systems.

5.3.1* Interior detection devices shall be installed in accordance with the manufacturer's published instructions.

5.3.2 When activated, interior protection devices shall annunciate at the protected property and/or transmit an alarm signal.

5.3.3 When activated, alarm signals from interior detection systems shall be verified in accordance with 9.6.1.1 prior to a request for service made to an AHJ.

5.3.3.1* Doors, Windows, Other Openings, and Building Perimeter.

Δ **5.3.3.1.1 Contacts.** Contacts shall be in compliance with applicable standards such as UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*.

5.3.3.1.2* Selection. The selection of the contact shall be based on the physical attributes of the mounting point of the contact on the doors, windows, or other openings.

5.3.3.1.3 Protective Wiring.

Δ **5.3.3.1.3.1** Screens, including wood doweling and mesh type, shall be in compliance with applicable standards, such as UL 606, *Standard for Linings and Screens for Use with Burglar-Alarm Systems*, and UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*.

5.3.3.1.3.2 Protective wiring shall include but not be limited to the following types:

(1) Grooved striping
(2) Lacing
(3) Open wiring
(4) Screens, including wood doweling and mesh type

5.3.3.1.4 Traps.

5.3.3.1.4.1 Traps shall be listed or labeled in compliance with applicable standards.

5.3.3.1.4.2 Traps shall include but not be limited to the following types:

(1) Ball
(2) Barrier bar
(3) Disconnecting

Δ **5.3.3.1.5 Shock (Vibration) Sensors.** Shock sensors shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.6 Glass Break Sensors.

Δ **5.3.3.1.6.1** Glass break sensors shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.6.2 Glass break sensors shall include but not be limited to the following types:

(1) Shock
(2) Audio

Δ **5.3.3.1.7 Sound Detectors.** Sound detectors shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

Δ **5.3.3.1.8 Photoelectric Detectors.** Photoelectric detector units shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.9 Motion Detection.

Δ **5.3.3.1.9.1** Motion detectors shall be in compliance with applicable standards, such as UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.3.1.9.2 Motion detectors used for protection of openings and building perimeters shall be installed in accordance with the manufacturer's published instructions.

5.3.3.1.9.3 Motion detectors shall not be installed in environments that negatively affect the operation.

5.3.3.1.9.4 Motion detectors shall include, but not be limited to, the following:

(1) Two or more technologies combined in a single device
(2) Microwave
(3) Passive infrared (PIR)

5.3.3.1.10* Video Motion Detection (VMD). When activated, video motion detectors shall annunciate at one or more of the following and display the captured image:

(1) The protected premises
(2) The monitoring station

5.3.4 Pressure-Sensitive Devices.

Δ **5.3.4.1** Pressure-sensitive devices shall be in compliance with applicable standards, such as UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.3.4.2 Pressure-sensitive devices shall include but not be limited to the following:

(1) Floor mats
(2) Stress sensors

5.4 Vaults, Safes, ATMs, and Secured Containers.

5.4.1* Section 5.4 shall not apply where other security standards supersede these requirements.

5.4.2 Vaults.

Δ **5.4.2.1** Vault detection devices shall be in compliance with applicable standards, such as UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.4.2.2 Vault detection devices shall be installed in accordance with the manufacturer's instructions.

5.4.2.3 Vault detection shall include but not be limited to one or more of the following components:

(1) Contacts
(2) Embedded cable
(3) Foil lining
(4)* Heat detection
(5) Shock
(6)* Smoke detection
(7) Sound

5.4.3 Safes.

Δ **5.4.3.1** Safe detection devices shall be in compliance with applicable standards, such as UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or UL 639, *Standard for Safety for Intrusion-Detection Units*.

5.4.3.2* Safe detection devices shall be installed in accordance with the manufacturer's instructions.

5.4.3.3 Safe detection shall include but not be limited to one or more of the following devices:

(1) Contacts
(2) Proximity
(3) Foil lining
(4) Shock
(5) Sound

5.4.4 Automatic Teller Machines (ATMs). Protection of ATMs shall be the same as for safes, and the requirements of 5.4.3 shall be met.

5.4.5 Secure Containers. Protection of secure containers shall be the same as for safes, and the requirements of 5.4.3 shall be met.

Chapter 6 Electronic Access Control Systems

6.1 General. This section shall apply to physical electronic access control systems only.

Δ **6.1.1 Equipment.** Electronic access control equipment shall be in compliance with applicable standards, such as UL 294, *Standard for Access Control System Units*.

6.1.2 Interconnecting Control Units.

6.1.2.1 Control units, subcontrols, and devices that are used to interconnect the control unit to system devices shall be located within the protected premises.

6.1.2.2 If the enclosures for such equipment are not located in such an area, the enclosures shall be protected by one of the following methods:

(1) Continuously under the notice of assigned security personnel
(2) Located in an area that is accessible only to authorized personnel
(3) Supervised to annunciate tampering

6.1.3* Portal. The system shall be designed to control the unauthorized access of people, vehicles, and/or property through a portal as prescribed by the AHJ.

6.1.4* Reader.

6.1.4.1* Readers shall be mounted in accordance with adopted local codes and the requirements of the AHJ.

6.1.4.2 When the portal is a door, readers shall be mounted on the latch side.

Exception: If there are barriers to mounting the reader on the latch side of the door, the reader shall be mounted at the closest location that is not behind the door when it is open.

6.1.4.3* Clearance between the reader and the portal shall be provided to enable the user to initiate the portal action.

6.1.4.4 Access to the readers shall not be obstructed where manual presentation is required.

6.1.4.5 Where manual presentation of access credentials is required for a vehicle, the reader shall be readily accessible from the operator's position of vehicles common to the site.

6.1.4.6 All readers shall provide a visual or audible indication that the credential has been recognized.

6.1.4.7* The maximum interval of time between the recognition of a valid credential and the unlocking of a portal shall not exceed 10 seconds.

6.1.5 Locking Systems.

6.1.5.1* Control of egress shall comply with the requirements of the applicable codes and standards based on the occupancy and usage of the facility.

6.1.5.2* Locking systems shall be installed in accordance with the manufacturer's instructions.

6.1.5.3 Installation of locking hardware on swinging, sliding, and overhead fire-rated door assemblies shall be in accordance with the listing of the doors and frames, in compliance with NFPA 80.

6.1.5.4* Portals shall automatically lock where the portal is supervised by the access control system.

6.1.5.5* Where delayed egress function is used in conjunction with an access control system, equipment shall be listed for the purpose and be installed in accordance with the applicable codes and standards based on the occupancy and usage of the facility.

6.1.5.6 Where a portal is a required means of egress and is provided with an active lock, the locking system shall comply with 6.1.5.6(1) OR 6.1.5.6(2) except as otherwise permitted by 6.1.5.7:

(1)* *Manual Request to Exit (RTE) on Door.* A manual RTE device meeting all the following criteria shall be provided:
   (a) The manual RTE device shall be provided on the egress side of the portal.
   (b) The manual RTE device shall be positioned on the door leaf, gate, or other physical barrier at the portal egress opening.
   (c) The manual RTE device, when operated, shall result in direct release of the active lock, independently of the access control system, in the direction of egress.

(2) *Automatic RTE and a Manual RTE Not on Door.* An automatic and a manual RTE device meeting all the following criteria shall be provided:
   (a) The automatic RTE device shall be provided on the egress side, arranged to detect an occupant approaching the portal, to release the active lock in the direction of egress upon detection of an approaching occupant.
   (b) The manual RTE device shall be provided to meet all the following criteria:
      i. The manual RTE device shall be provided on the egress side of the portal.
      ii. The manual RTE device shall be located 1015 mm to 1220 mm (40 in. to 48 in.) vertically above the floor and within 1525 mm (60 in.) of the portal.
      iii. The manual RTE device shall be readily accessible and clearly identified by a sign that reads: "PUSH TO EXIT."
      iv. The manual RTE device, when operated, shall result in direct release of the active lock, independently of the access control system, in the direction of egress.

6.1.5.7* The means of lock release required for egress portals by 6.1.5.6 shall not be required as follows:

(1) Where allowed by applicable codes
(2) Where approved by the AHJ

6.1.5.8 Wireless locking hardware communications shall not interfere with other wireless systems.

6.1.5.8.1 Wireless locking hardware shall conform to all industry standards for encryption.

6.1.5.8.2 Wireless locking hardware shall provide an alert of low battery in accordance with industry standards.

N **6.1.5.9 Locking Systems to Prevent Unwanted Entry.**

N **6.1.5.9.1** Locking systems to prevent unwanted entry shall comply with 6.1.5.9.2 through 6.1.5.9.6.

N **6.1.5.9.2** The locking system shall be capable of being engaged from the egress side without opening the door.

N **6.1.5.9.3** The unlocking and unlatching from the egress side shall be accomplished without the use of a key, tool, or special knowledge or effort.

N **6.1.5.9.4** The releasing mechanism for locking systems to prevent unwanted entry shall comply with all the following:
(1) The releasing mechanism shall open the door leaf with not more than one releasing operation.
(2) The manually actuated part of the releasing mechanism shall be located at a height not less than 0.86 m (34 in.) and not exceeding 1.21 m (48 in.) above the finished floor.
(3)* The door shall be capable of being unlocked or opened from outside the room with the necessary key or other credential.

N **6.1.5.9.5** The locking system shall not impedeor modify the door closer, panic hardware, or fire exit hardware.

N **6.1.5.9.6** The locking system shall be approved by the AHJ.

6.1.6 Position Sensor.

6.1.6.1* Where required, a position sensor shall monitor the position of the portal for held-open or forced-open conditions.

6.1.6.2 The position sensor shall be mounted such that no portion of the portal opening is greater than 152.4 mm (6 in.) before the sensor is activated.

6.1.6.3 Position sensors shall be monitored as applicable by the head-end controller or an integrated intrusion detection system so as to notify the system users of an event.

6.1.7* Portal Egress.

6.1.7.1 Free Egress.

6.1.7.1.1 Free egress, where a door position sensor is used, shall employ the use of an RTE device.

6.1.7.1.2* When the RTE controls the portal lock, the lock shall release on loss of power.

6.1.7.1.3 When activated, RTE devices shall prevent the position sensor, when used, from reporting a forced-open alarm.

6.1.7.1.4 The RTE shall be either manual or automatic.

6.1.7.1.4.1 Manual.

(A) The RTE device shall not require any special instruction or knowledge to use.

(B) If a manual RTE device is used as a fail-safe for an automatic RTE device, it shall be installed so as to directly release the locking mechanism.

6.1.7.1.4.2 Automatic.

(A) If the RTE device is a motion detector, it shall be listed for the purpose.

(B) Where automatic RTE devices are used to unlock portals, they shall be installed so that only intentional requests are executed.

6.1.7.2* Controlled Egress.

6.1.7.2.1 Controlled egress shall require the use of access credentials to be presented to a reader that is installed on the secured side of the portal, in accordance with 6.1.3.

6.1.7.2.2* Active locks used for controlled egress shall meet the requirements of 6.1.4.5.

6.1.8 Controllers.

6.1.8.1 A controller shall be listed for the purpose.

6.1.8.2 A controller shall be installed in accordance with the manufacturer's instructions.

6.1.8.3 A controller shall be installed in a space that protects it from damage, tampering, and access by unauthorized personnel.

6.1.9 Power Supplies.

6.1.9.1 Power supplies shall meet the requirements of Section 4.4.

6.1.9.2* Power supplies shall be sized based upon the application and the manufacturer's requirements.

6.1.9.3 The voltage and current of the power supply shall be the same as required by the associated field devices.

6.1.9.4 Power supplies shall be installed in a space that protects them from damage, tampering, and access by unauthorized personnel.

6.2 Administration Tools and Interface.

6.2.1* The configuration of the system operating parameters shall be in accordance with the facility requirements and subject to the approval of the AHJ.

6.2.2 System operating parameters shall be protected from unauthorized changes.

6.2.3 The operation of the electronic access control system shall be in compliance with the applicable fire and building codes.

6.2.4 The operation of the electronic access control system shall be in compliance with 4.1.3.

6.2.5 An electronic access control system shall be tested in accordance with Chapter 10.

6.3* Network Interface Device. In network interface device (NID) configurations, the level of encryption shall comply with the applicable level prescribed by the AHJ.

Chapter 7 Video Surveillance Systems

7.1 General.

7.1.1 This section shall apply to the installation requirements for closed circuit television (CCTV) systems and digital imaging systems.

7.1.2 The application and use of these systems shall be based on the requirements of the AHJ.

7.1.3 The installer shall ensure that the final image meets the design requirements.

7.1.4 The system shall be designed to allow for visual identification of a person, object, or scene. *(See Annex B.)*

7.1.5 Imaging Systems Security.

7.1.5.1 Control units, subcontrols, and devices that are used to interconnect the cameras to NIDs or CCTV control units shall be located within a secured area.

7.1.5.2 If the enclosures for such equipment are not located within a secured area, the enclosures shall be protected as determined by the security vulnerability assessment (SVA) or by one of the following methods:

(1) Continuously under the notice of assigned security personnel
(2) Located in an area that is accessible only to authorized personnel
(3) Supervised to annunciate tampering

7.1.6 Video surveillance systems shall comply with federal, state, and local privacy laws.

7.2 Cameras. Camera selection and location shall be based upon the requirements of the AHJ. *(See Annex C.)*

Δ **7.2.1** All cameras shall be listed in compliance with applicable standard(s), such as the following:

(1) UL 2044, *Standard for Commercial Closed-Circuit Television Equipment*
(2) UL 2802, *Standard for Performance Testing of Camera Image Quality*
(3) UL 60065, *Standard for Audio, Video and Similar Electronic Apparatus*

(4) UL 60950-1, *Standard for Information Technology Equipment*
(5) UL 62368, *Standard for Audio/Video, Information and Communication Technology Equipment*

7.2.2 All cameras shall be installed in accordance with the manufacturer's instructions.

7.2.3* The level of vandal resistance shall be determined by the SVA or the requirements of the AHJ.

7.2.4* In addition to the requirements of Chapter 4, cameras shall be installed to minimize the effect of the following environmental conditions:

(1)* Icing
(2)* Sunlight angles
(3)* Temperature extremes
(4)* Wind loading
(5)* Rain

7.2.5 Backlighting.

7.2.5.1* The camera field of view shall not have bright illumination behind the main subject.

7.2.5.2* When the backlighting conditions in 7.2.5.1 cannot be met or the scenes have extreme contrast, cameras and accessories having electronic compensation such as high dynamic range or backlight compensation shall be used.

7.2.6 Internet Protocol (IP) Cameras.

7.2.6.1 IP cameras shall, at minimum, meet IEEE standards for IP-based cameras.

7.2.6.2 IP cameras shall comply, at minimum, with the following:

(1) DHCP/Static IP addressing
(2) Username and password access to camera

7.3* Low-Level Lighting Conditions. Low-level lighting conditions of 10 lux [0.93 footcandle (fc)] or less within the field of view shall have special provisions to provide an image that meets the requirements of 7.1.3.

7.4* Enclosures. When enclosures are used, they shall be installed in accordance with the manufacturer's instructions.

7.4.1 Physical Dimensions. The enclosure shall be sized based on the dimensions of the camera/lens package and any other required equipment, such as connectors, other electronic devices, or transformers.

Δ **7.4.2 Listed.** Camera enclosures and equipment shall be in compliance with applicable standards, such as the following:

(1) UL 50, *Standard for Enclosures for Electrical Equipment, Non-Environmental Considerations*
(2) UL 50E, *Standard for Enclosures for Electrical Equipment, Environmental Considerations*
(3) UL 2044, *Standard for Commercial Closed-Circuit Television Equipment*
(4) UL 60065, *Standard for Audio, Video and Similar Electronic Apparatus*
(5) UL 60950-1, *Standard for Information Technology Equipment*
(6) UL 60950-22, *Standard for Information Technology Equipment — Equipment to Be Installed Outdoors*

7.4.3 Tamper Resistance for Enclosures. The level of tamper resistance shall be determined by a security vulnerability assessment or the requirements of the AHJ.

Δ **7.5* General Hardware and Mounts.** Mounting brackets shall be in compliance with applicable standards, such as UL 2044, *Standard for Commercial Closed-Circuit Television Equipment.*

7.5.1 Anchoring.

7.5.1.1 Anchoring shall be rated for the load and mounting surface.

7.5.1.2* All anchoring sets shall be installed in accordance with manufacturers' instructions.

7.5.1.3 Manufacturers' torque specifications shall be adhered to as applicable.

7.5.1.4 All manufacturers' torque specifications shall be adhered to as applicable and be appropriate for the surface to which the anchoring sets are mounted.

7.5.2 Mounts. Mounts shall be rated for the weight, external weight (e.g., snow or rain), twist, and wind loading of the equipment used.

7.5.3 Mounting Bolts. Mounting bolts and hardware shall be tightened in accordance with 7.5.1.4.

7.5.4* Tamper Resistance for General Hardware and Mounts. The level of tamper resistance shall be determined by an SVA or the requirements of the AHJ.

7.6 Lens. Lenses shall be selected to provide the field of view and image size as required in 7.1.3.

7.7* Physical Conductors.

7.7.1* All cabling and wiring used for the connection of video surveillance equipment shall be installed in accordance with the requirements of 4.6.3.

7.7.2* Cable Jacket Specifications. All cables shall have jackets appropriate for the installed environment.

7.7.3 Compatibility. All interconnecting cable shall be compatible with the video surveillance system equipment and be installed according to the equipment manufacturer's instructions and 4.6.3.

7.7.4* Connections.

7.7.4.1 The installer of the video surveillance system shall possess and understand the tools necessary to ensure that cable preparation and connections are installed in a workmanlike manner.

7.7.4.2 Twist-on connectors shall not be used.

7.7.5* Applications of Conductors and Wiring.

7.7.5.1* Control Wiring. All control wiring shall be sized to deliver the manufacturer's optimum operating voltage from the power supply or controller to the device being driven.

7.7.5.2 Power Cabling. The minimum size of power conductors shall be in accordance with *NFPA 70*.

7.7.5.3 Video Signal Transmission Wiring. Wiring used for video signal transmission shall not exceed the distance limitations in the video equipment manufacturer's instructions.

7.8 Radio Frequency (RF). (Reserved)

7.9 Camera Imaging.

7.9.1 Resolution shall be, at minimum, a native resolution of 640 × 480.

7.9.2 Compression shall be, at minimum, H.264.

7.10 Network Video Recorder (NVR). NVRs shall be installed in a secure location.

Chapter 8 Holdup, Duress, and Ambush Systems

8.1 General.

8.1.1 Construction.

Δ **8.1.1.1** The construction of holdup alarm initiating devices shall be in compliance with applicable standards, such as UL 636, *Standard for Holdup Alarm Units and Systems.*

Δ **8.1.1.2** The construction of private duress alarm initiating devices shall be in compliance with applicable standards, such as UL 636, *Standard for Holdup Alarm Units and Systems.*

8.1.2 Installation.

8.1.2.1 Systems that utilize wiring or low-powered radio frequency to connect initiating, annunciating, and remote control devices shall comply with Chapter 4.

8.1.2.2 The means of interconnecting wiring connections between initiating signaling devices and control units shall be supervised so that the occurrence of a single open in the installation wiring and its restoration to normal operation is indicated within 200 seconds.

8.1.2.3 Initiating devices shall be located in such a manner to prevent unintentional operation by employees, janitors, cleaners, and others with access to the equipment.

8.1.2.4 Initiating devices shall be mounted in such a manner to prevent unintentional operation by jarring, vibration, falling objects, and similar causes.

8.1.2.5* Portable initiating devices shall require positive, intentional action to initiate an alarm signal, in accordance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* Section 4.4.2.

