First Revision No. 2-NFPA 730-2024 [Section No. 2.3]

2.3 Other Publications.

2.3.1 BHMA Publications.

Builders Hardware Manufacturers Association, 355 Lexington Avenue, 15th Floor, New York, NY 10017.

ANSI/BHMA A156 Series, *Categories of Builders Hardware, 2015 - 2023* .

ANSI/BHMA A156.3, *Exit Devices*, ~~2014~~ 2020 .

2.3.2 UL Publications.

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

UL 294, *Access Control System Units*, ~~2018~~ 2023 .

UL 305, *Panic Hardware*, 2012, revised 2022 .

UL 437, *Key Locks*, 2013, revised ~~2017~~ 2023 .

UL 768, *Combination Locks*, ~~2013~~ 2006 , revised ~~2018~~ 2023 .

UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, 2011, revised 2020.

UL 2802, *Performance Testing of Camera Image Quality*, 2013, revised ~~2019~~ 2020 .

UL 2058, *Outline of Investigation for High-Security Electronic Locks*, 2005, revised 2013 .

2.3.3 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Springfield, MA ~~2003~~ 2020 .

Submitter Information Verification

Committee: PMM-AAA
Submittal Date: Tue May 21 16:33:57 EDT 2024

Committee Statement

Committee Statement: References are updated in accordance with the Reference policy.
Response Message: FR-2-NFPA 730-2024

Public Input No. 17-NFPA 730-2023 [Section No. 2.3.2]

First Revision No. 3-NFPA 730-2024 [Section No. 2.4]

2.4 References for Extracts in Advisory Sections.

NFPA 72®, National Fire Alarm and Signaling Code®, ~~2022~~ 2025 edition.

NFPA 99, *Health Care Facilities Code,* 2024 edition.

NFPA 731, *Standard for the Installation of Premises Security Systems,* ~~2023~~ 2026 edition.

~~*NFPA 5000* ® ; *Building Construction and Safety Code* ® , 2021 edition.~~

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue May 21 16:37:45 EDT 2024

Committee Statement

Committee Statement: This revision updates extracted text in accordance with the Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document. The extract is changed from NFPA 5000 to NFPA 99 to reference the base document as NFPA 5000 extracts the requirements from NFPA 99.

Response Message: FR-3-NFPA 730-2024

First Revision No. 4-NFPA 730-2024 [Section No. 3.3.14.2]

3.3.14.2* Health Care Facilities.

Buildings, portions of buildings, or mobile enclosures in which human medical, dental, psychiatric, nursing, obstetrical, or surgical care is provided. [~~**5000**~~ **99** ,~~2021~~ 2024]

A.3.3.14.2 Health Care Facilities.

Health care facilities include, but are not limited to, hospitals, nursing homes, limited care facilities, clinics, medical and dental offices, and ambulatory health care centers, whether permanent or movable. This definition applies to normal, regular operations and does not pertain to facilities during declared local or national disasters. A health care facility is not a type of occupancy classification as defined by NFPA 101. Therefore, the term *health care facility* should not be confused with the term *health care occupancy*. All health care occupancies (and ambulatory health care occupancies) are considered health care facilities; however, not all health care facilities are considered health care occupancies, as health care facilities also include ambulatory health care occupancies and business occupancies. [~~**5000**~~ **99** ,~~2021~~ 2024]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue May 21 17:04:01 EDT 2024

Committee Statement

Committee Statement: This revision updates extracted text in accordance with the Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document. The extract is changed from NFPA 5000 to NFPA 99 to reference the base document as NFPA 5000 extracts this definition from NFPA 99.

Response Message: FR-4-NFPA 730-2024

First Revision No. 5-NFPA 730-2024 [Section No. 3.3.30]

3.3.30* Monitoring Station.

A facility that receives signals from ~~electronic~~ premises security systems and has personnel in attendance at all times to respond to these signals. [**731,**~~2023~~ 2026]

A.3.3.30 Monitoring Station.

Services offered by a monitoring station can include the following:

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

[**731,**~~2023~~ 2026]

Submitter Information Verification

Committee: PMM-AAA
Submittal Date: Tue May 21 17:06:12 EDT 2024

Committee Statement

Committee Statement: This revision updates extracted text in accordance with the Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document.

