

NFPA® 731

Standard for the Installation of Electronic Premises Security Systems

2015 Edition



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

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA STANDARDS

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

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

In issuing and making NFPA Standards available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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

REMINDER: UPDATING OF NFPA STANDARDS

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

In order to determine whether an NFPA Standard has been amended through the issuance of Tentative Interim Amendments or corrected by Errata, visit the Document Information Pages on NFPA’s website. The Document Information Pages provide up-to-date, document specific information including any issued Tentative Interim Amendments and Errata.

To access the Document Information Page for a specific NFPA Standard, go to <http://www.nfpa.org/docinfo> to choose from the list of NFPA Standards or use the search feature on the right to select the NFPA Standard number (e.g., NFPA 101). In addition to posting all existing Tentative Interim Amendments and Errata, the Document Information Page also includes the option to sign-up for an “Alert” feature to receive an email notification when new updates and other information are posted regarding the document.

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Standards

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

Interpretations of NFPA Standards

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

Patents

The NFPA does not take any position with respect to the validity of any patent rights referenced in, related to, or asserted in connection with an NFPA Standard. The users of NFPA Standards bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Standards.

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

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

Law and Regulations

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

Copyrights

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

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

For Further Information

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

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

Copyright © 2014 National Fire Protection Association®. All Rights Reserved.

NFPA® 731

Standard for the

Installation of Electronic Premises Security Systems

2015 Edition

This edition of NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, was prepared by the Technical Committee on Premises Security and acted on by NFPA at its June Association Technical Meeting held June 9–12, 2014, in Las Vegas, NV. It was issued by the Standards Council on August 14, 2014, with an effective date of September 3, 2014, and supersedes all previous editions.

This edition of NFPA 731 was approved as an American National Standard on September 3, 2014.

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 has been revised to update dates of many referenced publications. The requirements for low-power radio (wireless) systems have also been updated. Requirements have been clarified relative to the provisions of the security vulnerability assessment versus the risk assessment. Chapter 10 has been 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.



Technical Committee on Premises Security

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

David Abbott, Ohio State University Medical Center, OH [U]
Randall I. Atlas, Atlas Safety & Security Design, Inc., FL [IM]
Paul H. Aube, Dessau, Canada [SE]
George Bish, Secure Watch Security, NC [IM]
 Rep. Electronic Security Association
Josh D. Brown, The Fauquier Bank, VA [U]
 Rep. Virginia Crime Prevention Association/National Crime Prevention Council
Louis Chavez, UL LLC, IL [RT]
David S. Collins, The Preview Group, Inc., OH [SE]
 Rep. American Institute of Architects
David A. Dagenais, Wentworth-Douglass Hospital, NH [U]
 Rep. NFPA Health Care Section
Michael D. DeVore, State Farm Insurance Company, IL [I]
 Rep. NFPA Industrial Fire Protection Section
Jon M. Evenson, The RJA Group, Inc., IL [SE]
Daniel P. Finnegan, Siemens Industry, Inc., NJ [M]
Louis T. Fiore, L. T. Fiore, Inc., NJ [IM]
 Rep. Professional Alarm Services Organizations of North America
Charles E. Hahl, The Protection Engineering Group, Inc., VA [SE]

Charles B. King, III, U.S. Department of Homeland Security, VA [E]
Jerry D. Loghry, EMC Insurance Companies, IA [I]
Stan J. Martin, Security Industry Alarm Coalition, Inc., TX [IM]
 Rep. Central Station Alarm Association
Anthony Mucci, Tyco Integrated Security, FL [M]
James Murphy, Vector Security Inc., PA [IM]
Isaac I. Papier, Honeywell, Inc., IL [M]
 Rep. National Electrical Manufacturers Association
Michael C. Peele, Georgetown University, DC [U]
James P. Simpson, National Joint Apprentice & Training Committee, MN [L]
 Rep. International Brotherhood of Electrical Workers
Tom G. Smith, Oklahoma City, OK [IM]
 Rep. National Electrical Contractors Association
Robert H. Stagg, Guardsmark, Inc., NC [SE]
Barry Stanford, AEG, CA [U]
Bill H. Strother, Weingarten Realty Management Co., TX [U]
 Rep. International Council of Shopping Centers
Michael Tierney, Kellen Company, CT [M]
 Rep. Builders Hardware Manufacturers Association
Lionel F. Weeks, Sinai Hospital of Baltimore, MD [U]
 Rep. International Assn. for Healthcare Security & Safety