8.2 Holdup Alarm Systems.

8.2.1 Installation.

8.2.1.1 The installation of holdup devices shall be in accordance with the manufacturer's instructions.

8.2.1.2 Fixed-in-place holdup alarm initiating devices shall be mounted at a height that is accessible from the work position of the individuals responsible for utilizing the device.

8.2.2 Operation.

Δ **8.2.2.1** A holdup alarm initiating device shall either lock into the alarm position or display a visual indication when it is operated.

8.2.2.2 Visual displays of the operation of a holdup device shall be permitted at the device, at the control unit to which it is connected, or at the location where the holdup alarm signal is received.

8.2.2.3 Visual indication of the operation of a holdup device shall require a manual operation to reset it.

8.2.2.4 Each holdup alarm initiating device shall require positive, intentional action to initiate a holdup alarm signal.

8.2.2.5 Operation of a holdup alarm initiating device shall not result in an audible signal at the protected premises or a visual signal that is visible to an attacking party.

8.2.2.6 Each holdup alarm initiating device shall be located so that it cannot be observed by the public.

8.2.2.7 The operation of a holdup alarm initiating device shall not be obvious to an attacking party.

8.2.2.8* Each employee expected to use a holdup alarm initiating device shall be instructed in the operation of the device.

8.2.2.9* A holdup alarm signal shall be transmitted to a monitoring station.

8.3 Duress Alarm Systems.

8.3.1 Installations. Portable duress alarm initiating devices shall be in compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* Section 4.2.4.

8.3.2 Operation.

Δ **8.3.2.1** A duress alarm initiating device shall either lock into the alarm position or display a visual indication when it is operated.

8.3.2.2 Visual displays of the operation of a duress device shall be permitted at the device, at the control unit to which it is connected, or at the location where the duress alarm signal is received.

8.3.2.3 Visual indication of the operation of a duress device shall require a manual operation to reset it.

8.3.2.4 Each duress alarm initiating device shall require positive, intentional action to initiate a duress alarm signal.

8.3.2.5* Operation of a duress alarm initiating device shall result in an audible signal or a visual signal at the location of the initiating device or at a staffed location elsewhere on the protected property.

8.3.2.5.1 In addition to the staffed location required in 8.3.2.5, a duress alarm signal shall be received at a constantly attended location at the protected premises or transmitted to a monitoring station.

8.3.2.6 Private Duress Alarm Systems.

8.3.2.6.1 Fixed-in-place duress alarm initiating devices shall be installed within 1.22 m (4 ft) of the workstation and accessible from the normal work position of the individuals responsible for utilizing the device.

8.3.2.6.2 Each private duress alarm initiating device shall be located so that it cannot be observed by the public.

8.3.2.6.3 The activation of a private duress alarm initiating device shall not be obvious to a hostile party.

8.3.2.6.4 Each person expected to use a private duress alarm initiating device shall be instructed in the operation of the device.

8.3.2.7 Public Duress Alarm Systems.

8.3.2.7.1 Each public duress alarm initiating device shall be located so that it is visible to the public.

8.3.2.7.2 Each public duress alarm initiating device shall be capable of being operated by the public.

8.3.2.7.3 Instructions for the operation of each alarm initiating device shall be clearly visible to a user of the device.

8.3.2.7.4 If there is no constantly attended location at the protected premises, the duress alarm signal shall be transmitted to a monitoring station.

8.4 Ambush Alarm Systems.

8.4.1 Installation. Ambush alarm initiating devices shall be located in or adjacent to the mechanism that is used to disarm the intrusion detection system.

8.4.2 Operation.

8.4.2.1* The initiation of an ambush signal shall be accomplished by entering a code sequence that is not similar to any code sequence that is used to perform any other operation in access control, intrusion detection, and holdup or duress systems.

8.4.2.1.1 Alarms that are manually initiated at an arming station shall require a double-action trigger.

8.4.2.2 Operation of an ambush alarm initiating device shall not result in an audible signal at the protected premises or a visual signal that is visible to an attacking party.

8.4.2.3 The operation of an ambush alarm initiating device shall not be obvious to an attacking party.

8.4.2.4* Each person expected to use an ambush alarm initiating device shall be instructed in the operation of the device.

8.4.2.5* An ambush alarm signal shall be transmitted to a monitoring station.

Chapter 9 Monitoring Stations

Δ **9.1 Application.** The performance and operation of monitoring stations that monitor premises security systems shall comply with the requirements of this chapter.

9.1.1 The requirements of Chapter 4 and Chapter 10 shall apply unless they are in conflict with this chapter.

9.2 Scope. This chapter shall cover the following:

(1) Public safety agencies monitoring stations
(2) Proprietary monitoring stations
(3) Commercial monitoring stations

9.2.1* Where a system is monitored, signals to be transmitted shall be known to both the property owner and the facility that receives the signal.

9.2.2 The actions that are to be taken by the monitoring station upon receipt of a signal shall be agreed upon by both the property owner and the monitoring station.

9.3 Public Safety Agencies.

9.3.1* This section shall be used for the facility requirements and operational survivability of alarm processing equipment and automation equipment and the receiving and processing of signals.

9.3.2 Building Construction.

9.3.2.1 Building construction requirements shall be governed by local and state building codes.

9.3.2.2 The operations room shall have a minimum fire-resistive construction rating of 1 hour.

9.3.2.3 Emergency lighting shall be provided for the operations room and those areas critical to maintaining overall operations.

9.3.3 Fire Protection.

9.3.3.1 The fire protection requirements shall be governed by local and state fire codes.

9.3.3.2 When a water-based fire suppression system is installed within the operations room, the equipment essential for monitoring shall be located so that the effects of water damage are minimized.

9.3.3.3 The operations room shall be provided with an automatic fire detection system installed in accordance with *NFPA 72*.

9.3.3.3.1 Signals from the fire alarm system shall be transmitted to a separate approved fire supervising station.

9.3.3.4 The operations room shall be provided with a minimum of two fire extinguishers that are in compliance with NFPA 10.

9.3.3.4.1 One extinguisher shall be located next to the monitoring equipment.

9.3.3.4.2 One extinguisher shall be located next to the main entry door.

9.3.4 Security.

9.3.4.1 Doors.

9.3.4.1.1 All doors that lead into the operations room and alarm equipment rooms shall be secured to prevent access by unauthorized personnel.

9.3.4.1.2 Any compromise of the doors shall be annunciated at a location within the facility that is constantly attended.

9.3.4.2 Key access shall be controlled by a designated security officer of the facility.

9.3.4.3 Access Control.

9.3.4.3.1 Access to operation rooms shall be restricted to authorized personnel.

9.3.4.3.2 All alarm equipment rooms shall be secured.

9.3.4.3.3 A process shall exist that records all persons entering the room.

9.3.4.3.4 Records shall be kept for 12 consecutive months.

9.3.4.3.5 All unauthorized entries shall be annunciated in the operations room.

9.3.4.4* Detection devices shall be installed to ensure that anyone approaching within 15.24 m (50 ft) of the facility is annunciated in the operations room.

Exception: Annunciation shall not be required for anyone approaching the main entrance via a public access point.

9.3.4.5 Lighting shall be provided for the perimeter security zone.

9.3.5 Standby Power.

9.3.5.1* The operations room, including alarm receiving and processing equipment, shall have emergency standby power satisfying the electrical requirements to maintain operations without a loss of signals during a primary power failure.

9.3.5.1.1* A minimum level 2, class 24, type 60 emergency power supply system (EPSS) shall be installed and maintained in accordance with NFPA 110.

9.3.5.1.2 A level 2, class 1.5, type O stored emergency power supply system shall be installed and maintained in accordance with NFPA 111.

9.3.5.1.3 The stored EPSS in 9.3.5.1.2 shall be sized to supply the required load for 4 hours.

9.3.5.1.4* Access to the standby power supply shall be controlled by the monitoring station to prevent access by unauthorized personnel.

9.3.6 Personnel.

9.3.6.1 A minimum of two operators shall be on the premises and on duty at all times.

9.3.6.2 At least one operator shall be in the operations room.

9.3.6.3* The operators shall be trained in the operation of the signal receiving equipment, automation equipment, and procedures.

9.3.7 Disposition of signals shall be in accordance with Section 9.6.

9.3.8 Record keeping shall be in accordance with Section 9.8.

9.3.9 Alarm Receiving and Signal Processing Equipment.

9.3.9.1 Signal Recording.

9.3.9.1.1 All alarm receivers shall be provided with an internal printer, external printer, or other method for recording all incoming signals.

9.3.9.1.2 All signals shall be date and time stamped upon receipt of the signal.

9.3.9.1.3 Clocks shall be synchronized with local time daily to ensure time stamp accuracy.

9.3.9.2 Maintenance and Servicing of Alarm Receiving and Signal Processing Equipment.

9.3.9.2.1* An emergency contact list shall be readily accessible and include the following:

(1) Receiving equipment service companies
(2) Communication providers
(3) Automation support services
(4) Power system service providers
(5) Utility providers
(6) Other critical service providers

9.3.9.2.2 Records of all maintenance and service shall be recorded in the maintenance log.

9.3.9.3 Operating Requirements.

9.3.9.3.1 Equipment shall be installed in compliance with the manufacturer's instructions.

9.3.9.3.2* Equipment shall be in compliance with FCC rules and regulations.

9.3.9.3.3 Surge protection shall be provided on all equipment that is sensitive to transient surges on primary power supply lines.

9.3.9.3.4 Surge protection shall be provided on all equipment that is sensitive to transient surges on communication circuits in accordance with *NFPA 70*.

9.3.9.3.5 All wiring to alarm receivers shall be in conformance with *NFPA 70*.

9.3.9.3.6 All signals shall be displayed and recorded in accordance with 9.7.10.

9.3.9.4* Alarm receiving equipment shall be in accordance with Section 9.7.

9.4 Proprietary Monitoring Stations.

Δ **9.4.1** Proprietary monitoring stations shall be physically configured and maintained in conformance with UL 1076, *Standard for Proprietary Burglar Alarm Units and Systems*, Clause "Proprietary Burglar Alarm Service."

9.4.2 Disposition of signals shall be in accordance with Section 9.6.

9.4.3 Surge protection shall be provided on all equipment that is sensitive to transient surges on primary power supply lines.

9.4.4 Surge protection shall be provided on all equipment that is sensitive to transient surges on communication circuits in accordance with *NFPA 70*.

9.4.5 All wiring to alarm receivers shall be in conformance with *NFPA 70*.

9.4.6 All signals shall be recorded and displayed in accordance with 9.7.10.

9.4.7 Alarm receiving equipment shall be in accordance with Section 9.7.

9.5 Central Monitoring Stations.

Δ **9.5.1** The monitoring station building or that portion of a building occupied by a monitoring station shall conform to the requirements of UL 827, *Standard for Central-Station Alarm Services*, clause "Facilities and Equipment."

9.5.2 Disposition of signals shall be in accordance with Section 9.6.

9.5.3 Surge protection shall be provided on all equipment that is sensitive to transient surges on primary power supply lines.

9.5.4 Surge protection shall be provided on all equipment that is sensitive to transient surges on communication circuits in accordance with *NFPA 70*.

9.5.5 All wiring to alarm receivers shall be in conformance with *NFPA 70*.

9.5.6 All signals shall be recorded and displayed in accordance with 9.7.10.

9.5.7 Alarm receiving equipment shall be in accordance with Section 9.7.

9.6 Disposition of Signals.

9.6.1 Notification of a public response agency shall not occur prior to enhanced verification of an alarm signal.

9.6.1.1 Methods of enhanced verification shall be one of the following or as approved by the public safety agency having jurisdiction at the protected premises:

(1) Enhanced call verification (ECV)
(2) Remote video verification (RVV)
(3) Remote audio verification (RAV)
(4)* Multiple trip verification (MTV)

9.6.1.1.1 Enhanced Call Verification (ECV).

9.6.1.1.1.1 ECV shall be the attempt by monitoring station personnel to verify whether an emergency exists at the protected premises.

9.6.1.1.1.2* At a minimum, the ECV procedure shall consist of at least two phone calls made after receipt of an alarm signal, the first of which is to the protected premises.

9.6.1.1.1.3 The maximum time for the first call to be made as required by 9.6.1.1.1.2 shall not exceed 60 seconds from the operator's receipt of the alarm.

9.6.1.1.1.4 The total time for the ECV procedure shall not exceed a reasonable time from the operator's receipt of the alarm.

9.6.1.1.1.5 Non–alarm monitoring activity shall not take priority over the ECV process.

Δ **9.6.1.1.1.6** If no contact to an authorized representative of the protected premises is made by the end of the time period as specified by 9.6.1.1.1.4, a notification to the public safety agency shall be made.

9.6.1.1.2* Remote Video Verification (RVV).

9.6.1.1.2.1 Cameras used for RVV shall be installed in accordance with Chapter 7.

9.6.1.1.2.2 The RVV procedure shall occur concurrently with an ECV in accordance with 9.6.1.1.1.

Δ **9.6.1.1.2.3** When through the use of RVV it is apparent that an unauthorized intrusion at the protected premises is occurring, an immediate notification to the public safety agency shall be made.

9.6.1.1.3* Remote Audio Verification (RAV).

9.6.1.1.3.1 Devices used for RAV shall be installed in accordance with the manufacturer's instructions.

9.6.1.1.3.2 The RAV procedure shall occur concurrently with an ECV in accordance with 9.6.1.1.1.

9.6.1.1.3.3 If two-way communication has been established through the use of RAV, the phone call to the protected premises requirement of ECV shall not be required.

Δ **9.6.1.1.3.4** When through the use of RAV it is apparent that an unauthorized intrusion at the protected premises is occurring, an immediate notification to the public safety agency shall be made.

9.6.1.1.4 Multiple Trip Verification (MTV). When MTV is provided by the cross-zoning of two sensors within a detection zone, the requirements of ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction,* shall be used.

9.6.2 Verified False. If the specific alarm has been verified as being false, monitoring station personnel shall not perform a notification to the public safety agency.

9.6.3 Holdup Alarm.

9.6.3.1* Upon actuation of a holdup alarm, the monitoring station shall immediately notify the public safety agency unless otherwise directed by special instructions.

9.6.3.2 The monitoring station shall not call the protected premises.

9.6.3.3 Alternative special instructions shall be allowed to supersede the requirements of 9.6.3.2.

9.6.4 Duress Alarm.

9.6.4.1 Private Duress Alarm.

9.6.4.1.1 Upon actuation of a private duress alarm, the monitoring station shall call the protected premises before notifying the public safety agency unless otherwise directed by special instructions.

9.6.4.1.2 If the call required in 9.6.4.1.1 is answered, the monitoring station personnel shall identify themselves and ask for a name and identification credential.

9.6.4.1.3 Monitoring station personnel shall notify the public safety agency if any one of the following occurs:

(1) The person at the protected premises does not give a valid identification credential.
(2) The call to the protected premises is not answered within six rings.
(3) The call is forwarded.
(4) The call results in a busy signal.

9.6.4.2 Public Duress Alarm.

9.6.4.2.1* Upon actuation of a public duress alarm, the monitoring station shall immediately notify the public safety agency unless otherwise directed by special instructions.

9.6.4.2.2 The notification in 9.6.4.2.1 shall not be required if the alarm signal is determined to be false by the use of enhanced verification in accordance with 9.6.1.1(1).

9.6.5 Ambush Alarm.

9.6.5.1* Upon actuation of an ambush alarm, the monitoring station shall immediately notify the public safety agency unless otherwise directed by special instructions.

9.6.5.2 The monitoring station shall not call the protected premises.

9.6.5.3 Alternative special instructions shall be allowed to supersede the requirements of 9.6.5.2.

9.6.6* Premises Hazards Information. If provided by the party responsible for the protected premises, information about facility hazards shall be retained and be accessible to monitoring station personnel to notify public safety agencies.

9.7 Transmission and Receiving Technologies.

9.7.1 Listed Equipment.

9.7.1.1 Transmission and receiving equipment that is constructed and installed in compliance with this standard shall be listed for the purpose for which it is used in accordance with applicable standards.

9.7.1.2 Transmission and receiving equipment shall be installed in accordance with the manufacturer's published installation instructions.

9.7.2* Transmission Verification.

9.7.2.1 The equipment providing off-premises signaling shall automatically initiate and complete a test signal transmission sequence to its associated receiver at least once every 7 days.

9.7.2.2 A successful signal transmission sequence of any other type within the same 7-day period shall fulfill the requirement to verify the integrity of the reporting system, provided signal processing is automated so that 7-day delinquencies are reported and reviewed by monitoring station personnel.

9.7.3 Change of Service.

9.7.3.1 The premises security system provider shall notify its customers or clients of any change in service that results in signals from their property being handled by a different monitoring company.

9.7.4 Federal Communications Commission (FCC). Electronic intrusion detection system equipment and installations shall comply with FCC rules and regulations, as applicable, concerning electromagnetic radiation, use of radio frequencies, and connections to a public telephone network of telephone equipment, systems, and protection apparatus.

9.7.5 *National Electrical Code*. Equipment shall be installed in compliance with *NFPA 70*.

9.7.6 Two-Way Communication. Two-way communications technology shall apply to systems in which both the protected premises and the monitoring station transmit signals.

9.7.6.1 Communications Integrity. Provision shall be made to monitor the integrity of the transmission technology and its communications path, and the following requirements shall apply:

(1) Any failure shall be annunciated at the monitoring station.
(2) If communications cannot be established with the monitoring station, an indication of this failure to communicate shall be annunciated at the protected premises.
(3) System units at the monitoring station shall be restored to service within 30 minutes of a failure.
(4)* The transmission technology shall be designed so that upon failure of a transmission channel serving a system unit at the monitoring station, the loss of the ability to monitor shall not affect more than 3000 transmitters.

9.7.6.2* Spare System Unit Equipment. The monitoring station shall maintain spare unit equipment so that full operation is restored within 1 hour.

9.7.7 One-Way Communication. One-way communications technology shall apply to systems where only the protected premise transmits signals.

9.7.7.1 Communications Integrity. Provision shall be made to monitor the integrity of the transmission technology and its communications path, and the following requirements shall apply:

(1) If communications cannot be established with the monitoring station, an indication of this failure to communicate shall be annunciated at the protected premises.
(2) System units at the monitoring station shall be restored to service within 30 seconds of a failure.
(3)* The transmission technology shall be designed so that upon failure of a transmission channel serving a system unit at the monitoring station, the loss of the ability to monitor shall not affect more than 3000 transmitters.

9.7.7.2 Spare System Unit Equipment. Spare receivers shall be provided in the monitoring station.

9.7.7.2.1 The spare receiver shall be online or able to be switched into the place of a failed unit within 30 seconds after detection of failure.

9.7.7.2.2 One spare receiver shall be provided as a backup for a maximum of five operating units.

9.7.7.2.3 A spare receiver shall have the same or greater capacity of any receiver that it is to replace.

9.7.8 Loading Capacity of a System Unit. If duplicate spare system units are maintained at the monitoring station and switchover is achieved in 30 seconds, then the system capacity shall be unlimited.

9.7.9 Unique Identifier. If a transmitter shares a transmission or communications channel with other transmitters, it shall have a unique transmitter identifier.

9.7.10 Recording and Display Rate of Subsequent Signals. Recording and display of signals at the monitoring station shall be at a rate no slower than one complete signal every 10 seconds.

9.7.11 Signal Error Detection and Correction.

9.7.11.1 Transmission of alarm, supervisory, and trouble signals shall be in a highly reliable manner to prevent degradation of the signal in transit, which in turn would result in either of the following:

(1) Failure of the signal to be displayed and recorded at the monitoring station
(2) An incorrect corrupted signal displayed and recorded at the monitoring station

9.7.11.2 Reliability of the signal shall be achieved by any of the following:

(1) Signal repetition — multiple transmissions repeating the same signal
(2) Parity check — a mathematical check sum algorithm of a digital message that verifies correlation between transmitted and received messages
(3) An equivalent means to 9.7.11.2(1) or 9.7.11.2(2) that provides a certainty of 99.99 percent that the received message is identical to the transmitted message

9.7.12 Unique Flaws Not Covered by This Standard. If a communications technology has a unique flaw that results in the failure to communicate a signal, the implementation of that technology for electronic intrusion signaling shall

compensate for that flaw so as to eliminate the risk of a signal being missed.