Response Message: FR-5-NFPA 730-2024

First Revision No. 6-NFPA 730-2024 [Section No. 3.3.34]

3.3.34* Reader.

A device used in physical security systems to read a credential that allows ~~a machine readable credential to be entered into an access control system~~ access through access control points . [**731,**~~2023~~ 2026]

A.3.3.34 Reader.

Readers can be of many types and are intended to include car tags, electronic key, magnetic stripe, proximity badge, biometric, or other identifier. [**731,**~~2023~~ 2026]

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue May 21 17:08:20 EDT 2024

Committee Statement

Committee Statement: This revision updates extracted text in accordance with the Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document.

Response Message: FR-6-NFPA 730-2024

First Revision No. 20-NFPA 730-2024 [Section No. 5.4.9]

5.4.9

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

(1) Nature of expected incidents

(2)* Incident response procedures

(3) Emergency contact information

(4) Division of responsibilities and authority among the facility personnel, including who can initiate the plan

(5) Identification of who is covered by the plan (e.g., who is to be evacuated)

(6)* Resources needed for the management of the incident

A.5.4.9(6)

See NFPA 3000 for additional information on active shooter planning and response.

(7) Guidance on the emergency use of funds, disposition of project property, and personal effects

(8) List of annexes to the plan, including but not limited to maps, floor plans, forms, location of personnel, telephone numbers, radio frequencies, and extraordinary procedures

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 16:44:00 EDT 2024

Committee Statement

Committee Statement: This revision provides the user additional resource of information regarding the pre-planning against an active shooter or hostile incident.

Response Message: FR-20-NFPA 730-2024

First Revision No. 22-NFPA 730-2024 [Section No. 12.1.3.2]

12.1.3.2

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

(1) Providing identification, as shown by review of the SVA, for patients, staff, and other people entering the facility

(2) Controlling access into and out of security-sensitive areas as identified in the SVA

(3) Defining and implementing procedures for the following situations:

(a) Security incident

(b) Hostage situation

(c)* Bomb

(d) Criminal threat

(e) Labor action

(f) Disorderly conduct

(g) Workplace violence

(h) Restraining orders

(i) Infant or pediatric abduction

(j) Situations involving VIPs or the media

(k) Ensuring access to emergency areas

(l) * Active shooter(s)

A.12.1.3.2(3)(l)

See NFPA 3000 for additional information on active shooter planning and response.

(4) Providing security at alternative care sites or vacated facilities

(5) Controlling vehicular traffic control on the facility property

(6) Protecting the facility assets, including property and equipment

(7) Establishing a policy for interaction with law enforcement agencies

(8) Ensuring compliance with applicable laws, regulations, and standards regarding security management operations

(9) Putting into place education and training of the facility security force to address the following:

(a) Customer service

(b) Use of physical restraints

(c) Use of force

(d) Response criteria

(e) Fire watch procedures

(f) Lockdown procedures

(g) Emergency notification procedures

Supplemental Information

File Name	Description	Approved

730_Chapter_12_12_1_3_2_FR-22.docx 730_Chapter_12_12_1_3_2_FR-22

Submitter Information Verification

Committee: PMM-AAA
Submittal Date: Thu May 23 16:57:34 EDT 2024

Committee Statement

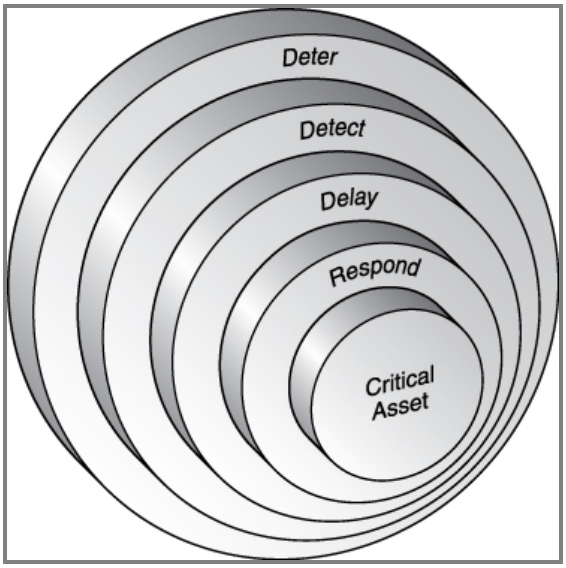
Committee Statement: This revision provides the user additional resource of information regarding the pre-planning against an active shooter or hostile incident.
Response Message: FR-22-NFPA 730-2024

First Revision No. 9-NFPA 730-2024 [Section No. A.5.2.3(5)]

A.5.2.3(5)

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

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



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

(1) Deter — discouraging an adversary from attempting an assault by reducing the likelihood of a successful attack.