Alternates

Shane M. Clary, Bay Alarm Company, CA [IM]
 (Alt. to S. J. Martin)
Dennis J. Delfosse, The RJA Group, Inc., CA [SE]
 (Alt. to J. M. Evenson)
Mark M. Hankewycz, The Protection Engineering Group, PC, VA [SE]
 (Alt. to C. E. Hahl)
Patrick D. Harris, National Crime Prevention Association, VA [U]
 (Alt. to J. D. Brown)
Thomas R. Janicak, Ceco Door Products, IL [M]
 (Alt. to M. Tierney)

Perry Levine, Siemens Industry, Inc., FL [M]
 (Alt. to D. P. Finnegan)
Kevin Patterson, Bosch Security Systems, NY [M]
 (Alt. to I. I. Papier)
Rodger Reiswig, Tyco/SimplexGrinnell, FL [M]
 (Alt. to A. Mucci)
Steven A. Schmit, UL LLC, IL [RT]
 (Alt. to L. Chavez)
James W. Tosh, Puget Sound Electrical JATC, WA [L]
 (Alt. to J. P. Simpson)
Bryan G. Warren, Carolinas Healthcare System, NC [U]
 (Alt. to L. F. Weeks)
William F. Wayman, Jr., Hughes Associates, Inc., MD [SE]
 (Alt. to W. D. Moore)

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

Chapter 1 Administration	731- 4	7.4 Enclosures	731-17
1.1 Scope	731- 4	7.5 General Hardware and Mounts	731-17
1.2 Purpose	731- 4	7.6 Lens	731-17
1.3 Application	731- 4	7.7 Physical Conductors	731-17
1.4 Retroactivity	731- 4	7.8 Radio Frequency (RF). (Reserved)	731-17
1.5 Equivalency	731- 4		
1.6 Units and Formulas	731- 4	Chapter 8 Holdup, Duress, and Ambush Systems	731-17
Chapter 2 Referenced Publications	731- 5	8.1 General	731-17
2.1 General	731- 5	8.2 Holdup Alarm Systems	731-18
2.2 NFPA Publications	731- 5	8.3 Duress Alarm Systems	731-18
2.3 Other Publications	731- 5	8.4 Ambush Alarm Systems	731-18
2.4 References for Extracts in Mandatory Sections	731- 5	Chapter 9 Monitoring Stations	731-18
Chapter 3 Definitions	731- 5	9.1 Application	731-18
3.1 General	731- 5	9.2 Scope	731-19
3.2 NFPA Official Definitions	731- 5	9.3 Public Safety Agencies	731-19
3.3 General Definitions	731- 6	9.4 Proprietary Monitoring Stations	731-20
Chapter 4 Fundamentals	731- 8	9.5 Commercial Monitoring Stations	731-20
4.1 General	731- 8	9.6 Disposition of Signals	731-20
4.2 Equipment	731- 8	9.7 Transmission and Receiving Technologies	731-21
4.3 Personnel Qualifications	731- 8	9.8 Record Keeping and Recording	731-23
4.4 Power	731- 8	9.9 Testing and Maintenance Requirements for All Transmission Technologies	731-23
4.5 System Functions	731-10	Chapter 10 Testing and Inspections	731-23
4.6 Installation and Design	731-10	10.1 Application	731-23
4.7 Special Requirements for Low-Power Radio (Wireless) Systems	731-11	10.2 Impairments	731-23
4.8 Grounding	731-11	10.3 General Testing, Inspection, and Maintenance	731-23
4.9 Zoning and Annunciation	731-12	10.4 System Testing	731-24
4.10 Software Control	731-12	10.5 Inspection and Testing Frequency	731-28
4.11 Interconnected and Combination Systems	731-12	10.6 Records	731-28
4.12 Documentation and Training	731-12	Chapter 11 Asset Protection Systems	731-28
Chapter 5 Intrusion Detection Systems	731-13	11.1 General	731-28
5.1 General	731-13	11.2 Equipment	731-28
5.2 Exterior Space Detection Systems	731-13	11.3 Power Sources for Asset Protection Systems	731-28
5.3 Interior Detection Systems	731-14	11.4 Antenna	731-28
5.4 Vaults, Safes, ATMs, and Secured Containers	731-14	11.5 Tag	731-28
Chapter 6 Electronic Access Control Systems	731-15	11.6 Deactivators and Detachers	731-28
6.1 General	731-15	11.7 Testing	731-28
6.2 Administration Tools and Interface	731-16	Annex A Explanatory Material	731-29
6.3 Network Interface Device	731-16	Annex B Camera Specifications	731-48
Chapter 7 Video Surveillance Systems	731-16	Annex C Camera Selection	731-49
7.1 General	731-16	Annex D Informational References	731-50
7.2 Cameras	731-16	Index	731-52
7.3 Low-Level Lighting Conditions	731-17		