9.7.13 Display and Recording Requirements for All Transmission Technologies.

9.7.13.1 Manual System. Any method of recording and display or indication of change of status signals shall be permitted provided all of the following conditions are met:

(1) Each change of status signal requiring action to be taken by the operator shall result in an audible signal and in a visual display that identifies the type of signal, the condition, and an account identifier.
(2) Each change of status signal shall be automatically recorded and provide the type of signal, condition, and an account identifier, in addition to the time and date the signal was received.
(3) Failure of an operator to acknowledge or act upon a change of status signal shall not prevent subsequent alarm signals from being received, indicated or displayed, and recorded.
(4) Change of status signals requiring action to be taken by the operator shall be displayed or indicated in a manner that clearly differentiates them from those that have been and acknowledged and acted upon.
(5) Each incoming signal to a receiver shall cause an audible signal that persists until manually acknowledged.

Δ **9.7.13.2 Automated System.** Any method of recording and display or indication of change of status signals shall be permitted provided all of the following conditions are met:

(1) Each change of status signal requiring action to be taken by the operator shall result in an audible signal and in a visual display that identifies the type of signal, the condition, and an account identifier.

Exception: Enabling the audible signal shall not be required in monitoring stations where operators are dedicated to handling change of status signals and are stationed within sight of the visual display.

(2) Each change of status signal shall be automatically recorded and provide the type of signal, condition, and an account identifier, in addition to the time and date the signal was received.
(3) Failure of an operator to acknowledge or act upon a change of status signal shall not prevent subsequent alarm signals from being received, indicated or displayed, and recorded.
(4) Change of status signals requiring action to be taken by the operator shall be displayed or indicated in a manner that clearly differentiates them from those that have been acknowledged and acted upon.

9.8* Record Keeping and Recording. Complete records of all signals received shall be retained for at least 12 consecutive months.

9.9 Testing and Maintenance Requirements for All Transmission Technologies. Testing and maintenance of communications methods shall be in accordance with the requirements of Chapter 10.

Chapter 10 Testing and Inspections

Δ **10.1* Application.** The inspection, testing, and maintenance of premises security systems shall comply with the requirements in this chapter.

10.1.1 This chapter shall apply to those systems installed under the provisions of this standard.

Δ **10.1.2*** Inspection, testing, and maintenance programs shall do the following:

(1) Satisfy the requirements of this standard
(2) Conform to the equipment manufacturer's recommendations
(3) Verify correct operation of the premises security systems

10.1.3* The system user, the premises security system provider for the protected premises, or the owner's designated representative shall be responsible for the inspection, testing, and maintenance of the systems and alterations of the systems.

10.1.4 Inspection, testing, or maintenance shall be permitted to be performed by a person or organization other than the owner if conducted under a written contract.

10.1.4.1 When the responsibility for the activities outlined in 10.1.3 is delegated to a third party, it shall be in writing with proof of such delegation provided to the AHJ upon request.

10.1.5 Inspection, testing, and maintenance procedures that are required by other parties and that exceed the requirements of this chapter shall be permitted.

10.2 Impairments.

10.2.1* System defects and malfunctions shall be corrected.

10.2.1.1* The repair shall begin within 24 hours of the indication that repair is required unless the system user or party responsible for the protected premises agrees to a delay.

Δ **10.2.1.2*** If the premises security system at the protected premises is impaired for more than 24 hours from the time of the defect or malfunction is identified, the owner or the designated party responsible for the protected premises shall be notified.

10.2.2* When it is determined that there is not a risk to the protected property or the occupant, repair to the system shall be permitted to begin outside the time required by 10.2.1.1 if the owner or responsible party is notified.

10.2.3 If a defect or malfunction is not corrected at the conclusion of system inspection, testing, or maintenance, written notice shall be provided to the party responsible for the protected premises within 24 hours.

10.2.4 A record shall be maintained by the system user or party responsible for the protected premises for a period of 1 year from the date the impairment is corrected.

10.2.5* Impairments that are outside the control of the monitoring station, the system user, or the party responsible for the protected premises shall not be subject to the requirements of 10.2.1.1.

10.3 General Testing, Inspection, and Maintenance.

10.3.1 Nothing in Chapter 10 shall be intended to prevent the use of alternative test methods or testing devices.

10.3.2 Alternative test methods or testing devices shall provide the same level of effectiveness and safety.

10.3.3 Alternative test methods shall meet the intent of the requirements of Chapter 10.

10.3.4 Service Personnel.

Δ **10.3.4.1*** Service personnel shall be qualified in the inspection, testing, and maintenance of premises security systems, including the mechanical components incorporated into the premises security systems.

Δ **10.3.4.2** Examples of qualified personnel shall be permitted to include, but not be limited to, individuals with one or more of the following qualifications:

(1)* Personnel trained and certified by the equipment manufacturer
(2) Personnel licensed or certified by a federal, state, or local authority
(3) Personnel certified by an accreditation program or industry-recognized program acceptable to the AHJ
(4) Trained and qualified personnel experienced in the servicing of premises security systems and employed by an organization listed by an approved testing laboratory

10.3.5 Notification.

10.3.5.1* Before proceeding with any testing, repairs, or maintenance, the system user, parties responsible for the protected premises, and facilities receiving alarm supervisory or trouble signals shall be notified of the testing or maintenance to prevent unnecessary response.

10.3.5.2 The system user or the party responsible for the protected premises and service personnel shall coordinate system testing to prevent interruption of critical facility systems or equipment.

10.3.6 Prior to system maintenance or testing, the information regarding the system and system alterations, including record of completion, owner's manual, and installation instructions, shall be provided by the party responsible for the protected premises to the service personnel upon request.

10.4 System Testing.

10.4.1 Acceptance Testing. All new systems shall be inspected and tested in accordance with the requirements of 10.4.3.

Δ **10.4.2 Re-acceptance Testing.**

10.4.2.1 Re-acceptance testing shall be performed after any of the following:

(1) Added or deleted system components
(2) Any modification, repair, or adjustment to system hardware or wiring
(3) Any modifications to the structure being protected

10.4.2.2* All components, circuits, systems operations, and site-specific software functions known to be affected by the change or identified by a means that indicates the changes shall be tested.

10.4.2.3 A revised record of completion in accordance with 4.12.2 shall be prepared to reflect any changes to the original and subsequent inspections attached as addenda to this current document.

Δ **10.4.3 Test Methods.** Premises security systems and other systems and equipment that are associated with security systems and accessory equipment shall be tested according to Table 10.4.3(a), Table 10.4.3(b), and Table 10.4.3(c).

10.4.3.1 Asset protection systems and accessory equipment shall be tested according to Table 10.4.3(c).

10.5* Inspection and Testing Frequency.

10.5.1 The inspection and testing frequency shall be performed in accordance with the security vulnerability assessment for the protected premises.

10.5.2 The inspection and testing frequency shall be performed in accordance with the manufacturer's published instructions for the devices and appliances that are used.

Δ **10.5.3** As an alternative means of compliance with 10.5.1 or 10.5.2, subject to the approval of the AHJ, premises security systems shall be permitted to be inspected, tested, and maintained under a written performance-based program.

Δ **10.5.3.1** Goals established under a performance-based program shall provide assurance that the premises security systems will perform its intended functions.

10.5.3.2 Technical justification for the inspection, testing, and maintenance intervals shall be documented.

10.5.3.3 The performance-based option shall include historical data.

10.5.3.4 Documentation of performance-based testing shall be in accordance with Section 10.7.

N **10.6 Maintenance.**

N **10.6.1*** Any device or system shall be maintained to function as designed.

N **10.6.2** All levels of protection shall be maintained as designed.

N **10.6.3** A record shall list repairs, including but not limited to the following:

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

N **10.6.4** Repair records shall be retained for not less than 1 year.

10.7 Records.

10.7.1 Permanent Records. The system user or party responsible for the protected premises shall be responsible for maintaining the records required in 4.12.2 for the life of the system for examination by any authority having jurisdiction.

10.7.1.1 The records shall be on a medium that will survive the retention period.

10.7.2 Maintenance, Inspection, and Testing Records.

10.7.2.1 Records shall be retained until the next test and for 12 consecutive months thereafter.

10.7.2.2 Paper or electronic media shall be permitted.

Δ Table 10.4.3(a) Test Methods

Devices	Test Methods
Control equipment	
(1) Function	Verify correct receipt of alarm, supervisory, and trouble signals (inputs); operation of evacuation signals and auxiliary functions (outputs); circuit supervision, including detection of open circuits and ground faults; and power supply supervision for detection of loss of ac power and disconnection of secondary batteries.
(2) Fuses	Verify rating and supervision for field-removable fuses that are not integral to the control equipment.
(3) Interfaced equipment	Verify integrity of circuits providing interface between two or more control units. Test interfaced equipment connections by operating or simulating operation of the equipment being supervised. Verify signals required to be transmitted at the control unit.
(4) Lamps and LEDs	Illuminate lamps and LEDs.
(5) Primary (main) power supply	Test under maximum load, including all alarm appliances requiring simultaneous operation. Test redundant power supplies separately.
Engine-driven generator	If an engine-driven generator dedicated to the system is used as a required power source, verify operation of the generator in accordance with NFPA 110.
Secondary (standby) power source	Disconnect all primary (main) power supplies and verify the occurrence of required trouble indication for loss of primary power. Measure or verify the system's standby and alarm current demand and verify the ability of batteries to meet standby and alarm requirements using manufacturer's data. Operate general alarm systems a minimum of 5 minutes and sounders for a minimum of 15 minutes. Reconnect primary (main) power supply at end of test.
Uninterruptible power supply (UPS)	If a UPS system dedicated to the system is used as a required power source, verify operation of the UPS system in accordance with NFPA 111.
Batteries — general tests	Prior to conducting any battery testing, verify that all system software stored in volatile memory is protected from loss.
(1) Visual inspection	Inspect batteries for corrosion or leakage along with the tightness of connections. Clean the batteries if necessary and confirm the connections are tight and the levels of electrolyte are as specified by the manufacturer.
(2) Battery replacement	Replace batteries in accordance with the recommendations of the alarm equipment manufacturer or when the recharged battery voltage or current falls below the manufacturer's recommendations.
(3) Charger test	With the batteries fully charged and connected to the charger, place an ampere meter in series with the battery under charge. Verify the charging current is in accordance with the manufacturer's recommendations for the type of battery used. In the absence of specific information, use $\frac{1}{30}$ to $\frac{1}{25}$ of the battery rating.
(4) Discharge test	With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery.
(5) Load voltage test	With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the float voltage for the entire battery is 1.42 volts per cell, nominal, under load. If possible, measure cells individually. An artificial load equal to the full premises security system is permitted to be used in conducting this test.
Battery tests (specific types)	
(1) Lead-acid type	With the batteries fully charged and connected to the charger, measure the voltage across the batteries with a voltmeter. Verify the voltage is 2.30 volts per cell ± 0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the battery does not fall below 2.05 volts per cell under load. Measure as required the specific gravity of the liquid in the pilot cell or all of the cells. Verify the specific gravity is within the range specified by the manufacturer. Although the specified specific gravity varies from manufacturer to manufacturer, a range of 1.205–1.220 is typical for regular lead-acid batteries, while 1.240–1.260 is typical for high-performance batteries. Do not use a hydrometer that shows only a pass or fail condition of the battery and does not indicate the specific gravity; such a reading does not give a true indication of the battery condition.
(2) Nickel-cadmium type	With the batteries fully charged and connected to the charger, place an ampere meter in series with the battery under charge. Verify the charging current is in accordance with the manufacturer's recommendations for the type of battery used. In the absence of specific information, use $\frac{1}{30}$ to $\frac{1}{25}$ of the battery rating.

(continues)

Δ Table 10.4.3(a) ***Continued***

Devices	Test Methods
(3) Sealed lead-acid type	With the battery charger disconnected, load test the batteries following the manufacturer's recommendations. Verify the voltage level does not fall below the levels specified. Load testing can be by means of an artificial load equal to the full connected load to the battery. Verify the float voltage for the entire battery is 1.42 volts per cell, nominal, under load. If possible, measure cells individually. With the batteries fully charged and connected to the charger, measure the voltage across the batteries with a voltmeter. Verify the voltage is 2.30 volts per cell ± 0.02 volts at 25°C (77°F) or as specified by the equipment manufacturer. Verify the battery performs under load, in accordance with the battery manufacturer's specifications.
Transient voltage surge suppression	Lightning protection equipment is to be inspected and maintained per the manufacturer's specifications. Additional inspections are required after any lightning strikes.
Sound and visual devices	
(1) Audible	Test in accordance with the manufacturer's published instructions.
(2) Visible	Test in accordance with the manufacturer's instructions.
Transmitting equipment	Verify receipt of the correct initiating device signal at the monitoring station.
Interface equipment	Verify integrity of single or multiple circuits providing interface between two or more control units. Test interfaced equipment connections by operating or simulating operation of the equipment being supervised. Verify signals required to be transmitted at the control unit.
Low-powered radio (wireless systems)	(1) Use the manufacturer's published instructions to verify correct operation after the initial testing phase has been performed by the supplier or by the supplier's designated representative. (2) Starting from the functional operating condition, initialize the system in accordance with the manufacturer's published instructions. Confirm that an alternative communications path exists between the wireless control unit and peripheral devices used to establish initiation, indication, control, and annunciation. Test the system for both alarm and trouble conditions. (3) Check batteries of all components in the system monthly unless the control unit checks the batteries and components daily.
Annunciators	Verify the correct operation and identification of annunciators. Verify the correct operation of the annunciator under a fault condition.
Conductors — metallic	
(1) Stray voltage	Test all installation conductors with a volt/ohmmeter to verify that there are no excessive stray (unwanted) voltages between installation conductors or between installation conductors and ground. Verify the maximum allowable stray voltage does not exceed 1 volt ac/dc, unless a different threshold is specified in the manufacturer's published instructions for the installed equipment.
(2) Ground faults	Test all installation conductors, other than those intentionally and permanently grounded, for isolation from ground per the installed equipment manufacturer's published instructions.
(3) Short-circuit faults	Test all installation conductors, other than those intentionally connected together, for conductor-to-conductor isolation per the manufacturer's published instructions for the installed equipment.
(4) Supervision	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices, sounders, and controlled devices on every initiating device circuit and sounder circuit.
Conductors — nonmetallic	
(1) Circuit integrity	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices, sounders, and controlled devices on every initiating device circuit and sounder circuit. Verify all circuits are monitored for integrity.
(2) Fiber optics	Test the fiber-optic transmission pathway by the use of an optical power meter or by an optical time domain reflectometer used to measure the relative power loss of the line. Test result data must meet or exceed ANSI/TIA 568.3-D, *Optical Fiber Cabling and Components Standard,* related to fiber-optic pathways and connection/splice losses and the control unit manufacturer's published specifications.
(3) Supervision	Verify that the introduction of a fault in any circuit monitored for integrity results in a trouble indication at the control unit. Open one connection at not less than 10 percent of the initiating devices and sounders. Test each initiating device and sounder circuit for correct indication at the control unit.

Δ Table 10.4.3(b) Test Methods of Initiating Devices

Initiating Devices	Test Methods
Intrusion Detection Devices	
Audio sensors	Using a sound level meter designed, constructed, and calibrated in accordance with ANSI/ASA S1.4, *American National Standard Electroacoustics — Sound Level Meters — Part 3: Periodic Tests*, determine that the average ambient sound does not exceed the manufacturer's recommendation for the ambient sound level during the period the intrusion detection system is armed. Ensure that the area covered by a single detector does not exceed the area of coverage specified by the detector manufacturer. Utilizing the method recommended by the manufacturer, test the operation of the system.
Contacts	
(1) Door	Open the door.
(2) Window	Open the window.
Exterior buried detectors	Test in accordance with manufacturer's published instructions
Glass break detectors	
(1) Audio	Test in accordance with manufacturer's published instructions
(2) Shock	Test in accordance with manufacturer's published instructions
Motion detection	
(1) Passive infrared (PIR)	Walk across the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
(2) Microwave	Walk into the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
(3) Dual technologies	Walk diagonally across the field of detection at the point farthest from the detector in an upright position at a rate of 762 mm ± 76.2 mm (30 in. ± 3 in.) per second.
Photoelectric detection	Disrupt the channel of detection by passing an object through the channel.
Pressure and stress sensors	Test in accordance with manufacturer's published instructions
Protective cable	Test in accordance with manufacturer's published instructions
Proximity sensors	Test in accordance with manufacturer's published instructions
Shock sensors	Test in accordance with manufacturer's published instructions
Sound detection — vault	Test in accordance with manufacturer's published instructions
Holdup devices	
(1) Fixed in place	Simulate a holdup alarm condition by activating the device.
(2) Portable	Simulate a holdup alarm condition by activating the device at the maximum distance of the area of intended use.
Duress devices	
(1) Fixed in place	Simulate a duress condition by activating the device.
(2) Portable	Simulate a duress condition by activating the device at the maximum distance of the area of intended use.
Ambush devices	
(1) Fixed in place	Simulate an ambush alarm condition by activating the device.
(2) Portable	Simulate an ambush condition by activating the device at the maximum distance of the area of intended use.
Access Control Components	
Controller	Test in accordance with manufacturer's published instructions
Readers	
(1) Key	Test in accordance with manufacturer's published instructions
(2) Magnetic stripe	Test in accordance with manufacturer's published instructions
(3) Radio frequency identification (RFID) card	Test in accordance with manufacturer's published instructions
(4) Biometric	Test in accordance with manufacturer's published instructions
Position sensor	Test in accordance with manufacturer's published instructions
Electric latch	Test in accordance with manufacturer's published instructions
Electric lock	Test in accordance with manufacturer's published instructions
Electromagnetic lock	Test in accordance with manufacturer's published instructions
Request-to-exit (RTE) devices	
(1) Manual	Test in accordance with manufacturer's published instructions
(2) Motion	Test in accordance with manufacturer's published instructions
CCTV Devices	
Video controller	Test in accordance with manufacturer's published instructions
Video switcher	Test in accordance with manufacturer's published instructions
Monitor	Test in accordance with manufacturer's published instructions
Camera	Test in accordance with manufacturer's published instructions
Enclosure	Test in accordance with manufacturer's published instructions

Δ Table 10.4.3(c) Test Methods of Asset Protection Systems

Asset Protection System	Test Method
Tuning	Perform antenna placement, tuning, and measurements for optimal performance in accordance with the manufacturer's published instructions.
Verification	Use the manufacturer's published instructions manual provided by the system supplier to verify correct operation. Initialize the systems in accordance with the manufacturer's operation manual. Conduct a test to verify the presence of the exit lanes and simulate the event of an unauthorized removal of a tagged asset. Test the system for alarm, interference, and trouble conditions.

10.7.2.3 A record of all inspections, testing, and maintenance shall be provided that includes the following information regarding tests:

(1) Date
(2) Test frequency
(3) Name of property
(4) Address
(5) Name of individual or company performing inspection, maintenance, tests, or combination thereof, and affiliation, business address, telephone number, and, if applicable, license information
(6) Name, address, and representative of approving agency(ies)
(7) Designation of the device(s) tested, for example, "Tests performed in accordance with Section _____ of NFPA 731"
(8) Functional test of devices
(9) Functional test of required sequence of operations
(10) Other tests as required by equipment manufacturers
(11) Other tests as required by the AHJ
(12) Signatures of tester and approved owner representative
(13) Disposition of problems identified during test (e.g., "Owner notified," "Problem corrected/successfully retested," "Device abandoned in place")

10.7.3 Monitoring Station Records. For monitoring station premises security systems, records pertaining to signals received at the monitoring station shall be maintained for not less than 12 consecutive months.