(2) Detect — determining that an undesirable event has occurred or is occurring. Detection includes sensing the event, communicating the alarm to an attended location, and assessing the alarm.

(3) Delay — impeding adversary penetration into a protected area.

(4) Respond — counteracting adversary activity and interrupting the undesirable event.

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

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

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

(1) *Permanent replacement.* Permanent replacement of a lost asset includes all of the cost to return it to its former location. Components of that cost are as follows:

(a) Purchase price or manufacturing cost

(b) Freight and shipping charges

(c) Make-ready or preparation cost to install it or make it functional

(2) *Temporary substitute.* In regard to tools of production and other items making up the active structure of an enterprise, it may be necessary to procure substitutes while awaiting permanent replacements. Components of temporary substitute costs may be as follows:

(a) Lease or rental

(b) Premium labor, such as overtime or extra shift work to compensate for the missing production

(3) *Related or consequent cost.* If other personnel or equipment are idle or underutilized because of the absence of an asset lost through a security incident, the cost of the down time is also attributable to the loss event.

(4) *Lost income cost.* If cash that might otherwise be invested is used to procure permanent replacements or temporary substitutes or to pay consequence costs, the income that might have been realized from the investment must also be considered as part of the loss.

(5) *Cost abatement.* To the extent it is available, insurance, or other indemnification for the loss should be subtracted from the costs enumerated above. For precision, that portion of the insurance premium cost attributable to the lost asset should be subtracted from the available insurance before the insurance is used to offset the loss.

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

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

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 13:41:51 EDT 2024

Committee Statement

Committee Statement: The figure is provided as guidance and information, it doesn't deter from the users understanding of the mandatory section. The annex material is revised to remove unnecessarily opinionated text. The SVA provides details on the vulnerabilities, and the intent is to provide benefits to the workplace personnel.

Response Message: FR-9-NFPA 730-2024

Public Input No. 10-NFPA 730-2023 [Section No. A.5.2.3(5)]

First Revision No. 1-NFPA 730-2024 [Section No. A.5.4.8]

A.5.4.8

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

(1) Response of security personnel

(2) Response of emergency services

(3) Access points for emergency services

(4) Communication procedures

More information is available in NFPA ~~1561~~ 1550 .

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu Mar 07 13:56:50 EST 2024

Committee Statement

Committee Statement: As part of the Emergency Response and Responder Safety Document Consolidation Plan as approved and amended by the NFPA Standards Council, NFPA 1550 is a combination of Standards NFPA 1500, NFPA 1521, and NFPA 1561. The reference to NFPA 1561 is revised to NFPA 1550.

Response Message: FR-1-NFPA 730-2024

First Revision No. 21-NFPA 730-2024 [Section No. A.11.1.3.2(7)(e)]

A.11.1.3.2(7)(e)

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

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

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

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

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

See FEMA 428/BIPS-07 , *Primer ~~for~~ to Design Safe Schools Projects in Case of Terrorist Attacks and School Shootings* , for material on shelter-in-place.

See NFPA 3000 for additional information on active shooter planning and response.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 16:54:55 EDT 2024

Committee Statement

Committee Statement: This revision provides the user additional resource of information regarding the pre-planning against an active shooter or hostile incident.