NFPA 731**Standard for the****Installation of Electronic Premises Security Systems****2015 Edition**

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

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

A reference in brackets [] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex D. 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 publications can be found in Chapter 2 and Annex D.

Chapter 1 Administration

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

1.2 Purpose.

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 electronic premises security systems.

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.

1.3.1 Electronic Premises Security Systems. Electronic 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, *National Electrical Code*.

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.

1.3.5.1 Electronic Hardware Components. This standard applies to new installations of electronic 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, an electronic 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. Electronic 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.

1.4.1 The provisions of this standard reflect situations and the state of the art 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 A device or system having materials or forms that differ from those detailed in this standard shall be permitted to be examined and tested according to the intent of the standard and, if found equivalent, shall be approved.

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

1.6 Units and Formulas.

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

1.6.2 Primary and Equivalent Values. If a value for a measurement as given in this standard is followed by an equivalent value in other units, the first stated value shall be regarded as the requirement. A given equivalent value might be approximate.

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

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this 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*, 2013 edition.

NFPA 70®, *National Electrical Code*®, 2014 edition.

NFPA 72®, *National Fire Alarm and Signaling Code*, 2013 edition.

NFPA 80, *Standard for Fire Doors and Other Opening Protectives*, 2013 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems*, 2013 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*, 2013 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 S1.4 with Amd. S1.4A-1985, *Specification for Sound Level Meters*, 1983, revised 2006.

2.3.2 SIA Publications. Security Industry Association, 635 Slaters Lane, Suite 110, Alexandria, VA 22314.

ANSI/SIA CP-01, *Control Panel Standard — Features for False Alarm Reduction*, 2007.

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

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

ANSI/UL 294, *Standard for Access Control System Units*, 1999, revised 2010.

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

ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, 2007, revised 2009.

ANSI/UL 636, *Standard for Holdup Alarm Units and Systems*, 1996, revised 2010.

ANSI/UL 639, *Standard for Safety for Intrusion-Detection Units*, 2007, revised 2012.

ANSI/UL 827, *Standard for Central-Station Alarm Services*, 2008, revised 2012.

ANSI/UL 1076, *Standard for Proprietary Burglar Alarm Units and Systems*, 1995, revised 2010.

ANSI/UL 2044, *Standard for Commercial Closed-Circuit Television Equipment*, 2008, revised 2010.

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

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*, 2013 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 monitoring or control of traffic through portals of a protected area by identifying the requestor and approving entrance or exit.

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.

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

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

3.3.5 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, 2013]

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 indicate a hostile situation.

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 Electronic Premises Security System. See 3.3.31.4.

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

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

3.3.14* Machine Readable Credential. A device or scheme containing some knowledge, an identifying credential, or a biometric identifier.

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

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

3.3.16.1* Commercial Monitoring Station. A monitoring station having ownership that is not the same ownership as the properties being monitored.

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

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

3.3.17 Point ID. The ability to identify, at the monitoring station, an intrusion detection device by address or zone number.

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

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

3.3.20* Prime Contractor. The entity contractually responsible for providing services to a subscriber as required by this standard.

3.3.21 Protective Wiring.

3.3.21.1 Fine Wire Lacing. Bare, hard-drawn, solid copper wire not larger than 24 AWG or film-coated solid copper wire not larger than 26 AWG or the equivalent applied to a door or similar surface in continuous parallel strips.

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

3.3.21.3 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 102 mm (4 in.).