10.7.3.1 Upon request, a hard copy record shall be provided to the AHJ.

10.7.3.2 Paper or electronic media shall be permitted.

Chapter 11 Asset Protection Systems

11.1 General. Unless specifically referenced in this chapter, the requirements of Chapter 4 shall not apply to asset protection systems.

11.2* Equipment. The asset protection equipment shall be in compliance with applicable standards.

11.2.1 The application and use of these systems shall be based on the requirements of the owner.

11.2.2 The installation shall meet the following:

(1) Accommodate the design requirements of the owner
(2) Comply with applicable requirements of the *ADA Accessibility Guidelines for Buildings and Facilities (ADAAG)*
(3) Comply with applicable fire and life safety codes
(4) Comply with *NFPA 70*

11.3 Power Sources for Asset Protection Systems.

11.3.1 A 10A, 2-pole ganged disconnect device that provides short-circuit and overload protection and has a minimum 3.048 mm (0.12 in.) open circuit clearance in accordance with *NFPA 70* and with applicable local codes shall be installed at a readily accessible location.

11.3.2 Power shall be provided by a 3-wire, 24-hour, unswitched circuit.

11.4 Antenna. Antennas shall be installed in accordance with the manufacturer's installation instructions.

11.5 Tag.

11.5.1 The application and use of tags shall be based on the requirements of the owner.

11.5.2 The installation shall be in accordance with the manufacturer's instructions.

11.6 Deactivators and Detachers.

11.6.1 The installation shall meet the following criteria:

(1) Conform with the design requirements
(2) Be in accordance with the manufacturer's instructions
(3) Be in compliance with applicable standards such as *NFPA 70*

11.6.2 The application and use of non-powered detachers shall be as follows:

(1) Based on the requirements of the owner
(2) Based on the design requirements
(3) In accordance with the manufacturer's instructions

11.7 Testing. Testing of asset protection systems shall be in accordance with Chapter 10.

Annex A Explanatory Material

Annex A is not a part of the requirements of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.3.1 General. Words used in the present tense include the past tense; words used in the masculine gender include the feminine and neuter; the singular number includes the plural, and the plural number includes the singular.

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.3.2.4 Listed. The means for identifying listed equipment may vary for each organization concerned with product evaluation; some organizations do not recognize equipment as listed unless it is also labeled. The authority having jurisdiction should utilize the system employed by the listing organization to identify a listed product.

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

A.3.3.2 Active Lock. Examples of active locks are electromagnets, electric locks that do not allow free egress, and other locking devices that control egress as well as ingress.

A.3.3.3 Ancillary Functions. Examples of ancillary functions are environmental monitor points, fire detection points, turning lights on and off, control of heating and air-conditioning equipment, or tracking attendance.

A.3.3.4 Annunciator. An annunciator can log alarms or display a continuous status of devices or systems. The annunciator can signal audibly, visually, or both to indicate a change of status.

A.3.3.5.1 Antenna. Antennas can be self-contained devices that contain displays and annunciators and that are permanently mounted to a wall or floor or permanently embedded in the building structure.

A.3.3.5.4 Electronic Article Surveillance (EAS). Systems typically consist of a controller, antenna, and tags. Tags are fixed to items or merchandise and are removed or deactivated when the item is properly purchased or approved for leaving the protected premises. Exit lanes are created at the exit points of the protected premises by means of a detection system that sounds an alarm or alerts staff when it senses a tag. There are several major types of EAS systems.

A.3.3.6 Closed Circuit Television (CCTV). The closed circuit signal can connect by, but is not limited to, coaxial, unshielded twisted pair (UTP), category cable (Cat 5, 5e, 6, etc.), fiber optics, microwave, radio frequency (RF), light (infrared or laser), local area networks (LANs), wide area networks (WANs), and Internet.

A.3.3.10.1.2 Duress Alarm Initiating Device. Often these alarms are triggered by unobtrusive sensors so as not to 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.

A.3.3.10.1.3 Holdup Alarm Initiating Device. A holdup device at the protected premises can be at a bank teller window or store cash register. It is usually initiated by actions of the operator or teller. The alarm is silent, to protect the cashier.

A.3.3.11 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.

•

A.3.3.13 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

A.3.3.13.1 Central Monitoring Station. These are monitoring stations that are neither proprietary nor public safety agency monitoring stations and are usually owned and operated to sell monitoring services to commercial or residential clients for a fee.

A.3.3.13.2 Proprietary Monitoring Station. The properties can be either contiguous or noncontiguous. The proprietary monitoring station can be located at the protected premises or at one of the multiple noncontiguous properties.

A.3.3.16 Premises Security System Provider. A premises security system provider might or might not operate a monitoring station.

•

A.3.3.18 Reader. Readers can be of many types and are intended to include car tags, electronic key, magnetic stripe, proximity badge, biometric, or other identifier.

A.3.3.20 Request to Exit (RTE). The RTE can be manual or automatic. An automatic RTE is often a motion detector on the inside of the portal. The motion detector should be adjusted so that it detects a person approaching the door but is not activated by something pushed under the door from the exterior side of the portal.

A.3.3.22 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.

A.3.3.24.1 Alarm Signals. Alarm signals come from many different systems such as intrusion detection, ambush, duress, holdup alarms, and access control. These systems are defined in this standard for purposes of equipment installation.

However, telling dispatching agencies the type of system is not necessarily of help to the police or guard responding to these alarms. In the simplest terms, dispatching agencies need the following minimum information:

(1) Address
(2) Name of business at protected premises
(3) Type of alarm (intrusion detection or manual such as holdup, panic, or duress)
(4) Class (audible or silent)
(5) Premises (commercial, factory, bank, mercantile, jewelry store, etc.)
(6) Location at premises (zone or area of building)
(7) Device type (motion detector, glass break, door contact, etc.)
(8) Verification attempted (yes or no)
(9) Verification type (call, video, third party)

A.3.3.27.1 Combination System (as related to premises security). In addition to providing some or all of the security services described in this standard, a combination system can also provide other services such as fire alarm, industrial supervision and the like. Control units used in combination systems are intended to be designed to be used with each type of service that is being provided and have been listed for the application.

A.3.3.27.2 Digital Imaging System (DIS). Digital video can connect by, but is not limited to, coaxial, Cat 5, fiber optics, microwave, infrared, local area network (LAN), or wide area network (WAN).

A.3.3.27.5 Integrated System. Other systems include, but are not limited to, fire alarm, building automation, lighting, and administrative controls.

A.3.3.28.1 Ball Trap. Such devices are intended to secure a conductor that is used to protect an air conditioner or similar opening so that the circuit is interrupted if the conductor is removed or cut.

A.3.3.28.3 Disconnecting Trap. Such devices are designed to allow the disassembly of the device without the use of tools for the purpose of servicing such objects. These devices are installed in such a manner that a protective circuit is interrupted if the conductor or cord is cut or moved.

Δ **A.3.3.29 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 UL 608, *Standard for Burglary-Resistant Vault Doors and Modular Panels*.

A.4.2.2 The intent of this subsection is that those devices that receive power from a two-wire circuit, initiating device circuit, or addressable device circuit be listed for use with that control panel. It is not the intent of this subsection to require a compatibility listing for those devices that receive power only from the auxiliary power outputs of the control panel or remote power supply. The system designer does need to be aware of the voltage and current requirements and limitations of both the control unit and the devices powered from the auxiliary output.

A.4.2.4 The presence of an apparent life safety device or appliance creates an expectation that the safety feature is functional, resulting in a false sense of security. It is not the intent to prohibit listed devices that can perform both functions.

A.4.3.1.1 Examples of qualified personnel include individuals who can demonstrate experience on similar systems that they have designed.

Δ **A.4.3.2** The installers of premises security systems should be familiar with the equipment that they are to install. This includes knowing the application limits of the devices and appliances for a particular design. The installer should have an understanding of the causes of false alarms and methods that can be taken to decrease the possibility of their occurrence.

A.4.3.2.2(4) There are various levels of recognized accrediting organizations, ranging from those that accredit installation companies to those that issue certifications for installers. They are not necessarily equal, so each program should be examined to verify that it meets the intent of the interested parties and laws governing the type of system being installed.

Δ **A.4.4.1.3** Other premises security systems can include secondary power supplies. System designers should base the decision for secondary power and capacity on the SVA and the design objectives.

Δ **A.4.4.2.1(4)** Some locations protected by premises security systems might not be near the electric utility grid and alternative power could be sufficient. Alternative power includes solar, wind, and batteries.

Δ **A.4.4.3.5** Secondary power for premises security systems can be greater than the minimum based on the SVA and the design. Consideration should be given to whether access to the system is readily available and to the property being protected. For example, if a standby power source is to be installed in a vault with a time lock mechanism, the capacity of the standby power should exceed the time lock.

The designer should be aware of other standards that can require additional battery capacity.

A.4.4.4.5 Batteries should be securely mounted in such a manner as not to be subject to mechanical damage.

A.4.5.2 When a premises security system is used in conjunction with egress control, consideration should be given to building and fire codes.

A.4.6.1.2 Examples of environmental factors that should be considered include, but are not limited to, the following:

(1) Fog
(2) Rain
(3) Snow
(4) Humidity and corrosion
(5) Cold and heat
(6) Vibration
(7) Radio frequency interference (RFI)
(8) Electrical discharge
(9) Alternating current induction
(10) Dust
(11) Smoke
(12) Animals and insects
(13) Vegetation
(14) Decorations and marketing aids

A.4.6.2.3 The means of indication might be the failure to arm the system until the manually reset device is restored to its normal condition.

A.4.6.2.5 Additional information can be found in *NFPA 70*, Article 110.

A.4.6.2.6 The system designer and the installer should be aware that induced transients such as line noise or alternating current voltage could be injected into a premises security system. *NFPA 70* provides methods for preventing these induced transients from being injected into the system. The system designer and the installer should be familiar with all of *NFPA 70*, particularly Chapters 3, 6, and 8, regarding this issue.

A.4.6.3.3 A splice that is to be soldered should be joined mechanically before being soldered. Each splice and joint should be covered either with insulation equivalent to that of the conductors or with not less than two layers of electrical tape. A splice located in an area of dampness should be treated with a listed sealant or be equivalently treated.

Electrical connections to a device manufacturer's supplied leads should be either of the following methods:

(1) Soldered and heat shrink-wrapped
(2) Crimped with a listed insulating crimp connector

Care should be taken to ensure that each connection between a device's leads and a wire or cable provides the required strain relief.

Electrical connections to terminals on a device should be made by first crimping or soldering spade, tinned wire, or "O"-type connection terminals of a size appropriate to the device's terminals to the conductors from the wires or cables. These connection terminals should be insulated either by manner of their construction and use or by adding heat shrink over the connection for each connector. Poorly performed connections that do not include all the strands of the conductor, that are bent or misshapen, or that do not properly fit the terminals on the device are not acceptable. Care should be taken to ensure that each connection between a device and the wire's or cable's conductors provides adequate strain relief so that a firm tug does not break or damage the connection.

A.4.6.3.4 The intent of this requirement is to shield the wiring from induction of alternating current, in accordance with *NFPA 70*.

A.4.6.3.5 Consideration should be given to selecting appropriate cables in areas that require flexibility of the conductors, such as pole-to-pole cables and elevator traveling cables. Cables might need to have a special listing for applications such as aerial cable.

A.4.6.3.11 The intent of this requirement is to assist service technicians who might not have installed the system, so that they can quickly identify circuits that might be in trouble. Terminal identification can be a schematic on the inside of the control panel door.

A.4.6.3.12 Some examples of properly mounted devices and protected cables are as follows:

(1) If a field device is not mounted on a back box to which raceway can be attached, and it is not possible to provide such a box, then wiring should be protected from abrasion at the raceway end or enclosure. The device and the metal raceway should not be more than 76.2 mm (3 in.) apart.
(2) The orientation of the installed metal raceway relative to the installed device should be so as to facilitate removal, reconnection of a replacement, and reinstallation without the need to damage any finished surfaces or extend time fishing for wires or cables. Generally, such metal raceway should be installed so that its extension would be roughly perpendicular to the finished surface in which the device is installed.
(3) Wire or cable ends at the point of connection to a device should have the outside protective sheathing removed so that the ends of the internal insulated conductors extend at least 50.8 mm (2 in.). The wires or cables should be cut so that, including the stripped end, they extend at least 152.4 mm (6 in.) beyond the finished surface at the point of device installation. Where inserting the cut cable back into the opening is difficult, additional stripping of outside sheathing is acceptable. Removal of the outside sheathing should be performed without damaging the insulation of the internal conductors of the wires or cables. In some cases, manufacturers can provide unique instructions for their product. Stripping of sheathing is not necessarily an acceptable practice with products such as coaxial cable or category network cable.
(4) Conductors should be stripped to the length prescribed by the manufacturer of the device to which the conductors should be connected. The stripped portion of the conductor should have the same number of conductors as the unstripped portion.

A.4.7 The term *low-power* is used to eliminate potential confusion with other transmission media, such as optical fiber cables.

Low-power radio devices are required to comply with the applicable low-power requirements of 47 CFR 15, "Radio Frequency Devices."

A.4.7.1 Equipment listed for household use would not comply with this requirement.

A.4.7.3.1 This requirement is not intended to preclude verification and local test intervals prior to alarm transmission.

A.4.7.3.2 The Federal Communications Commission (FCC) treats alarm retransmission in a very specific way. The following is an extract of the FCC requirements in 47 CFR 15, Section 15.231:

"Periodic operation in the band 40.66 – 40.70 MHz and above 70 MHz

(1) The provisions of this section are restricted to periodic operation within the band 40.66 – 40.70 MHz and above 70 MHz. Except as shown in paragraph (e) of this section, the intentional radiator is restricted to the transmission of a control signal such as those used with alarm systems, door openers, remote switches, etc. Continuous transmissions, voice, video and the radio control of toys are not permitted. Data is permitted to be sent with a control signal. The following conditions shall be met to comply with the provisions for this periodic operation:
    (a) A manually operated transmitter shall employ a switch that will automatically deactivate the transmitter within not more than 5 seconds of being released.
    (b) A transmitter activated automatically shall cease transmission within 5 seconds after activation.
    (c) Periodic transmissions at regular predetermined intervals are not permitted. However, polling or supervision transmissions, including data, to deter-

mine system integrity of transmitters used in security of safety applications are allowed if the total duration of transmissions does not exceed more than 2 seconds per hour for each transmitter. There is no limit on the number of individual transmissions, provided the total transmission time does not exceed 2 seconds per hour.

(d) Intentional radiators which are employed for radio control purposes during emergencies involving fire, security, and safety of life, when activated to signal an alarm, may operate during the pendency of the alarm condition.

(e) Transmission of setup information for security systems may exceed the transmission duration limits in paragraphs (a)(1) and (a)(2) of this section, provided such transmission are under the control of a professional installer and do not exceed 10 seconds after a manually operated switch is released or a transmitter is activated automatically. Such setup information may include data.

In addition, devices operated under the provisions of this paragraph shall be provided with a means for automatically limiting operation so that the duration of each transmission shall not be greater than 1 second and the silent period between transmissions shall be at least 30 times the duration of the transmission but in no case less than 10 seconds."

A.4.7.4.1 Examples of interference are impulse noise and adjacent channel interference.

Δ **A.4.9.1** The primary purpose of premises security system annunciation should be to enable responding personnel to identify the location of an event quickly and accurately.

A.4.9.2 Ideally, one zone should be dedicated to each detection device. If more than one device resides on a zone, the area covered by all zone devices should not exceed the area that one person can maintain under surveillance from a single location.

A.4.9.4 If the system serves more than one building, each building should be indicated separately.

Δ **A.4.10.2** The installed software version number can be located at or within the premises security system or it can be kept elsewhere within the protected premises. The AHJ is to be made aware of the location, and if it is acceptable an alternate location can be used.

Δ **A.4.10.3** A commonly used method of protecting against unauthorized changes follows (in ascending levels of access):

(1) Access Level 1, which is access by persons who have a general responsibility for safety supervision and who could be expected to investigate and initially respond to an electronic premises security alarm or trouble signal

(2) Access Level 2, which is access by persons who have a specific responsibility for safety and security and who are trained to operate the premises security system

(3) Access Level 3, which is access by persons who are trained and authorized to do the following:

(a) Reconfigure the site-specific data held within or controlled by the premises security system

(b) Maintain the premises security system in accordance with the manufacturer's published instructions and data

(4) Access Level 4, which is access by persons who are trained and authorized either to repair the premises security system or to alter its site-specific data or operating system program, thereby changing the basic mode of operation

A.4.11.2.2(2) Listed digital interfaces include serial communications ports, gateways, RS485, or other similar communications protocols.

Δ **A.4.12.2** Examples of parties responsible for the protected premises include but are not limited to the owner of the protected property, the leaseholder of the tenant space where the system is installed, and an employee or agent of the owner or the leaseholder.

Documentation that can compromise the premises security system should be protected in such a way as to prevent the unauthorized release of critical system locations, operations, and functions.

A.4.12.2.1(1) The owner's manual should include the following:

(1) A detailed narrative description of the system inputs, signaling, ancillary functions, annunciation, intended sequence of operation, expansion capability, application considerations, and limitations

(2) Operator instructions for basic system operations, including alarm acknowledgement, system reset, interpretation of system outputs (LEDs, CRT display, and printout), operation of manual ancillary function controls, and change of printer paper

(3) A detailed description of routine maintenance and testing as required and recommended, as would be provided under a maintenance contract, including testing and maintenance instructions for each type of device installed, and that includes the following:

(a) Listing of the individual system components that require periodic testing and maintenance

(b) For each type of device installed, step-by-step instructions detailing the requisite testing and maintenance procedures and the intervals at which these procedures should be performed

(c) A schedule that correlates the testing and maintenance procedures recommended in Chapter 10

(d) Troubleshooting instructions that detail each trouble condition generated from monitored field wiring, including opens, grounds, and loop failures, and that include a list of all trouble signals annunciated by the system, a description of the conditions(s) that cause such trouble signals, and step-by-step directions describing how to isolate such problems and correct them or call for service, as appropriate

(e) A service directory, including a list of company names and emergency (24/7/365) telephone numbers of those companies providing service for the system

A.4.12.2.1(3) Many installers have their own record of completion forms. Examples of record of completion forms are shown in Figure A.4.12.2.1(3)(a) through Figure A.4.12.2.1(3)(e).

RECORD OF COMPLETION INSPECTION & TESTING REPORT

Date: _____ Time: _____

Protected Premises:
Name: _____
Address: _____
_____
Representative: _____
Signature: _____
Telephone: _____

Alarm Service Company:
License #: _____
Name: _____
Address: _____
_____
Representative: _____
Signature: _____
Telephone: _____

TYPE OF SYSTEM (check all that apply)

❑ Exterior intrusion detection ❑ Access control ❑ Video surveillance
❑ Interior intrusion detection ❑ Holdup, duress, or ambush

(Attach an Inspection & Test Report for each type of system checked above.)

