

NFPA[®]

731

Standard for the
Installation of
Premises Security Systems

2020



This is a preview. [Click here to purchase the full publication.](#)

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.

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.

Copyright © 2019 National Fire Protection Association®. All Rights Reserved.

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)

Richard J. Roux, NFPA Staff Liaison

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)

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	7.10 Network Video Recorder (NVR)	731- 19
1.1 Scope	731- 4	Chapter 8 Holdup, Duress, and Ambush Systems	731- 19
1.2 Purpose	731- 4	8.1 General	731- 19
1.3 Application	731- 4	8.2 Holdup Alarm Systems	731- 19
1.4 Retroactivity	731- 4	8.3 Duress Alarm Systems	731- 19
1.5 Equivalency	731- 5	8.4 Ambush Alarm Systems	731- 20
1.6 Units and Formulas	731- 5	Chapter 9 Monitoring Stations	731- 20
Chapter 2 Referenced Publications	731- 5	9.1 Application	731- 20
2.1 General	731- 5	9.2 Scope	731- 20
2.2 NFPA Publications	731- 5	9.3 Public Safety Agencies	731- 20
2.3 Other Publications	731- 5	9.4 Proprietary Monitoring Stations	731- 21
2.4 References for Extracts in Mandatory Sections	731- 6	9.5 Central Monitoring Stations	731- 21
Chapter 3 Definitions	731- 6	9.6 Disposition of Signals	731- 22
3.1 General	731- 6	9.7 Transmission and Receiving Technologies	731- 23
3.2 NFPA Official Definitions	731- 6	9.8 Record Keeping and Recording	731- 24
3.3 General Definitions	731- 6	9.9 Testing and Maintenance Requirements for All Transmission Technologies	731- 24
Chapter 4 Fundamentals	731- 8	Chapter 10 Testing and Inspections	731- 24
4.1 General	731- 8	10.1 Application	731- 24
4.2 Equipment	731- 8	10.2 Impairments	731- 24
4.3 Personnel Qualifications	731- 8	10.3 General Testing, Inspection, and Maintenance	731- 24
4.4 Power	731- 8	10.4 System Testing	731- 25
4.5 System Functions	731- 10	10.5 Inspection and Testing Frequency	731- 25
4.6 Installation and Design	731- 10	10.6 Maintenance	731- 25
4.7 Special Requirements for Low-Power Radio (Wireless) Systems	731- 11	10.7 Records	731- 25
4.8 Grounding	731- 12	Chapter 11 Asset Protection Systems	731- 29
4.9 Zoning and Annunciation	731- 12	11.1 General	731- 29
4.10 Software Control	731- 12	11.2 Equipment	731- 29
4.11 Interconnected and Combination Systems	731- 12	11.3 Power Sources for Asset Protection Systems	731- 29
4.12 Documentation and Training	731- 13	11.4 Antenna	731- 29
Chapter 5 Intrusion Detection Systems	731- 13	11.5 Tag	731- 29
5.1 General	731- 13	11.6 Deactivators and Detachers	731- 29
5.2 Exterior Space Detection Systems	731- 14	11.7 Testing	731- 29
5.3 Interior Detection Systems	731- 14	Annex A Explanatory Material	731- 29
5.4 Vaults, Safes, ATMs, and Secured Containers	731- 15	Annex B Camera Specifications	731- 49
Chapter 6 Electronic Access Control Systems	731- 15	Annex C Camera Selection	731- 51
6.1 General	731- 15	Annex D Homeland Security Advisory System	731- 52
6.2 Administration Tools and Interface	731- 17	Annex E Critical Infrastructure Protection	731- 59
6.3 Network Interface Device	731- 17	Annex F Special Events	731- 60
Chapter 7 Video Surveillance Systems	731- 17	Annex G Special Topics	731- 62
7.1 General	731- 17	Annex H Informational References	731- 86
7.2 Cameras	731- 17	Index	731- 88
7.3 Low-Level Lighting Conditions	731- 18		
7.4 Enclosures	731- 18		
7.5 General Hardware and Mounts	731- 18		
7.6 Lens	731- 18		
7.7 Physical Conductors	731- 18		
7.8 Radio Frequency (RF). (Reserved)	731- 19		
7.9 Camera Imaging	731- 19		

NFPA 731

Standard for the

Installation of Premises Security Systems

2020 Edition

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

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

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

A reference in brackets [] following a section or paragraph indicates material that has been extracted from another NFPA document. 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

1.1 Scope. This standard covers the application, location, installation, performance, testing, and maintenance of 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 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.

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.

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.

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.

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.

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.

▲ **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.

▲ **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.

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.

3.3.15 Premises Security System. See 3.3.27.6.

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.

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

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.

△ 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.

△ 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.

△ 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.

△ 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.

△ 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.

△ 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.