3.3.22* Reader. A device that allows a machine readable credential to be entered into an access control system.

3.3.23 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, 2013]

3.3.24* 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.

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

3.3.26* Screens. A fully framed assembly of grooved-wood dowels or meshed screening that is intended to form a protective barrier over windows or on doors, and on which fine wire lacing is installed in parallel runs of opposite polarity at intervals not exceeding 102 mm (4 in.).

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

3.3.28 Signals.

3.3.28.1* Alarm Signals. A signal indicating an unauthorized event at a protected premises.

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

3.3.28.3 Trouble Signals. A signal indicating a fault in a monitored circuit or component.

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

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

3.3.31 System.

3.3.31.1* 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.

3.3.31.2* 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.

3.3.31.3 Duress Alarm System.

3.3.31.3.1 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.

3.3.31.3.2 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.

3.3.31.4 Electronic 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.

3.3.31.5 Holdup Alarm System.

3.3.31.5.1 Manual Holdup Alarm System. A system or portion thereof in which the initiation of a holdup signal depends solely on operation of manually operated hand or foot initiating devices installed within the working area.

3.3.31.5.2 Semi-automatic Holdup Alarm System. A system or portion thereof in which the initiation of a holdup signal does not depend solely on operation of manually operated hand or foot initiating devices installed within the working area.

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

3.3.31.7 Partition System. A part of one control unit that through software acts as a separate control unit.

3.3.32 Trap.

3.3.32.1* 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.

3.3.32.2 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.

3.3.32.3* 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.

3.3.33* Vault (as related to premises security). An enclosure of heavy, reinforced construction with walls, floor, roof, and door(s) designed and constructed to delay penetration.

3.3.34 Verification.

3.3.34.1 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.

3.3.34.2 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 an electronic 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.

3.3.34.3 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.

3.3.34.4 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.

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

4.1.2 When an electronic 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.

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

4.2.2* The electronic 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.

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 electronic 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.

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

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 electronic 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, National Electrical Code*.

4.4.1.2 Power supplies shall be reliable and of adequate capacity for the intended service.

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

- (1) Intrusion detection systems
- (2) Holdup, duress, and ambush systems

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 The primary supply shall have a high degree of reliability and adequate capacity for the intended service.

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

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

4.4.2.5 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.

4.4.2.6 An overcurrent protective device of suitable 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.



4.4.2.7 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

4.4.2.8 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 proper 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.

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

- (1) A storage battery dedicated to the electronic 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 electronic premises security system with 15 minutes of capacity under maximum alarm load
- (3) An emergency generating system as defined in *NFPA 70, National Electrical Code*, Article 700

4.4.3.5* Under maximum quiescent load (system functioning in a nonalarm condition), the secondary supply shall have sufficient capacity to operate an electronic premises security system for a minimum of 4 hours and, at the end of that period, shall be capable of operating all alarm-sounding devices for 15 minutes.

4.4.3.6 Operation of secondary power shall not affect the required performance of an electronic 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.

4.4.3.8 The secondary power supply shall automatically provide power to the electronic 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.

4.4.3.10 Storage batteries dedicated to the electronic premises security system or an uninterruptible power supply (UPS) arranged in accordance with the provisions of *NFPA 111, Standard*

on Stored Electrical Energy Emergency and Standby Power Systems, 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.

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, National Electrical Code*
- (2) Not adversely affected by battery gases
- (3) In accordance with the requirements of *NFPA 70, National Electrical Code*, Article 480

4.4.4.4 Cells shall be insulated against grounds and crosses and be mounted securely in such a manner so as not to be subject to mechanical injury by the following means:

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

4.4.4.5 Battery racks shall be protected against corrosion.

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

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

4.4.4.8 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

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

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

4.4.4.11 Supervision means appropriate for the batteries and charger employed shall be provided to detect a failure of battery charging and initiate a trouble signal in accordance with 5.1.1.1.

4.4.5 Engine-Driven Generator Installation. The installation of engine-driven generators shall conform to the provisions of

NFPA 70, National Electrical Code, Article 700, and NFPA 110, Standard for Emergency and Standby Power Systems.

4.5 System Functions.

4.5.1 Electronic premises security system functions shall be permitted to be performed automatically.

4.5.2* The performance of electronic 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.