DESCRIPTION OF TRANSMISSION

Off-Premises Monitoring:
❑ Central station
❑ Proprietary station
❑ Law enforcement center
❑ None

Monitoring Station:
Name: _____
Address: _____
_____
Telephone: _____

Type of Transmission (indicate the number of each type provided):

_____ Digital _____ Cellular _____ Long-range radio _____ Data packet network
_____ Direct wire _____ Multiplex _____ Derived channel _____ Other

Transmitters:

Mfr.: _____ Mfr.: _____ Mfr.: _____
Model: _____ Model: _____ Model: _____
Transmission type: _____ Transmission type: _____ Transmission type: _____

SYSTEM POWER SUPPLIES

Primary (Main): Nominal voltage: _____ Amps: _____
Overcurrent protection: Type: _____ Rating: _____
Location of disconnecting means: _____
Disconnecting means (panel and breaker number): _____

Secondary (Standby):

Battery ❑ None _____ Hours of backup battery (calculated capacity)
Number of batteries: _____ Date of battery mfg.: _____ Last replacement date: _____
Battery size (AH): _____ Type of battery: _____ Next replacement date: _____

Engine-Driven Generator
Number of generators: _____ Automatic starting: ❑ Yes ❑ No
Location: _____
Party responsible for testing: _____
Test frequency: _____ Date of last test: _____
Transfer switch location: _____ Manual or Automatic (M/A): _____

Δ **FIGURE A.4.12.2.1(3)(a) Sample Record of Completion Report.**

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS INSPECTION & TESTING REPORT

SYSTEM DESCRIPTION

Type of System:
(Check only one; use additional forms for other systems at same premises)

- ❑ Exterior intrusion detection
- ❑ Interior intrusion detection
- ❑ Holdup system
- ❑ Duress system
- ❑ Ambush system

Control Unit:
Mfr.: _____
Model: _____

Type of Circuit:

- ❑ End of line Number of circuits: _____
- ❑ Addressable Number of addresses: _____
- ❑ Wireless Number of transmitters: _____

DETECTION DEVICES

Quantity	Type of Detection	Device Type or Model
_____	Audio sensors	_____
_____	Contacts — door	_____
_____	Contacts — window	_____
_____	Exterior buried detectors	_____
_____	Motion detection	_____
_____	Photoelectric detection	_____
_____	Pressure & stress sensors	_____
_____	Protective cable	_____
_____	Protective wiring	_____
_____	Proximity sensors	_____
_____	Shock sensors	_____
_____	Sound detection	_____
_____	Holdup devices — portable	_____
_____	Holdup devices — fixed in place	_____
_____	Duress devices — portable	_____
_____	Duress devices — fixed in place	_____
_____	Ambush devices	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____

SIGNALING DEVICES

Location	Quantity	Type
❑ None		
❑ Interior	_____	❑ Bell ❑ Siren ❑ Horn ❑ Other _____
❑ Exterior	_____	❑ Bell ❑ Siren ❑ Horn ❑ Other _____

NOTIFICATION OF TESTING

Notify party responsible for the protected premises:
Name: _____ Date _____ Time _____
Monitoring station:
Name: _____ Date _____ Time _____

 NFPA 731 (p. 1 of 3)

Δ FIGURE A.4.12.2.1(3)(b) Sample Intrusion Detection or Holdup and Duress Systems Report.

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS
INSPECTION & TESTING REPORT (continued)

SYSTEM INSPECTION AND TEST

Component	**Visual Check**		**Functional Test**		**Comments**
	Yes	No	Pass	Fail	
Control unit	☐	☐	☐	☐	
Arming means	☐	☐	☐	☐	
Primary power circuit disconnect	☐	☐	☐	☐	
Secondary power	☐	☐	☐	☐	
Batteries	☐	☐	☐	☐	
Voltage at end of test	☐	☐	☐	☐	
Generator records	☐	☐			
Signaling device(s)	☐	☐	☐	☐	
Protective circuit supervision	☐	☐	☐	☐	

DETECTION DEVICE INSPECTION AND TEST

Location/Address	**Visual Check**		**Functional Test**		**Results/Explanation**
	Yes	No	Pass	Fail	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	
	☐	☐	☐	☐	

(Attach additional sheets as necessary to list all devices.)

NFPA 731 (p. 2 of 3)

Δ **FIGURE A.4.12.2.1(3)(b)** *Continued*

INTRUSION DETECTION OR HOLDUP AND DURESS SYSTEMS INSPECTION & TESTING REPORT (continued)

TRANSMISSION TEST

Signal/Component	Yes	No	Time	Comments
Line security	❑	❑		
Alarm signal	❑	❑		
Supervisory signal	❑	❑		
Trouble signal	❑	❑		
Other:	❑	❑		

FINAL TEST REPORT

The following did not operate properly:

NOTIFICATION OF END OF TESTING

Notify party responsible for the protected premises:

Name: Date: Time:

Monitoring station:

Name: Date: Time:

System restored to normal operation: Date: Time:

Testing was performed in accordance with applicable NFPA standards.

Name of inspector: Date:

Signature: Time:

Party responsible for the protected premises: Date:

Signature: Time:

 NFPA 731 (p. 3 of 3)

Δ **FIGURE A.4.12.2.1(3)(b)** *Continued*

ACCESS CONTROL INSPECTION & TESTING REPORT

COMPONENTS

Quantity	Type of Components	Device Type or Model
_____	Controller	_____
_____	Power supply	_____
_____	Reader	_____
_____	Key	_____
_____	Magnetic stripe	_____
_____	RFID card	_____
_____	Biometric	_____
_____	Position sensor	_____
_____	Electric latch	_____
_____	Electric lock	_____
_____	Electromagnetic lock	_____
_____	Request to exit	_____
_____	Manual	_____
_____	Motion	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

NOTIFICATION OF TESTING

Notify party responsible for the protected premises:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

SYSTEM INSPECTION AND TEST

Component	Visual Check		Functional Test		Comments
	Yes	No	Pass	Fail	
Control unit	❑	❑	❑	❑	_____
Primary power circuit disconnect	❑	❑	❑	❑	_____
Secondary power	❑	❑	❑	❑	_____
Batteries	❑	❑	❑	❑	_____
Voltage at end of test	❑	❑	❑	❑	_____
Generator records	❑	❑			_____
Power supply	❑	❑	❑	❑	_____

Δ **FIGURE A.4.12.2.1(3)(c) Sample Access Control Report.**

ACCESS CONTROL
INSPECTION & TESTING REPORT (continued)

COMPONENT INSPECTION AND TEST

Location/Address	Visual Check		Functional Test		Results/Explanation
	Yes	No	Pass	Fail	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	
	❑	❑	❑	❑	

(Attach additional sheets as necessary to list all devices.)

NFPA 731 (p. 2 of 3)

Δ FIGURE A.4.12.2.1(3)(c) *Continued*

ACCESS CONTROL
INSPECTION & TESTING REPORT (continued)

TRANSMISSION TEST

Signal	Yes	No	Time	Comments
Alarm signal	❑	❑	_____	_____
Trouble signal	❑	❑	_____	_____

FINAL TEST REPORT

The following did not operate properly: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

NOTIFICATION OF END OF TESTING

Notify party responsible for the protected premises:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

System restored to normal operation: Date: _____ Time: _____

Testing was performed in accordance with applicable NFPA standards.

Name of inspector: _____ Date: _____

Signature: _____ Time: _____

Party responsible for the protected premises: _____ Date: _____

Signature: _____ Time: _____

Δ **FIGURE A.4.12.2.1(3)(c)** ***Continued***

VIDEO SURVEILLANCE INSPECTION & TESTING REPORT

COMPONENTS

Quantity	Type of Components	Device Type or Model
_____	Video controller	_____
_____	Video switcher	_____
_____	Video multiplexer	_____
_____	Monitor (monochrome or color)	_____
_____	Recorder (Tape or DVR)	_____
_____	Camera	_____
_____	Enclosure	_____
_____	Pan tilt zoom (PTZ)	_____
_____	Alarming inputs	_____
_____	Other: _____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

NOTIFICATION OF TESTING

Notify party responsible for the protected premises:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

SYSTEM INSPECTION AND TEST

Component	Visual Check		Functional Test		Comments
	Yes	No	Pass	Fail	
Control unit	❑	❑	❑	❑	_____
Primary power circuit disconnect	❑	❑	❑	❑	_____
Secondary power	❑	❑	❑	❑	_____
Batteries	❑	❑	❑	❑	_____
Voltage at end of test	❑	❑	❑	❑	_____
Generator test records	❑	❑			_____
Remote controls	❑	❑	❑	❑	_____
Variable lenses	❑	❑	❑	❑	_____

 NFPA 731 (p. 1 of 2)

Δ FIGURE A.4.12.2.1(3)(d) Sample Video Surveillance Test Report.

VIDEO SURVEILLANCE INSPECTION & TESTING REPORT (continued)

COMPONENT INSPECTION AND TEST

Location/Address	Visual Check		Functional Test		Results/Explanation
	Yes	No	Pass	Fail	
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____
_____	❑	❑	❑	❑	_____

(Attach additional sheets as necessary to list all devices.)

TRANSMISSION TEST

Signal	Yes	No	Time	Comments
Digital signal	❑	❑	_____	_____

FINAL TEST REPORT

The following did not operate properly: _____

_____

_____

_____

_____

_____

NOTIFICATION OF END OF TESTING

Notify party responsible for the protected premises:

Name: _____ Date: _____ Time: _____

Monitoring station:

Name: _____ Date: _____ Time: _____

System restored to normal operation: Date: _____ Time: _____

Testing was performed in accordance with applicable NFPA standards.

Name of inspector: _____ Date: _____

Signature: _____ Time: _____

Party responsible for the protected premises: _____ Date: _____

Signature: _____ Time: _____

 NFPA 731 (p. 2 of 2)

Δ **FIGURE A.4.12.2.1(3)(d)** ***Continued***

ADDITIONAL DEVICES
INSPECTION & TESTING REPORT

COMPONENT INSPECTION AND TEST

Type/Location/Address	Visual Check		Functional Test		Results/Explanation
	Yes	No	Pass	Fail	
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________
____________	❑	❑	❑	❑	____________

(Attach additional sheets as necessary to list all devices.)

Additional devices System type: ____________________

 NFPA 731

Δ **FIGURE A.4.12.2.1(3)(e) Additional Devices Test Report.**

A.4.12.3.1 Training should be based on the level of involvement with the system that the user will have. That level can be as simple as how to arm and disarm an intrusion detection system to as complex as how to set levels of access within an access control system.

Training can be provided by, but is not limited to, one-to-one personal training, interactive video or CD-ROM, web-based distance learning, or user training manuals. Training needs to be ongoing, not only for new users of a premises security system but as reinforcement for existing users. Training for all users should take place if the existing system changes due to a system enhancement or a tenant improvement.

A.4.12.3.3 The documentation should contain, at a minimum, the names of the users trained, the date the training was provided, and the scope of the training.

A.5.1.4.2 One method of monitoring for integrity of initiating circuits is to utilize supervision devices located at the end of the circuit.

A.5.1.6.2 The mechanism, such as a keypad or other human/machine interface (HMI), is to be located no farther than a normal 15-second walk from the point of entry. Depending on the size of the premises, the mechanism can be opposite the point of entry, in the next room, or even the same room. This provision is in this standard so that compliance with ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, can be achieved.

A.5.1.7 NFPA 731 is an installation standard. If the AHJ or others have adopted this standard for use, then the installation is to be installed in accordance with the requirements contained within. However, NFPA 731 does not require that a particular method of detection or protection is used over another. The design and selection of devices and appliances should be through the security vulnerability assessment (SVA).

A.5.2.1.2(1) A single stacked photoelectric detector unit with two or more beams can be used as a substitute, provided that two beams are broken before signal initiation.

A.5.2.2 It is not intended that this section apply to video motion detection technology.

A.5.2.3.2 This section covers exterior structures. These structures are those that provide protection and act as a deterrent to unauthorized entry into the exterior surroundings of the premises. An exterior structure can be, but is not limited to being, one of the following:

(1) Fence
(2) Wall
(3) Gate
(4) Area between two or more fences or walls
(5) Sally port
(6) Moat

A.5.2.4.3 This use of video is for detection and is not intended for surveillance. In most cases, the image will not be displayed until after the system detects motion within the field of view. Surveillance systems generally display or capture the image within the field of view constantly. Also see A.5.3.3.1.10.

A.5.3.1 In many cases, UL 681, *Standard for Installation and Classification of Burglar and Holdup Alarm Systems*, provides guidance that applies to various levels of protection needs as determined by a vulnerability assessment.

A.5.3.3.1 The term *perimeter* as used here can refer to interior or exterior structural surfaces.

A.5.3.3.1.2 The system designer and installer are reminded to consider the opening that is to be protected by the contact. A contact that might serve well for a window might not be suitable for a door. A contact for wood frame construction might not operate correctly within a metal frame.

The gap or distance in which the contact will operate when removed from the magnet should also be considered. The optimal distance in which the contact should open is 12.7 mm (0.50 in.). In some applications, such as a contact on a gate, the gap should be wider, to prevent a false alarm.

A.5.3.3.1.10 This use of video is for detection and is not intended for surveillance. In most cases, the image will not be displayed until after the system detects motion within the field of view.

Surveillance systems generally display or capture the image within the field of view constantly. While there are a multitude of positive applications for video surveillance, and though it might be useful in selective alarm system accounts, it is not effective enough in most scenarios at this time to use as a global dispatch reduction tool, and not recommended as a requirement for police dispatch.

There are currently two prominent methods for detecting motion using video. One of them uses an extensive amount of software and algorithms to discern normal activity and objects within the field of view from abnormal. One application is for video analytics such as person or facial recognition. The other method uses a simpler approach by monitoring changes within individual pixels of the image. The amount of pixels, location of pixels within the field of view, and sensitivity to changes in the color spectrum and light can be programmed.

Camera placement relative to the environment in which it is to be used is extremely critical, more so than a PIR. The on-site installation time and effort required to determine the optimal settings for a single camera is far greater than what's required to utilize a PIR. Also, the out-of-the-box performance for discerning an object capable of threat (i.e., a person) from a shadow or changes in light and reflections is far better with a PIR than with a camera equipped with video motion detection.

A.5.4.1 Various U.S. government agencies, state and local jurisdictions, and organizations can have requirements that would apply to these areas.

The Drug Enforcement Administration (DEA) in applying the Controlled Substance Act details alarm protection of containers and vaults that store certain levels of narcotics.

In another example, 12 CFR Part 326, Sections 326.0–326.8 lays out what the FDIC regulates as the "Part 326—Minimum Security Devices and Procedures and Bank Secrecy Act." Everything beyond 326.4 deals with the Bank Secrecy Act (BSA) as it relates to the USA Patriot Act. These minimum standards do not spell out what a safe should have, just that a safe must be used for the protection of cash.

A.5.4.2.3(4) To provide detection of "burning bars," heat and/or smoke detectors can be used to detect the products of combustion and heat. When used exclusively in this application, the requirements of *NFPA 72* are not intended to be met.

A.5.4.2.3(6) See A.5.4.2.3(4).

A.5.4.3.2 See A.5.3.1.

A.6.1.3 Examples of portals include, but are not limited to, doors, gates (personnel and vehicular), lift gates, sliders, barriers, turnstiles (mechanical and optical), mantraps, and sally ports.

A.6.1.4 Readers include, but are not limited to, magnetic stripe, radio frequency identification (RFID) (long and short range), bar code, keypad, Wiegand, biometrics, and smart cards (contact and contactless), or any other device that provides a unique identity of the card or person. Based on the threat level, systems can employ a single reader or a combination of these devices.

A.6.1.4.1 The requirements of the Americans with Disabilities Act and other applicable standards should be considered when selecting mounting criteria.

A.6.1.4.3 An example of portal action would be in health care facilities where gurneys or other such appliances can be in use.

A.6.1.4.7 The actual interval of time should be as short as possible. Typically, most systems complete this sequence within 3 seconds or less. The 10-second interval cited in 6.1.4.7 is the maximum time allowed.

Δ **A.6.1.5.1** Applicable codes and standards can include, but are not limited to, NFPA *101*, *NFPA 5000*, *NFPA 72*, and amendments adopted by the AHJ. Based on the security vulnerability assessment (SVA) of the protected premises, the designer can also consider UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

A.6.1.5.2 In addition to the manufacturer's instructions, the type and rating of the door should be considered. The installation of locking hardware should not compromise the fire rating of a door or door frame. NFPA 80 should be consulted. The manufacturer's specification for the fire-rated door and frame should also be consulted before any field modifications are made.

Locking hardware should be appropriate for the application, and repeated use should not result in the inability of the portal to be secured. Consideration should also be given to other portal hardware that can affect the ability of the portal to be secured.

Use of magnetic door locks ("mag locks") on certain portals poses significant security concerns. For the purpose of life safety, many codes and standards require power interruption to magnetic door locks during fire alarm conditions or loss of primary power. Whenever magnetic lock power is interrupted, the portal can become a free point of both egress and ingress. This is not necessarily an acceptable condition for many premises. Electric portal hardware, which allows mechanical egress, can be a more secure alternative.

A.6.1.5.4 The portal locks can be bypassed during specific time periods of a day, based upon the access control system time schedule. When the portal locks are bypassed, the portal can automatically close but not lock.

Δ **A.6.1.5.5** Applicable codes and standards can include, but are not limited to, NFPA *101*, *NFPA 5000*, *NFPA 72*, and amendments adopted by the AHJ. Based on the SVA of the protected premises, the designer might also wish to consider UL 1034, *Standard for Burglary-Resistant Electric Locking Mechanisms*.

A.6.1.5.6(1) The manual RTE device referenced in 6.1.5.6(1) is typically a push-pad device (e.g., panic hardware or fire exit hardware) that has a microswitch or similar feature that directly interrupts power to the lock.

A.6.1.5.7 The means of lock release detailed in 6.1.5.6 are not necessarily required for occupancies such as detention and correctional occupancies, psychiatric hospitals, or other occupancies where locked doors are permitted and egress or relocation is supervised by trained staff, provided staff has a means to release the lock and the AHJ approves such an installation.

N **A.6.1.5.9.4(3)** Other credentials could include electronic keypads, electronic card readers, or remote unlocking devices.

A.6.1.6.1 Examples of position sensors include, but are not limited to, edge sensors, gate arm limit switches, and contact switches. Position sensors can also be used for other applications such as relocking, arming, and disarming of an intrusion detection system and other approved control functions. The integration of the access control system should not compromise the primary objectives of the access control system.

The use of an access control system in integration with an intrusion detection system should not create false alarms from the system not being properly disarmed prior to entry.

A.6.1.7 The two methods of authorized egress are free egress and controlled egress.

A.6.1.7.1.2 The RTE can bypass the door position switch and not be used to control the lock at the portal. If the RTE also controls the portal lock, concerns for life safety would dictate that the lock be fail-safe on loss of power.

A.6.1.7.2 Controlled egress can be used for applications such as anti-passback, mustering, patient wandering, infant abduction, and two-person rule.

A.6.1.7.2.2 Controlled egress can be enforced by an alarm being sounded if the portal is opened without presentation of a valid credential or by preventing the opening of the portal. If opening the portal is prevented and the portal is a required means of egress, then the requirements for active locks should be used.

A.6.1.9.2 Depending upon the design of the system, one or several power supplies can be used. The power supplies should be sized to provide adequate power for simultaneous use of all associated devices, such as readers, RTE motion detectors, locks, controllers, and so forth. Power calculations need not take into account simultaneous inrush current.

As a result of certain conditions, such as temperature, device inrush requirements, tolerances, and other environmental factors, it is recommended that power supplies be designed with a safety factor of 25 percent.

A.6.2.1 The system operating parameters can be based on an SVA of the protected premises.

A.6.3 This standard currently applies to the protected premises. Network configurations that send data off-premises can need additional protection in the form of encryption. Current encryption schemes can be certified by the National Institute of Standards and Technology (NIST) in accordance with Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. Typically, encryption schemes

used for security applications employ a minimum 128-bit algorithm.

A.7.2.3 In the absence of an SVA or AHJ requirement, consideration should be given to protecting the cameras from vandalism.

The quality of the image should not be impaired by the method used to provide vandal resistance. Suitable installation techniques could include the mounting and positioning of the camera so that, without compromising the requirements of Section 7.2, it is not readily accessible to a vandal. Information regarding SVA procedures can be found in NFPA 730.

A.7.2.4 With the addition of any device that requires power, consideration should be given to the power consumption of these devices. Additional power supplies or a change in wiring size might be required.

A.7.2.4(1) The use of a heater within an enclosure might be required to protect the camera, lens, and auto iris.

A.7.2.4(2) Whenever possible, the camera should not look directly into the sun or other source of light.

A.7.2.4(3) The selection of enclosures should be appropriate for the prevalent environmental conditions. Heaters, blowers, defrosters/defoggers, and wipers can be required. The purpose of sunshields or sun hoods will reduce the heating effect of the sun on the camera housing.

A.7.2.4(4) Mounts and remote positioning devices should be selected and installed to withstand local wind conditions and provide a usable image based upon the requirements of the AHJ.

A.7.2.4(5) A method should be provided so that external moisture does not impair the ability of the camera to produce a usable image as required by the AHJ.

A.7.2.5.1 If a camera has a view that looks directly into a bright light source or extremely high contrast scene, the quality of the foreground image is degraded. The camera should be relocated so that its field of view is perpendicular to the light source or be positioned so that the source of light is behind the camera.

A.7.2.5.2 Backlight compensation (BLC), if utilized, allows the camera to be able to reduce the level of the video at the bright areas and then reproduces the overall video signal at an average video level. Most cameras now have this feature, and the more advanced cameras have the means to set the parameters for each application. The installing technician should be aware of the location of the sensing windows for BLC to work correctly. Anytime that BLC is used, it should be field adjusted.

A.7.3 Low-level lighting conditions can be compensated for in many ways, including, but not limited to, the following:

(1) Cameras listed by their manufacturer to operate at 10 lux (0.93 fc) or less
(2) Use of light amplification devices such as a starlight scope
(3) Nonvisible scene illumination such as infrared (IR) or ultraviolet (UV)
(4) Addition of artificial light such as high-mast lighting or perimeter pole lights

A.7.4 In addition to the manufacturer's instructions, the choice of an enclosure should be based on application, environmental concerns, an SVA, or the AHJ. An enclosure should be chosen that best protects the camera and lens combination from the ambient environment. Some considerations are indoor or outdoor location, temperature extremes, high humidity or condensing moisture, salt water exposure, rain, snow, hazardous or volatile atmospheres, vandalism, and tampering. Each camera location should be assessed to determine which factors exist and the appropriate enclosure type and enclosure options chosen to best suit the needs of that location.

A.7.5 Mounting assemblies have a few basic requirements. The selection criteria consist of the following:

(1) Overall length of the camera housing
(2) Total weight of the camera, lens, and housing
(3) Type of mounting required (wall, pole, or ceiling)

When mounting equipment, the installer should consider such factors as weight of the unit, the mounting rating (structural load on the hardware), and the orientation of the equipment (inverted mounting).

Weight. The weight of the overall unit is needed to select the proper mounting bracket, but it is also a necessary factor when fastening the mounting bracket to a surface. All mounting brackets require either screws or bolts to mount to a surface.

Mounting Ratings. Mounting ratings should be as follows:

(1) For equipment less than 13.6 kg (30 lb)
    (a) Wood fasteners should penetrate a minimum of 50.8 mm (2 in.) into the surface.
    (b) In concrete, lead anchors or expansion bolts should have at least 27.2 kg (60 lb) pull-out strength.
    (c) In steel, bolts should be long enough to accommodate a lock washer and nut.
(2) For equipment up to 36.3 kg (80 lb)
    (a) In wood, 9.52 mm (⅜ in.) diameter bolts should penetrate a minimum of 88.9 mm (3½ in.) into the surface.
    (b) In concrete, lead anchors or expansion bolts should have at least 68 kg (150 lb) pull-out strength.
    (c) In steel, 9.52 mm (⅜ in.) diameter bolts should be long enough to accommodate a lock washer and nut.

Inverted Mounting of Equipment. Most weight loads of the mounts, if used in a ceiling application, are reduced by a factor of 50 percent. Consult the manufacturers' specification sheets for specific requirements.

A.7.5.1.2 Anchoring sets should be appropriate for the surface to which they are mounted.

A.7.5.4 Such hardware can include tamper-resistant bolts, nuts, screws, locks, and similar equipment.

A.7.7 This section is meant to be applicable to the various types of wire and cable used to supply power, control, or video connections to video surveillance equipment and includes, but is not limited to, coaxial type, UTP, and fiber-optic (FO) cable.

A.7.7.1 Installers should know the electrical codes and how to apply them according to their area of work. Knowledge of raceways should include the following as they apply to low-voltage systems:

(1) Practices necessary for the installation of raceways
(2) Purpose of each raceway

(3) Tools required for the professional installation of raceways
(4) Restrictions of raceways

A.7.7.2 Underground/direct burial, pole-to-pole outside/UV protected, and return air plenum/plenum rated are examples of different insulation jacketing.

A.7.7.4 It should be the responsibility of the installer to use the appropriate connectors and methods of installation as dictated by the equipment and cable manufacturers' instructions. The selection of connectors should be based on a consideration of the environment, the conductor type, and the specific use (control, power, video, or data).

A.7.7.5 The applications for wiring within video surveillance systems are as follows:

(1) Control
(2) Power
(3) Video signal transmission

Because sufficient voltage and signal levels are imperative for proper system operation, consideration should be given to designing voltage drop (power and signal) allowances that would result in adequate operating voltage (or signal) at the various pieces of equipment.

A.7.7.5.1 The purpose of low-voltage control cabling is to carry various low-voltage signals to devices within the video surveillance system. Such devices can include, but are not limited to, the following:

(1) Remote positioning devices (pan/tilt units, scanner units, domes)
(2) Cameras (primary input power)
(3) Zoom lenses
(4) Auxiliary devices (low-voltage wipers and washers, low-voltage heaters and blowers, remote relays)

A.8.1.2.5 To minimize the unintentional operation of a portable device, factors such as jarring, contact with clothing, and similar sources should be considered.

A.8.2.2.8 The party responsible for the protected premises should ensure that this training takes place. In addition, employees should be trained to follow the procedures provided by their employer and the law enforcement agency having jurisdiction.

Δ **A.8.2.2.9** Off-premises locations that are used to receive holdup alarm signals should be equipped to retransmit signals to the law enforcement center that serves the property. Alarms are usually annunciated at a monitoring station. One example of off-premises locations that can receive alarm signals is one that complies with UL 827, *Standard for Central-Station Alarm Services*.

A.8.3.2.5 The intent of a duress system is to notify on-site personnel of a potentially hostile civil disturbance or emergency at the protected property and for summoning assistance to the area of the civil disturbance or emergency.

A.8.4.2.1 To reduce the incidence of inadvertent ambush signals, the following steps should be taken:

(1) If an ambush feature is provided in a control unit that is also used to operate other systems, the default setting should be that it is disabled.
(2) An ambush signal should be sent only by a unique code.
(3) A control panel that is also used to operate other systems should not derive the ambush code from an existing operating code such as a "user code plus ambush digit" sequence.

A.8.4.2.4 Each person who is expected to use an ambush alarm initiating device should be instructed to follow the procedures provided by the operator of the protected premises and the law enforcement agency having jurisdiction.

Δ **A.8.4.2.5** Alarms are usually annunciated at a monitoring station. One example of off-premises locations that can receive alarm signals is one that complies with UL 827, *Standard for Central-Station Alarm Services*.

A.9.2.1 These signals can include, but are not be limited to, the following:

(1) Alarms (including intrusion detection, holdup, and duress)
(2) Supervisory
(3) Trouble
(4) Restorals
(5) Open/close events
(6) Access control activity
(7) Video surveillance
(8) Audio surveillance

A.9.3.1 This section does not include any requirements for the handling or dispatching of calls for assistance and should be directed only at electronically received signals.

A.9.3.4.4 The determination of the type of detection device to be used should be based on an SVA for the facility. NFPA 730 can be used.

Building designers should consider security through environmental design and should provide zones immediately around the facility to ensure security of the grounds and the safety of the personnel within.

A.9.3.5.1 Standby power should have sufficient capacity to be able to operate HVAC necessary to maintain the environmental range of the monitoring equipment. Lighting should be provided to allow operators to perform normal functions.

A.9.3.5.1.1 The emergency power supply system (EPSS) can be used to supply other building loads. The EPSS should be sized to handle all loads simultaneously without having to shift other loads off the system. When life safety equipment is connected to the EPSS, consideration should be given to increasing the EPSS to level 1, type 10.

Δ **A.9.3.5.1.4** Guidance on preventing unauthorized access to the power supply can be found in UL 827, *Standard for Central-Station Alarm Services*.

A.9.3.6.3 All training should be in compliance with the manufacturer's recommendations, and a program should be in place for the continuing education of operators. Resources for this education include, but are not limited to, the Central Station Alarm Association, the Security Industry Association, and the Association of Public Communication Officers.

A.9.3.9.2.1 The list should contain, at a minimum, a contact name, phone number, after-hours cell phone number, and service contract information for each provider.

A.9.3.9.3.2 At a minimum, equipment should be able to operate within an environment of high-energy radio frequencies. In

addition, the equipment should not interfere with or be interfered with by any electronic equipment within the facility. The equipment should also be shielded from electromagnetic interference and radio frequencies as required.

A.9.3.9.4 Special consideration and contingency plans need to be considered. If the monitoring station is receiving signals from any high-risk facilities as defined by the Department of Homeland Security (DHS), provisions should be considered for implementing emergency transfer to the backup location.

A.9.6.1.1(4) Cross-zoning is one method of MTV. This method is used where there are technology limitations with the installation environment. An analysis of the application and use of cross-zoning should be performed, because this method might not be appropriate in many locations. With this method, at least two sensors within the same area of coverage should be installed. In this case, all sensors within the area should have tripped before an alarm is generated. The use of cross-zoning for intrusion detection systems is not the same as cross-zoning for fire alarm systems.

It is intended that cross-zoning would use separate sensors, not two detection means within a single sensor. This is a method of "dual technology." Cross-zoning is best achieved by using two separate sensors. Both could use the same technology or different technologies, which could include the use of a door contact for one of the zones.

A.9.6.1.1.1.2 The intent of 9.6.1.1.1.2 is for the monitoring station to call the protected premises first to verify the signal. It is realized, however, that there could be cases in which the protected premises might not have phone service. In those cases, the monitoring station can make the first call to a primary contact number that is provided by the system user.

A.9.6.1.1.2 Remote video verification (RVV) is intended to be used as a supplement to enhanced call verification (ECV). If through the use of RVV it is apparent that a crime or unauthorized entry is taking place at the protected premises, the information obtained can be transmitted or communicated to the public safety agency so it can coordinate the response protocol.

A.9.6.1.1.3 Remote audio verification (RAV) is intended to be used as a supplement to ECV. If through the use of RAV it is apparent that a crime or unauthorized entry is taking place at the protected premises, the information obtained can be transmitted or communicated to the public safety agency so that it can coordinate the response protocol.

RAV can be one way or two way. With one-way RAV, the monitoring station can listen in to the protected premises after an alarm activation. With two-way RAV, the monitoring station can, in addition to listening in, engage in a conversation with individuals who are on the protected premises.

A.9.6.3.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.4.2.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.5.1 The term *immediately* in this context is intended to mean "without unreasonable delay." Routine handling should take a maximum of 90 seconds from receipt of the alarm signal by the monitoring station until the initiation of notification to the public safety agency.

A.9.6.6 Facility hazards information should be provided to the first responders and can include information on rapid entry systems, dangerous chemicals or gases, explosive materials, or any other dangerous condition that might exist. Information on special security notices such as attack dogs, smoke bandits, chemical releasing agents, or security traps should also be maintained.

A.9.7.2 Transmission methods are changing. The uses of traditional landline-based communication methods are no longer as common as they once were. Voice over Internet Protocol (VoIP), facility and non-facility based as provided by common carriers, cable communication providers, and Internet providers, is becoming the new norm. The users of these communication methods need to be aware that control units that use communication technologies that are based on the public switched telephone network (PSTN) and using plain old telephone service (POTS) might not function on these new communication paths. Having a test signal sent in once every 7 days adds a level of reliability to verify that there is an active communication path between the protected premises and the monitoring station.

A.9.7.6.1(4) The intent of 9.7.6.1(4) is not to limit each line to 3000 transmitters but to require that if 3000 transmitters are exceeded on a single path, a redundant path is provided. This is to be considered primarily when broadband communication (Internet) solutions are used.

A.9.7.6.2 An inventory of spare equipment at the monitoring station allows personnel to replace any failed piece of equipment.

A.9.7.7.1(3) The intent of 9.7.7.1(3) is not to limit each line to 3000 transmitters but to require that if 3000 transmitters are exceeded on a single path, a redundant path is provided. This is to be considered primarily when broadband communication (Internet) solutions are used.

A.9.8 These records include, but are not limited to, the following:

(1) Signal history
(2) Documentation of personal identification codes (PICs)
(3) Public safety agency notification information

Note: Although the information on the PICs should be retained, it should be kept confidential and made available on a need-to-know basis.

A.10.1 More stringent inspection, testing, and maintenance procedures that are required by other parties can be permitted.

A.10.1.2 Equipment performance can be affected by building modifications, occupancy changes, changes in environmental conditions, device location, physical obstructions, device orientation, physical damage, improper installation, degree of cleanliness, or other obvious problems that might not be indicated through electrical supervision.

Δ **A.10.1.3** The premises security system provider responsible for the premises security system is the individual or organization

that ensures that inspection, testing, and maintenance are performed.

A.10.2.1 Examples of system defects and malfunctions are a trouble signal to the control panel or controller, a reader that is not operating, a video surveillance camera that is no longer providing an image, and other similar events.

A.10.2.1.1 The time period to initiate a repair should be less than 24 hours based on an agreement with the owner and the premises security system provider.

A.10.2.1.2 Notification to the owner is so that other security measures can be implemented.

A.10.2.2 Temporary mitigating measures should be considered by the owner or responsible party during impairments based on an SVA to the protected property or the occupants. Depending on the SVA, the AHJ can be consulted. The recommendations from the consultation should be implemented for the period that the system is impaired.

A.10.2.5 Additional security measures might be needed during the period of the impairment. These impairments can be caused by, but are not limited to, the following:

(1) Telecommunication errors
(2) Accident
(3) Fire
(4) Acts of God
(5) Loss of carrier
(6) Other transmission method failures

A.10.3.4.1 Door assemblies that are incorporated into the premises security system need to be periodically inspected to ensure they function correctly. Mechanical components and subcomponents (e.g., door leaves, hinges, locks, door closers) can prevent the door assembly from being able to perform its security function if they are malfunctioning, broken, or missing.

A.10.3.4.2(1) The factory training and certification should be specific and current to the equipment that is being used, and proof of this factory training and certification should be made available to the AHJ upon request.

A.10.3.5.1 In addition to advising the personnel within the protected premises that the system is being tested, repaired, or maintained and that signals generated from the system(s) should not be acted upon, the owner or responsible party should be advised that the system or a part of the system might not be fully functional during the testing, repairing, or maintenance procedure and that appropriate safeguards should be taken, based upon the perceived risk.

The party responsible for the protected premises should also be informed that if the system is placed into a degraded mode, some, if not all, information from those nodes can be lost during the time in which the node(s) is down.

A.10.4.2.2 This section requires that only the portions of the system that might have been affected by a modification need to be tested. As an example, if a door contact is added to zone 12, then only zone 12 is required to be tested. If there is a change to several zones, then only those zones would be required to be tested.

On the other hand, if there is a change to the system firmware or software that could affect the entire system, then the entire system should be tested.

A.10.5 Premises security systems and other systems and equipment that are associated with security systems and accessory equipment should be tested at the frequencies according to Table A.10.5.

Table A.10.5 Test Frequency

System, Device, or Equipment	Frequency
Intrusion detection system	Annually
(1) Exterior detectors	Annually
(2) Interior detectors	Annually
Holdup, duress, or ambush system	Annually
(1) Portable devices	Annually
(2) Exterior fixed devices	Annually
(3) Interior fixed devices	Annually
Access control system	Annually
(1) Readers	Annually
(2) Position switches	Annually
(3) Electric hardware	Annually
(4) Request-to-exit devices	Annually
CCTV system	Annually
(1) Camera enclosures	Annually and before adverse weather conditions
(2) Recorders	Annually
Sounding devices	Annually
Batteries — general tests	Annually
Off-premises transmission equipment	Quarterly or by automatic monthly test
Interface equipment	Annually

N **A.10.6.1** Equipment should be covered under a service agreement. Any device or system not functioning as designed should be repaired or replaced on a priority basis. The priority basis should be established by procedures developed in the SVA, manufacturer's instructions, or by the applicable standards.

Δ **A.11.2** Typical standards include UL 60950-1, *Standard for Information Technology Equipment – Safety – Part 1: General Requirements*; FCC 47 CFR Part 15; "Radio Frequency Devices"; and UL 1037, *Antitheft Alarms and Devices.*

Annex B Camera Specifications

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

B.1 Cameras. For cameras placed to record images at a point of customer transactions, such as a teller window, the area of interest (face, license plate, etc.) should cover a minimum of 15 percent of the camera's field of view under normal resolution of 300 horizontal lines (HL) or more. Action within the scene requires that at least 20 percent or more of the overall width of the scene be used. For an average human head that is 15.24 cm (6 in.) wide, a 0.914 m (3 ft) wide field of view meets this guideline. For a license plate width of approximately 304.8 mm (12 in.), a 1.828 m (6 ft) field of view is sufficient.

The focal length necessary to achieve an approximately 0.914 m (3 ft) wide field of view for a given detector size and camera-to-subject distance is provided in Table B.1(a) (SI Units) and Table B.1(b) (U.S. equivalent units). The camera has to be in focus at the position of this subject.

Table B.1(a) and Table B.1(b) are based on the following calculations using either the scene width formula or the scene height formula.

[B.1a]

$$f = c\left(\frac{d}{w}\right)$$

or

[B.1b]

$$f = v\left(\frac{d}{h}\right)$$

where:
f = focal length of lens
c = width of the charge-coupled-device (CCD) chip
d = distance from camera
w = width of field of view
v = height of CCD chip
h = height of field of view

Cameras that provide overviews of interior and exterior locations should have their focal lengths selected to meet the field-of-view requirements of the AHJ. Note, however, that exit cameras should have sufficient depth of field to be in focus at distances of 0.914 m (3 ft) and beyond to ensure that subjects exiting are in focus.

Another method takes into account the total viewing area of the scene as a percentage of the monitor. Calculate the viewing area of the scene and also of the critical viewing area by multiplying the horizontal and vertical dimensions *[see Table B.1(c)]*. Divide the critical viewing area by the total viewing area to get the size of the critical viewing area in the monitor.

If the proportion of the critical viewing area is as expected, use the calculated focal length. If not, then change the focal length until the correct proportion is found, or change the distance of the camera until the correct proportion is found. If this does not solve the problem, a new lens might have to be chosen that is nearer to the requirement.

Table B.1(b) Approximate Focal Length Needed for 3 ft Wide Field of View

	Focal Length Based on Distance to Subject					
Detector Size (in.)	**2 ft**	**5 ft**	**10 ft**	**15 ft**	**20 ft**	**30 ft**
¼	2.3	5.9	11.7	17.6	23.5	35.2
⅓	3.1	7.8	15.7	23.5	31.3	47.0
½	4	10.1	20.2	30.3	40.4	60.7

Table B.1(c) Field of View

Camera Formats (in.)	Horizontal (mm)	Vertical (mm)
¼	3.2	2.4
⅓	4.4	3.3
½	6.4	4.8
⅔	8.8	6.6

B.2 Example. A 8.46 mm (⅓ in.) camera is viewing an entrance gate to a factory. The car coming through the gate is the critical view.