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

4.5.4 Electronic 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.

4.6.1.2* The site shall be inspected for environmental factors that affect the operation of the electronic 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 to normal.

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, National Electrical Code*.

4.6.3 Wiring.

4.6.3.1 The installation of all wiring, cable, and equipment shall be performed in a workmanlike manner in accordance with *NFPA 70, National Electrical Code*, and specifically with 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, National Electrical Code, Article 770*.

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

4.6.3.4* Unless specifically allowed by the manufacturer's wiring specifications, low-voltage electronic premises security system wiring shall be spaced at least 51 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* Electronic premises security system wiring and cables shall be of the appropriate gauge, strands, insulation, and electrical properties as specified by the equipment manufacturer.

4.6.3.6 Connections of conductors to terminal parts shall ensure a good 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 proper 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, National Electrical Code*.

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 non-alarm 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.

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

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.

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.

Exception: Until the expiration date for this exception of June 30, 2013, the time period for a low-power radio transmitter with only a single, connected alarm-initiating device shall be permitted to be increased to four times the minimum time interval permitted for a 1-second transmission up to the following:

- (1) Four hours maximum for a transmitter serving a single initiating device
- (2) Four hours maximum for a retransmission device (repeater) where disabling of the repeater or its transmission does not prevent the receipt of signals at the receiver/control unit from any initiating device transmitter

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, National Electrical Code*.

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 an electronic 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 acceptable to 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.

4.11 Interconnected and Combination Systems.

4.11.1 General.

4.11.1.1 Electronic 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 Electronic premises security system components shall be permitted to share control equipment or be able to operate as stand-alone 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 5.1.2.

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 an electronic 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.

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

4.11.3.2 To maintain the integrity of electronic 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 electronic premises security system.

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 electronic 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.

4.12.2* Documentation.

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 electronic premises security system
- (5) Name and contact telephone number of the organization monitoring the electronic 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* The user training shall be documented and maintained for 1 year, with the system documentation made available to the AHJ upon request.

Chapter 5 Intrusion Detection Systems

5.1 General.

5.1.1 Interconnecting Control Units.

5.1.1.1 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.

5.1.1.2 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

5.1.2 Monitoring Integrity of Conductors.

5.1.2.1 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.

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

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

5.1.2.2* 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.

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

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

5.1.3 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

5.1.4 Entry/Exit Delay.

5.1.4.1 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.

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

5.1.4.3 The entry time shall not exceed 240 seconds.

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

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

5.1.5* Installation Requirements.

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

5.1.5.2 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.

5.2.1.1 Photoelectric detector units shall be in compliance with applicable standards, such as ANSI/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.

5.2.2.1 Motion detection units shall be in compliance with applicable standards, such as ANSI/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.

5.2.3.1 Exterior structure detectors shall be in compliance with applicable standards, such as ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, and ANSI/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.

5.2.4.1 Exterior buried detectors shall be in compliance with applicable standards, such as ANSI/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.

5.3.3.1.1 Contacts. Contacts shall be in compliance with applicable standards such as ANSI/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.

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

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

5.3.3.1.6 Glass Break Sensors.

5.3.3.1.6.1 Glass break sensors shall be in compliance with applicable standards, such as ANSI/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

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

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

5.3.3.1.9 Motion Detection.

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

5.3.3.1.9.2 Motion detectors shall be used only in a suitable environment and for an opening or area that is suitable.

5.3.3.1.9.3 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.

5.3.4.1 Pressure-sensitive devices shall be in compliance with applicable standards, such as ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or ANSI/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.

5.4.2.1 Vault detection devices shall be in compliance with applicable standards, such as ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or ANSI/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.

5.4.3.1 Safe detection devices shall be in compliance with applicable standards, such as ANSI/UL 634, *Standard for Connectors and Switches for Use with Burglar-Alarm Systems*, or ANSI/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.

6.1.1 Equipment. Electronic access control equipment shall be in compliance with applicable standards, such as ANSI/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 for the portal action appropriate for its application.

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, *Standard for Fire Doors and Other Opening Protectives*.

6.1.5.4* Portals shall automatically secure 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 (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

6.1.6 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 can be opened greater than 152.4 mm (6 in.) before activating the sensor.

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.*)

7.2.1 All cameras shall be listed or labeled in compliance with applicable standards.

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.