⅓ chip

Width (c) = 4.8 mm = 0.048 m (0.15 ft)

Height (v) = 3.6 mm = 0.036 m (0.11 ft)

Distance to gate (d) = 30.48 m (100 ft)

Width of gate (w) = 3.65 m (12 ft)

Car dimension (front) = 1.524 m × 1.524 m (5 ft × 5 ft)

Focal length $f = c \times (d/w)$ = 0.048 m × (30.48 m/3.65 m) = 0.40 m [0.16 ft × (100 ft/12 ft) = 1.33 ft]

Scene height $h = v \times (d/f)$ = 0.036 m × (30.48 m/0.4 m) = 2.75 m [0.11 ft × (100 ft/1.33 ft) = 9 ft]

Scene area = 3.65 m × 2.74 m = 10 m^2 (12 ft × 9 ft = 108 ft^2)

Critical area = 1.524 m × 1.524 m = 2.3 m^2 (5 ft × 5 ft = 25 ft^2)

Percent size of car in monitor = 25 × (100/108) = 23.1 percent

The car covers about 23 percent of the monitor. This allows positive identification of the car coming through the gate.

Table B.1(a) Approximate Focal Length Needed for 0.914 m Wide Field of View

	Focal Length Based on Distance to Subject					
Detector Size (m)	**0.6096 m**	**1.524 m**	**3.048 m**	**4.572 m**	**6.096 m**	**9.144 m**
0.0762	2.370104	1.79832	3.56616	5.36448	7.1628	10.72896
0.100584	0.94488	2.3744	4.78536	7.1628	9.54024	14.3256
0.1524	1.2192	3.07848	6.15696	9.23544	12.31392	18.50136

Scene identification should require that each camera within a system is able to be differentiated by its image's physical appearance. No system should have any two cameras looking from the same angle down two identical hallways. Each scene should be separable by visual recognition. The installer should follow the manufacturer's recommendations concerning the various compatibility issues that occur between the cameras and lens. Such compatibility issues can be physical or electronic.

B.3 Megapixel (MP) Cameras. The megapixel size for MP cameras should be based on the field of view and necessary needs for the ability to zoom in on a fixed image.

Annex C Camera Selection

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

C.1 Criteria. A number of common camera selection criteria should be reviewed by the system installer prior to the installation to verify that the design objective is met. The criteria are as follows:

(1) Monochrome or color
(2) Light level and sensitivity
(3) Resolution
(4) Backfocus adjustment
(5) Format
(6) Sync and phase

C.1.1 Monochrome or Color. All white balance settings on or within the camera are set according to the manufacturer's specification to provide proper color rendition. In the event of a dual-chip technology camera system, the installer should perform setup procedures deemed necessary by the manufacturer to provide a proper white balance during high-light situations and proper black/white (B/W) sensitivity during low-light situations.

C.1.2 Light Level and Sensitivity. Sensitivity, measured in footcandles or lux (lumens per square meter), indicates the minimum light level required to get an acceptable video picture. Sensitivity at faceplate indicates the minimum light required at the charge-coupled-device (CCD) chip to get an acceptable video picture. Minimum scene illumination indicates the minimum light required at the scene to get an acceptable video picture.

To see properly, a video surveillance camera requires a certain amount of light produced by natural or artificial illumination. B/W cameras work with any type of light source, but color cameras need light that contains all the colors in the visible spectrum.

The amount of light is defined by lux or footcandles. One lux is a candlelight volume at a 0.914 m (3 ft) distance. The following are some examples of natural light:

(1) Full daylight is 10,000 lux (929 footcandles).
(2) Very dark day is 100 lux (9.3 footcandles).
(3) Twilight is 10 lux (0.93 footcandles).
(4) Deep twilight is 1 lux (0.093 footcandles).
(5) Full moon is 0.1 lux (0.0093 footcandles).
(6) Quarter moon is 0.01 lux (0.00093 footcandles).

A good B/W camera can see in full-moon conditions. However, a color camera might need additional illumination in low-light conditions.

Usually light falls on the subject. A certain percentage is absorbed and the balance is reflected. The reflected light moves toward the lens in the camera. Depending on the iris opening of the camera, a certain portion of the light falls on the CCD chip. This light then generates a charge, which is converted into a voltage. The following variables should be listed on the data sheet to indicate the minimum scene illumination:

(1) Reflectance
(2) F-stop
(3) Usable video
(4) Automatic gain control (AGC)
(5) Shutter speed

C.1.2.1 Reflectance. Light from a light source falls on the subject. Depending on the surface reflectivity, a certain portion of the light is reflected back toward the camera. Following are a few examples of surface reflectivity:

(1) Snow is 90 percent.
(2) Grass is 40 percent.
(3) Brick is 25 percent.
(4) Black is 5 percent.

Most camera manufacturers use an 89 percent or 75 percent (white surface) reflectance surface to define the minimum scene illumination. If the actual scene has the same reflectance as in the data sheet, then there is no problem, but in most cases this is not true. A black car will reflect only 5 percent of the light, so at least 15 times more light is required at the scene to give the 75 percent reflectance.

C.1.2.2 Lens Speed. The reflected light starts moving toward the camera. The first device it meets is the lens, which has a certain iris opening. While specifying the minimum scene illumination, the data sheet usually specifies an F-stop of F1.4 or F1.2. The F-stop gives an indication of the iris opening of the lens. The larger the F-stop value, the smaller the iris opening, and vice versa. If the lens being used at the scene does not have the same iris opening, then the light required at the scene needs to be compensated for the mismatch in the iris opening.

C.1.2.3 Usable Video. After passing through the lens, the light reaches the CCD chip and generates a charge that is proportional to the light falling on a pixel. This charge is read out and converted into a video signal. Usable video is the minimum video signal specified in the camera data sheet to generate an acceptable picture on the monitor. It is usually measured as a percentage of the full video.

C.1.2.4 AGC. As the light level reduces, the AGC switches on and the video signal gets a boost. Unfortunately, the noise present also gets a boost. However, when the light levels are high, the AGC switches off automatically, because the boost could overload the pixels, causing vertical streaking and so forth.

The data sheet should indicate if the AGC is on or off when the minimum scene illumination is being measured. If the data sheet indicates AGC is "on," but in reality the AGC is "off," then the minimum scene illumination in the data sheet should be modified.

C.1.2.5 Shutter Speed. Most cameras now have an electronic shutter speed that allows the user to adjust the timing of the charge read of the CCD chip. The standard readout is 50 times [phase alternate by line (PAL)] and 60 times [National Television Standards Committee (NTSC)] per second. If the shutter

speed is increased to 1000 times per second, for example, the light required at the scene should be 20 times more (for PAL). Increasing the shutter speed allows the picture to be crisper but requires more light.

C.1.3 Resolution.

C.1.3.1 All cabling and signal transmission methods should be installed with the proper connections, splices, and amplification to ensure that the image resolution is maintained at the maximum capability of the system's design.

C.1.3.2 IP camera resolution is measured in native and enhanced resolution scales. IP cameras will generally have a native resolution that can be digitally enhanced for higher resolution.

C.1.4 Backfocus Adjustment. The term *backfocus* refers to the course adjustment on the camera that positions the imager behind the lens. This adjustment allows for the proper positioning of the fine-focus adjustment on the lens. *Focus* refers to adjustment of the distance between the lens and the imager device in the camera. Focusing aligns the focal plane of the lens with the imager in the camera. When focusing, the iris of the lens must be opened to create the shortest depth of field. The lens should be focused and then the iris closed to increase the depth of field. An installer must know the relationship between F-stop and depth of field and how to properly focus both manual and auto-iris lenses.

C.1.5 Format. Knowing the size of the imager is necessary in selecting the appropriate focal lens to provide the desired view.

C.1.6 Sync and Phase. Power requirements of the video equipment are determined and established during the design phase. The line-locking feature of a camera means that the camera's vertical sync pulse locks to the incoming alternating current (ac) power line frequency. The reason is to ensure that the vertical pulses from many different cameras occur at the same time, eliminating any vertical roll when the cameras are switched. Direct current (dc)–operated cameras cannot be line-locked. Vertical sync of each camera should be adjusted according to the manufacturer's instructions.

C.1.7

C.1.7.1 Frame Rate. Most IP cameras have the ability to select how many frames per second a camera will send digital video. A frame is an individual picture that is taken. Standard movie-quality video is 30 frames per second, however the human eye can only register the difference in frames per second in motion video when the frames per second is 15 or lower. An increase of frames per second will increase video clarity and storage requirements, and a decrease in frames per second will decrease video clarity and storage requirements.

C.1.7.2 Compression. Compression is an algorithm that takes certain frames, called key frames, and measures them against other frames of video after the key frame. The differences between the key frames and the frames after the key frame are the only data sent for each frame.

C.1.7.3 Bandwidth. Bandwidth is the amount of data, measured in bytes, that the digital video will require on the network in order to transmit the video.

C.1.7.4 Bandwidth Calculators. Bandwidth calculators are tools provided by the camera and NVR manufacturers that approximate the bandwidth required for an IP video surveillance system.

N Annex D Homeland Security Advisory System

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

N **D.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. [**730:**B.1]

The following threat response recommendations are voluntary. [**730:**B.1]

N **D.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. [**730:**B.2]

N **D.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.

[**730:**B.2.1]

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.
[**730:**B.2.1]

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
[**730:**B.2.1]

N **D.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.
[**730:**B.2.2]

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.
[**730:**B.2.2]

N **D.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.
[**730:**B.2.3]

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.
[**730:**B.2.3]

N **D.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. [**730:**B.3]

N **D.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.
[**730:**B.3.1]

N **D.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.
[**730:**B.3.2]

N **D.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. [**730:**B.4]

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

[**730:**B.4]

N **D.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.

[**730:**B.5]

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

[**730:**B.5]

N **D.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. [**730:**B.6]

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. [**730:**B.6]

N **D.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. [**730:**B.6.1]

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

[**730:**B.6.1]

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.

[**730:**B.6.1]

N **D.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.

[**730:**B.6.2]

N **D.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: burn-

ing 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.

[**730:**B.6.3]

N **D.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.

[**730:**B.6.4]

N **D.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. [**730:**B.7]

N **D.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. [**730:**B.7.1]

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)

[**730:**B.7.1]

N **D.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. [**730:**B.7.2]

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. [**730:**B.7.2]

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. [**730:**B.7.2]

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. [**730:**B.7.2]

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.

[**730:**B.7.2]

N **D.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.

[**730:**B.7.3]

N **D.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.

[**730:**B.7.4]

N **D.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.

[**730:**B.7.5]

N **D.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. [**730:**B.7.6]

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. [**730:**B.7.6]

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. [**730:**B.7.6]

For more information, visit the web site for the Centers for Disease Control and Prevention, www.cdc.gov. [**730:**B.7.6]

N **D.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. [**730:**B.8]

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 easier to obtain than weapons-grade uranium or plutonium. [**730:**B.8]

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. [**730:**B.8]

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. [**730:**B.8]

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. [**730:**B.8]

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. [**730:**B.8]

In general, potential targets include the following:

(1) Strategic missile sites and military bases
(2) Centers of government, such as Washington, DC, 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

[**730:**B.8]

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 with-

stand 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.

[**730:**B.8]

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. [**730:**B.8]

N **D.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 1609 km (1000 miles) of a high-altitude nuclear detonation could be affected. Battery-powered radios with short antennas generally would not be affected. [**730:**B.8.1]

Although an EMP is unlikely to harm most people, it could harm those with pacemakers or other implanted electronic devices. [**730:**B.8.1]

N **D.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.

[**730:**B.8.2]

N **D.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. Remem-

ber 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.

[**730:**B.8.3]

N **D.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.

[**730:**B.8.4]

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.

[**730:**B.8.4]

N **D.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.

[**730:**B.9]

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."

[**730:**B.9]

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.

[**730:**B.9]

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. [**730:**B.9]

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. [**730:**B.9]

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.

[**730:**B.9]

N Annex E Critical Infrastructure Protection

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

N **E.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. [**730:**C.1]

N **E.2 Chemical Facilities.**

N **E.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. [**730:**C.2.1]

N **E.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. [**730:**C.2.2]

N **E.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. [**730:**C.2.3]

N **E.2.4** Some chemicals can be particularly attractive targets because of the potential for greater consequences. [**730:**C.2.4]

N **E.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. [**730:**C.2.5]

N **E.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. [**730:**C.2.6]

N **E.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. [**730:**C.2.6.1]

N **E.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. [**730:**C.2.6.2]

N **E.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

[**730:**C.2.6.3]

N **E.2.6.4** Consideration should be given to protecting equipment containing hazardous chemicals against sabotage and accidents. [**730:**C.2.6.4]

N **E.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. [**730:**C.2.6.5]

N **E.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. [**730:**C.2.6.6]

N E.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. [**730:**C.2.6.7]

N E.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. [**730:**C.2.6.8]

N E.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.

[**730:**C.2.7]

N E.3 Water Treatment Facilities.

N E.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. [**730:**C.3.1]

N E.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. [**730:**C.3.1.1]

N E.3.1.2 Supply interruptions can also occur as an indirect result of contamination. [**730:**C.3.1.2]

N E.3.2 Water treatment facilities should comply with the procedures in E.3.2.1 through E.3.2.3. [**730:**C.3.2]

N E.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. [**730:**C.3.2.1]

N E.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. [**730:**C.3.2.2]

N E.3.2.3 Water authorities should reasonably ensure that fire hydrants and other entry points to the distribution system are tamper resistant. [**730:**C.3.2.3]

N E.4 Power Distribution Facilities. See *NFPA 70*. [**730:**C.4]

N Annex F Special Events

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

N F.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. [**730:**D.1]

N F.2 Security Plan and Security Vulnerability Assessment. A security plan, as described in NFPA 730 Chapter 6, should be developed. A security vulnerability assessment (SVA), as detailed in NFPA 730 Chapter 5, should be conducted. [**730:**D.2]

N F.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. [**730:**D.3]

N F.3.1 Security Committee.

N F.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. [**730:**D.3.1.1]

N F.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. [**730:**D.3.1.2]

N F.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. [**730:**D.3.1.3]

N F.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." [**730:**D.3.2]

N **F.3.3 Event Planning Measures.**

N **F.3.3.1 Personnel.**

N **F.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 NFPA 730 Chapter 6 for guidance on security personnel). [**730:**D.3.3.1.1]

N **F.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. [**730:**D.3.3.1.2]

N **F.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. [**730:**D.3.3.1.3]

N **F.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. [**730:**D.3.3.1.4]

N **F.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. [**730:**D.3.3.2]

N **F.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. [**730:**D.3.3.3]

N **F.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. [**730:**D.3.3.4]

N **F.3.3.5 Parking and Traffic Control.**

N **F.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. [**730:**D.3.3.5.1]

N **F.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. [**730:**D.3.3.5.2]

N **F.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. [**730:**D.3.3.5.3]

N **F.3.4 Ingress and Egress.**

N **F.3.4.1 General.**

N **F.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. [**730:**D.3.4.1.1]

N **F.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. [**730:**D.3.4.1.2]

N **F.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. [**730:**D.3.4.1.3]

N **F.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. [**730:**D.3.4.2]

N **F.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. [**730:**D.3.5]

N F.3.6 Other Considerations.

N F.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. [**730:**D.3.6.1]

N F.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. [**730:**D.3.6.2]

N F.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.

[**730:**D.4]

N F.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.

[**730:**D.5]

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 pre-employment screening cannot be overemphasized. [**730:**D.5]

N Annex G Special Topics

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

N G.1 General. Annex G is a collection of information that appeared in the first edition of NFPA 730 and is provided here for informational purposes only. [**730:**E.1]

N G.2 Exterior.

N G.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. [**730:**E.2.1]

N G.2.1.1 Concrete Planters. Concrete planters and bollards (discussed in G.2.1.2) are being used to protect the White House and other federal government buildings in Washington, DC. [**730:**E.2.1.1]

N G.2.1.1.1 In testing performed by the U.S. Army Corps of Engineers, a concrete planter, designed as shown in Figure G.2.1.1.1, was capable of stopping a 6804 kg (15,000 lb) vehicle traveling at 22.4 m/sec (50 mph). This planter should also stop a 2041.2 kg (4500 lb) vehicle traveling at 13.4 m/sec (30 mph), which is approximately the weight of a pickup truck and the likely speed it could attain in a short distance. (Specific infor-

mation on the design of a planter to stop such a vehicle was not provided in the U.S. Army Field Manual 19-30). [**730:**E.2.1.1.1]

N **G.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 1.21 m (4 ft) apart. [**730:**E.2.1.1.2]

N **G.2.1.2 Bollards.** For narrower sidewalks or as an alternative to planters, bollards can be used. Bollards are 1.82 m (6 ft) to 2.13 m (7 ft) cylinders of steel, usually filled with concrete, and partially buried, leaving a 0.91 m to 1.21 m (3 ft to 4 ft) section above ground. [**730:**E.2.1.2]

N **G.2.1.2.1** In testing performed by the U.S. Army Corps of Engineers, concrete-filled steel bollards *(see Figure G.2.1.2.1)* spaced 1.21 m (4 ft) apart, at a height of 0.91 m (3 ft) above grade, and buried in concrete to a depth of 1.21 m (4 ft) stopped a 2041 kg (4500 lb) vehicle traveling at 13.4 m/sec (30 mph). The concrete portion of the bollard had a diameter of 203.2 mm (8 in.), and the steel pipe was 12.7 mm (½ in.) thick. [**730:**E.2.1.2.1]

N **G.2.1.2.2** When the bollards were reinforced with a 304.8 mm (12 in.) "C" channel *(see Figure G.2.1.2.2)*, the design was capable of stopping a 6804 kg (15,000 lb) vehicle traveling at 22.4 m/sec (50 mph). [**730:**E.2.1.2.2]

N **G.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 G.2.1.3)*, was capable of stopping a 1814 kg (4000 lb) vehicle traveling at 22.4 m/sec (50 mph).

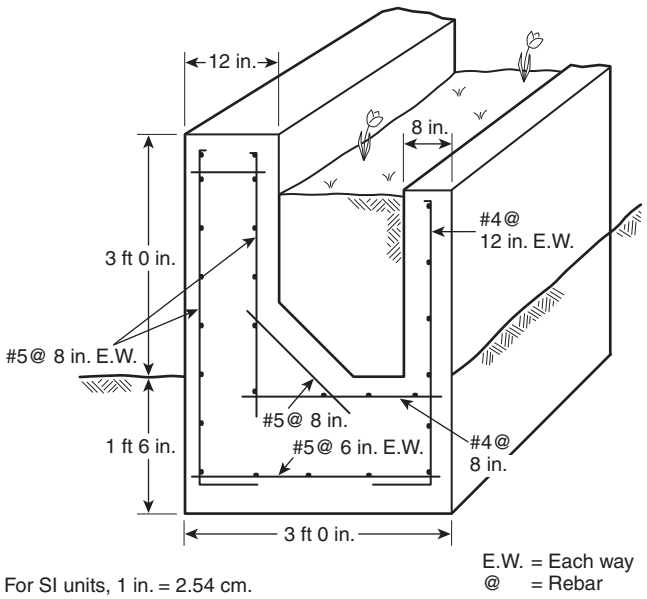


FIGURE G.2.1.1.1 Concrete Planter. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*** **[730:Figure E.2.1.1.1]**

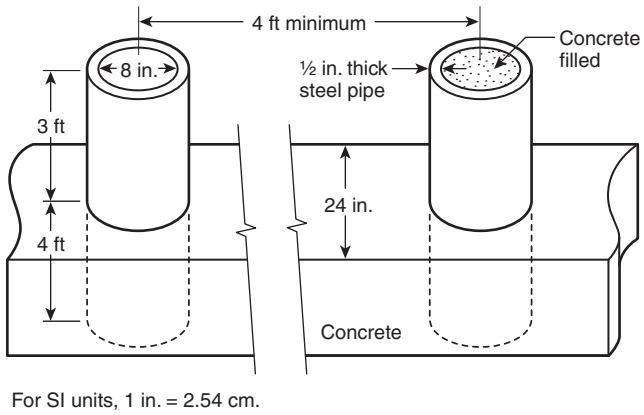


FIGURE G.2.1.2.1 Concrete-Filled Bollard. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*** **[730:Figure E.2.1.2.1]**

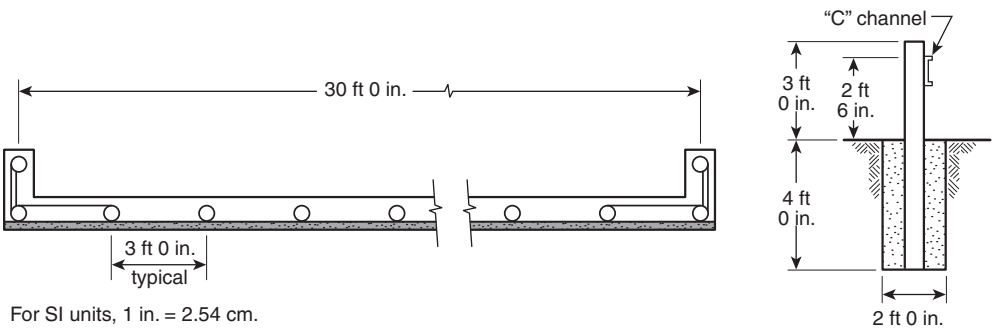
Jersey barriers can be used in place of planters and bollards where aesthetics are not of concern. [**730:**E.2.1.3]

N **G.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. [**730:**E.2.2]

N **G.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. [**730:**E.2.2.1]

N **G.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. NFPA 730, 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. [**730:**E.2.2.2]

N **G.2.2.2.1 Height.** Chain-link fences are available in heights ranging from 1.21 m (4 ft) for residential application to 3.65 m (12 ft) or more for use in prison facilities. In industrial or commercial security applications, the minimum recommended height for a chain-link fence is 2.4 m (8 ft), including 2.13 m (7 ft) of fabric (the chain-link material) and a top guard (discussed in NFPA 730, 6.4.3.7) of approximately 0.3 m (1 ft). However, some fence manufacturers recommend that the fence height be 2.74 m (9 ft), at which height the top of the fence is out of standing reach of most intruders. [**730:**E.2.2.2.1]



For SI units, 1 in. = 2.54 cm.

FIGURE G.2.1.2.2 Concrete-Filled Steel Bollard with 12 in. "C" Channel. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*** **[730:Figure E.2.1.2.2]**

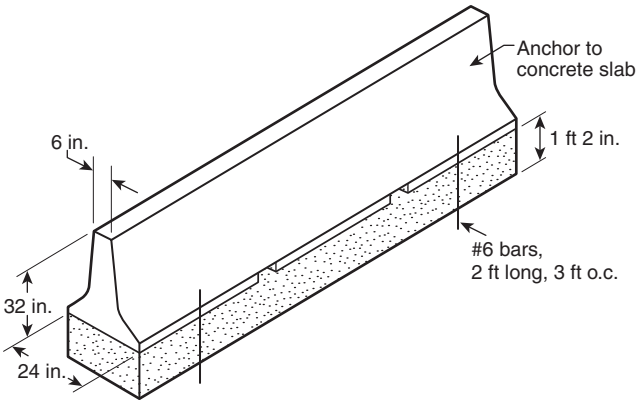
N **G.2.2.2.2 Posts.** The posts for a chain-link fence include terminal (end, corner, and gate) posts and line posts. For a fence with 2.13 m (7 ft) high fabric, the posts should be set in concrete at a minimum depth of 0.91 m (36 in.) and the surface of the concrete crowned to shed water. The posts should be set an additional 76.2 mm (3 in.) deeper for each 304.8 mm (12 in.) increase in the height of the fence. The diameter of the hole for a terminal post should be at least 304.8 mm (12 in.) and 228.6 mm (9 in.) 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 3.04 m (10 ft), measured from center to center between terminal posts. End posts should be set within 50.8 mm (2 in.) of building walls. [**730:**E.2.2.2.2]

N **G.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. [**730:**E.2.2.2.3]

N **G.2.2.3 Rails and Tension Wires.**

N **G.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 5.48 m (18 ft) lengths, is joined with connectors that allow for expansion and contraction. On fences 3.65 m (12 ft) and more in height, a center rail is necessary. [**730:**E.2.2.3.1]

N **G.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 0.3 m (1 ft) of the top of the fabric, and be securely attached to the terminal posts. A bottom tension wire that is within the bottom 152.4 mm (6 in.) of the fabric should also be provided. Some fences have a bottom rail in place of the bottom tension wire. [**730:**E.2.2.3.2]



For SI units, 1 in. = 2.54 cm.

FIGURE G.2.1.3 Jersey Barrier. ***(Source: U.S. Army Corps of Engineers, Field Manual 19-30.)*** **[730:Figure E.2.1.3]**

N **G.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 50.8 mm (2 in.) per side. [**730:**E.2.2.4]

N **G.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 6.35 mm (¼ in.) 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. [**730:**E.2.2.4.1]

N **G.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 1.82 m (6 ft) in height and in residential applications, both the top and bottom selvages should be knuckled, also for safety reasons. [**730:**E.2.2.4.2]

N **G.2.2.4.3** The fabric should be stretched taut and securely fastened to the posts at 381 mm (15 in.) intervals. The top edge of the fabric should be fastened to the top rail or top tension wire at intervals not exceeding 0.6 m (2 ft) and the bottom

edge of the wire to the bottom rail or bottom tension wire at intervals not exceeding 0.6 m (2 ft). [**730:**E.2.2.4.3]

N **G.2.2.4.4** The bottom of the fabric should extend to within 50.8 mm (2 in.) of hard ground or paving. On soft ground, the fabric should extend below the surface of the soil, or U-shaped stakes, approximately 0.6 m (2 ft) in length, can be driven into the ground to secure the fabric. Culverts, troughs, or other openings that are larger than 61,935.36 mm^2 (96 $in.^2$) in area should be protected by fencing or iron grills to prevent unauthorized entry while allowing for proper drainage. [**730:**E.2.2.4.4]

N **G.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 457 mm (18 in.) in length, attached to the fence posts either vertically or at an angle of approximately 45 degrees. [**730:**E.2.2.5]

N **G.2.2.5.1** When the top guard is angled, the arms, or outriggers, should be of sufficient strength to withstand a weight of 113.4 kg (250 lb) applied at the outer strand of barbed wire. The top strand of barbed wire should be at a height 0.3 m (1 ft) vertically above the top of the fabric, with the other wires spaced uniformly along the arm. [**730:**E.2.2.5.1]

N **G.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. [**730:**E.2.2.5.2]

N **G.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. [**730:**E.2.2.5.3]

N **G.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, 0.63 mm (0.025 in.) thick and 25.4 mm (1 in.) or 31.75 mm (1 1/4 in.) wide, with needle-sharp barbs that are spaced on 101 mm (4 in.) 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 2.13 m (7 ft) to avoid the possibility of contact with pedestrian traffic. Barbed tape should never be used at heights below 2.13 m (7 ft). [**730:**E.2.2.5.4]

N **G.2.2.6 Gates.**

N **G.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. [**730:**E.2.2.6.1]

N **G.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 381 mm (15 in.) intervals. The gate should be mounted so that it cannot be lifted off its hinges. The bottom of the gate should be within 50.8 mm (2 in.) of the ground. [**730:**E.2.2.6.2]

N **G.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 0.91 m (3 ft) 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 2.13 m (7 ft) 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. [**730:**E.2.2.6.3]

N **G.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. [**730:**E.2.2.6.4]

N **G.2.2.7 Locks.**

N **G.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. [**730:**E.2.2.7.1]

N **G.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. [**730:**E.2.2.7.2]

N **G.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. [**730:**E.2.3]

N **G.2.3.1 General.**

N **G.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. [**730:**E.2.3.1.1]

N **G.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. [**730:**E.2.3.1.2]

N **G.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. [**730:**E.2.3.2]

N **G.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). [**730:**E.2.3.2.1]

N **G.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. [**730:**E.2.3.2.2]

N **G.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. [**730:**E.2.3.3]

N **G.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. [**730:**E.2.3.3.1]

N **G.2.3.3.2 Pressure Systems.** Pressure systems use two liquid-filled hoses buried about 152.4 mm (6 in.) deep and 1.52 m (5 ft) apart. Each pair of hoses, usually up to 99.06 m (325 ft) 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. [**730:**E.2.3.3.2]

N **G.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. [**730:**E.2.3.3.3]

N **G.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. [**730:**E.2.3.4]

N **G.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. [**730:**E.2.3.4.1]

N **G.2.3.4.1.1 Outdoor Microwave Systems.** These systems are either monostatic, in which 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 1.82 m to 9.75 m (6 ft to 32 ft) wide by 1.52 m to 3.96 m (5 ft to 13 ft) high over ranges up to 198.12 m (650 ft). [**730:**E.2.3.4.1.1]

N **G.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. [**730:**E.2.3.4.1.2]

N **G.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. [**730:**E.2.3.4.2]

N **G.2.4 Lighting.**

N **G.2.4.1 Lighting Terms.**

N **G.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). [**730:**E.2.4.1.1]

N **G.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. [**730:**E.2.4.1.2]

N **G.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 lux (lx) (1 lm/m^2) or footcandles (fc) (1 lm/ft^2) . [**730:**E.2.4.1.3]

N **G.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 meter (cd/m^2) [square foot (cd/ft^2)]. [**730:**E.2.4.1.4]

N **G.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. [**730:**E.2.4.2]

N **G.2.4.2.1 Incandescent Lamps.**

N **G.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. [**730:**E.2.4.2.1.1]

N **G.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. [**730:**E.2.4.2.1.2]

N **G.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. [**730:**E.2.4.2.2]

N **G.2.4.2.3 High-Intensity Discharge (HID) Lamps.** HID lamps include mercury vapor, metal halide, and high-pressure sodium. [**730:**E.2.4.2.3]

N **G.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. [**730:**E.2.4.2.3.1]

N **G.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. [**730:**E.2.4.2.3.2]

N **G.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. [**730:**E.2.4.2.3.3]

N **G.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. [**730:**E.2.4.2.3.4]

N **G.2.4.3 Warm-Up and Restrike Times.** Table G.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. [**730:**E.2.4.3]

N **G.2.4.4 Floodlight Luminaires.**

N **G.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. [**730:**E.2.4.4.1]

N **G.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. [**730:**E.2.4.4.2]

N **G.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. [**730:**E.2.4.4.3]

N **G.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. [**730:**E.2.4.4.4]

N **G.2.4.4.5 Street Light Luminaires.**

N **G.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. [**730:**E.2.4.4.5.1]

Table G.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

[**730:**Table E.2.4.3]

N **G.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. [**730:**E.2.4.4.5.2]

N **G.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. [**730:**E.2.4.4.5.3]

N **G.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. [**730:**E.2.4.4.6]

N **G.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 304.8 mm (12 in.) to 609.6 mm (24 in.), and the wattage of the lamp, which can range from 250 watts to 3000 watts. [**730:**E.2.4.4.7]

N **G.3 Portals.**

N **G.3.1 Doors.**

N **G.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. [**730:**E.3.1.1]

N **G.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. [**730:**E.3.1.2]

N **G.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. [**730:**E.3.1.3]

N **G.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. [**730:**E.3.1.4]

N **G.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. [**730:**E.3.1.5]

N **G.3.1.6** Other security measures that should be considered for doors are described in G.3.1.6.1 through G.3.1.6.9. [**730:**E.3.1.6]

N **G.3.1.6.1** Assuming exterior doors are of solid construction, they should be equipped with a good deadbolt with at least a 25.4 mm (1 in.) throw lock. [**730:**E.3.1.6.1]

N **G.3.1.6.2** Exterior doors must fit tightly in the frame with no more than 3.175 mm (⅛ in.) 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. [**730:**E.3.1.6.2]

N **G.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. [**730:**E.3.1.6.3]

N **G.3.1.6.4** If an exterior door has a glass panel within 1016 mm (40 in.) 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. [**730:**E.3.1.6.4]

N **G.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. [**730:**E.3.1.6.5]

N **G.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. [**730:**E.3.1.6.6]

N **G.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. [**730:**E.3.1.6.7]

N **G.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. [**730:**E.3.1.6.8]

N **G.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. [**730:**E.3.1.6.9]

N **G.3.1.7** Specialty doors include those described in G.3.1.7.1 through G.3.1.7.4. [**730:**E.3.1.7]

N **G.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. [**730:**E.3.1.7.1]

N **G.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. [**730:**E.3.1.7.2]

N **G.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. [**730:**E.3.1.7.3]

N **G.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. [**730:**E.3.1.7.4]

N **G.3.2 Windows.**

N **G.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. [**730:**E.3.2.1]

N **G.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. [**730:**E.3.2.2]

N **G.3.2.3** Bars should be steel of at least 12.7 mm (½ in.) in least dimension and spaced 152.4 mm (6 in.) apart on center. If a grille is used, the material should be at least No. 9 gauge 50.8 mm (2 in.) square mesh. Bars and grilles must be securely fastened to the window frame so they cannot be pried loose. [**730:**E.3.2.3]

N **G.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. [**730:**E.3.2.4]

N **G.3.3 Ironwork.** Ironwork, such as crossbars, gates, and screens, are used on doors and windows to protect against unauthorized intrusion. [**730:**E.3.3]

N **G.3.3.1 Crossbars.**

N **G.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. [**730:**E.3.3.1.1]

N **G.3.3.1.2** A steel crossbar should have cross-sectional dimensions of at least 44.45 mm × 12.7 mm (1¾ in. × ½ in.). 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. [**730:**E.3.3.1.2]

N **G.3.3.2 Flat or Round Iron Bars.**

N **G.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 19.05 mm (¾ in.) diameter, while flat bars are usually 38.1 mm × 9.52 mm (1½ in. × ⅜ in.). 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 127 mm (5 in.) apart and horizontal bars 609.6 mm (24 in.) or less. [**730:**E.3.3.2.1]

N **G.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. [**730:**E.3.3.2.2]

N **G.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. [**730:**E.3.3.2.3]

N **G.3.3.2.4** Iron gates are used as security devices on entrances to stores and mercantile occupancies. Round bars should be at least 38.1 mm (1½ in.) diameter, while flat bars should be at least 38.1 mm × 9.52 mm (1½ in. × ⅜ in.); vertical bars should be spaced not more than 127 mm (5 in.) apart. The lock used to secure the gate should be of the deadbolt type, with a minimum bolt throw of 25.4 mm (1 in.) 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. [**730:**E.3.3.2.4]

N **G.3.3.3 No. 18 Gauge Sheet Steel Panel.**

N **G.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. [**730:**E.3.3.3.1]

N **G.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 152.4 mm (6 in.) 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. [**730:**E.3.3.3.2]

N **G.3.3.4 No. 8 Gauge Wire Mesh Screening.**

N **G.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 1.39 m^2 (15 ft^2)] should have stiffener bars welded along their centers. [**730:**E.3.3.4.1]

N **G.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. [**730:**E.3.3.4.2]

N **G.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. [**730:**E.3.3.5]

N **G.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. [**730:**E.3.4]

N **G.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. [**730:**E.3.4.1]

N **G.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. [**730:**E.3.4.1.1]

N **G.3.4.1.1.1 Laminated Glass.** This material consists of two sections of 3.175 mm (⅛ in.) thick glass bonded to an interlayer of 1.52 mm (0.060 in.) or thicker polyvinyl butyral (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 7.14 mm (9/32 in.) and is designed to fit the nominal 6.35 mm (1/4 in.) frame of a show window. [**730:**E.3.4.1.1.1]

N **G.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 22.22 mm (7/8 in.) thickness. [**730:**E.3.4.1.1.2]

N **G.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 3.175 mm (1/8 in.) 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. [**730:**E.3.4.1.1.3]

N **G.3.4.1.2 Application of UL-Listed Burglary-Resisting Glazing Materials.**

N **G.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. [**730:**E.3.4.1.2.1]

N **G.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. [**730:**E.3.4.1.2.2]

N **G.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. [**730:**E.3.4.1.2.3]

N **G.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. [**730:**E.3.4.1.2.4]

N **G.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. [**730:**E.3.4.1.2.5]

N **G.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. [**730:**E.3.4.1.2.6]

N **G.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. [**730:**E.3.4.1.2.7]

N **G.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. [**730:**E.3.4.1.2.8]

N **G.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. [**730:**E.3.4.1.2.9]

N **G.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 9.52 mm (3/8 in.) 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. [**730:**E.3.4.1.2.10]

N **G.3.4.2 Bullet-Resisting Glazing Materials.** UL 752, *Standard for Bullet-Resisting Equipment*, 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. [**730:**E.3.4.2]

N **G.3.4.2.1 UL-Listed Bullet-Resisting Glazing Materials.**

N **G.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. [**730:**E.3.4.2.1.1]

N **(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 30.16 mm ($1\frac{3}{16}$ in.) upward to provide protection at all ballistic levels. [**730:**E.3.4.2.1.1(A)]

N **(B) Acrylics.** These materials are usually monolithic in structure and available in thicknesses ranging from 31.75 mm to 44.45 mm ($1\frac{1}{4}$ in. to $1\frac{3}{4}$ in.). They provide protection only at the handgun levels and not in the high-power rifle category. [**730:**E.3.4.2.1.1(B)]

N **(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 19.05 mm to 44.45 mm ($\frac{3}{4}$ in. to $1\frac{3}{4}$ in.). They provide protection only at the handgun levels. [**730:**E.3.4.2.1.1(C)]

N **(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 22.86 mm (0.9 in.) to more than 50.8 mm (2 in.), 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. [**730:**E.3.4.2.1.1(D)]

N **G.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. [**730:**E.3.4.2.1.2]

N **G.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. [**730:**E.3.4.2.2]

N **G.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. [**730:**E.3.4.2.2.1]

N **G.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. [**730:**E.3.4.2.2.2]

N **G.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. [**730:**E.3.4.2.2.3]

N **G.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. [**730:**E.3.4.2.3]

N **G.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. [**730:**E.3.4.2.3.1]

N **G.3.4.2.3.2** ASTM ballistic tests are performed on 304.8 mm × 304.8 mm (12 in. × 12 in.) or 755.65 mm × 755.65 mm (29.75 in. × 29.75 in.) test samples at a distance of 7.62 m (25 ft) from the weapon. Spall is detected by perforation of an aluminum foil sheet mounted 152.4 mm (6 in.) 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 a 203.2 mm (8 in.) diameter circle and at 0 degree angle of obliquity. [**730:**E.3.4.2.3.2]

N **G.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. [**730:**E.3.4.2.3.3]

N **G.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. [**730:**E.3.4.2.3.4]

N **G.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. [**730:**E.3.4.2.4]

N **G.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. [**730:**E.3.4.2.4.1]

N **G.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 2.13 m (7 ft) 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. [**730:**E.3.4.2.4.2]

N **(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. [**730:**E.3.4.2.4.2(A)]

N **(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. [**730:**E.3.4.2.4.2(B)]

N **(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. [**730:**E.3.4.2.4.2(C)]

N **(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 15.87 mm (⅝ in.) 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. [**730:**E.3.4.2.4.2(D)]

N **(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. [**730:**E.3.4.2.4.2(E)]

N **(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. [**730:**E.3.4.2.4.2(F)]

N **(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. [**730:**E.3.4.2.4.2(G)]

N **G.3.5 Locking Hardware.**

N **G.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. [**730:**E.3.5.1]

N **G.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. [**730:**E.3.5.2]

N **G.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.