Response Message: FR-21-NFPA 730-2024

First Revision No. 10-NFPA 730-2024 [Section No. A.20.3.2]

A.20.3.2

IES ~~G-1~~ G-1-22 , ~~*Guideline*~~ *Guide for Security Lighting for People, Property, and* ~~*Public Spaces*~~ *Ciritcal Infrastructure* , is for design and implementation of security lighting. The guideline is intended for use by property owners and managers, crime prevention specialists, law enforcement and security professionals, risk managers, lighting specifiers, contractors, the legal profession, and homeowners concerned about security and the prevention of crime. It covers basic security principles, illumination requirements for various types of properties, protocol for evaluating current lighting levels for different security applications, and security survey and crime search methodology. Guidelines include exterior and interior security lighting practices for the reasonable protection of persons and property. There are many complexities to exterior lighting design, including but not limited to “dark sky” compliance, light wash through adjacent properties, and energy conservation. Proper illumination should encourage authorized users to occupy spaces and discourage intruders.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 14:19:49 EDT 2024

Committee Statement

Committee Statement: The title of IES G-1 has been updated since the original 2003 submission referred to in this standard. The revision reflects the updated naming for the version year 2022.

Response Message: FR-10-NFPA 730-2024

Public Input No. 1-NFPA 730-2023 [Section No. A.20.3.2]

First Revision No. 11-NFPA 730-2024 [Section No. E.4.2.1]

E.4.2.1

As a result of increased security awareness, there has been a move away from the traditional key and lock systems to more sophisticated access control systems. The technology used in access control systems ranges from simple push-button locks to computerized access control systems integrated with video surveillance systems. Regardless of the technology used, all access control systems have one primary objective — to screen or identify people prior to allowing entry. ~~Since identification is the foundation of all access control systems, they generally require that the user be in possession of a machine readable credential.~~ Establishing a person's identity can be based on three methods: something known by a person (e.g., password), something possessed by a person (e.g., card or key), or something physically unique about the person (e.g., fingerprint). Electronic access control equipment should be listed to UL 294, *Access Control System Units*.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 14:23:42 EDT 2024

Committee Statement

Committee Statement: The revision adds text that was taken from E.4.2.3.2 Biometric Systems, which provided better clarification for the methods of verifying identity than the existing text. The means for establishing identity were relevant to the whole section of 4.2.3, and therefore was better placed before it than recessed within a sub-section of it.

Response Message: FR-11-NFPA 730-2024

Public Input No. 16-NFPA 730-2023 [Section No. E.4.2.1]

First Revision No. 12-NFPA 730-2024 [Section No. E.4.2.3.2 [Excluding any Sub-Sections]]

~~Establishing a person's identity can be based on three methods: something known by a person (a password), something possessed by a person (a card or key), and something physical about a person (a personal characteristic). Biometric access control devices, or personal characteristic verification locks, rely on the third method.~~ Since duplication of individual physical characteristics is very rare, biometric devices, in theory, could offer the highest security possible. Biometric systems measure a unique characteristic of the person seeking access. ~~These systems are classified as fingerprint, hand or palm geometry, handwriting, voice, and retinal verification systems. Typically, biometric readers are connected to a CPU but can also be used alone.~~ The most readily available commercial systems for access control are fingerprint, palm, iris, and facial systems. Additionally, legacy retina, handwriting, and voice systems may exist but have been deprecated and should not be considered for new access control purposes.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 14:31:12 EDT 2024

Committee Statement

Committee Statement: The opening section on means of establishing identity was relocated to E.4.2.1. This revision provides updated recommendations based on current industry technology.

Response Message: FR-12-NFPA 730-2024

Public Input No. 4-NFPA 730-2023 [Section No. E.4.2.3.2 [Excluding any Sub-Sections]]

First Revision No. 13-NFPA 730-2024 [Section No. E.4.2.3.2.1 [Excluding any Sub-Sections]]

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

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 14:35:59 EDT 2024

Committee Statement

Committee Statement: The length of time that optical finger print scanners have been available is well in excess of 10 years; updating the length of time they have been available does not further the explanation of what they are. The language has been updated to simplify the text and provide only the relevant information.

Response Message: FR-13-NFPA 730-2024

Public Input No. 15-NFPA 730-2023 [Section No. E.4.2.3.2.1 [Excluding any Sub-Sections]]

First Revision No. 17-NFPA 730-2024 [New Section after E.4.2.3.2.5]

E.4.2.3.2.6 Iris Verification Systems.

Iris verification systems use the unique pattern within the iris of the eye as a means of identifying a person. The user looks into an eyepiece that images the iris. The image is compared to information stored in a computer.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 15:21:08 EDT 2024

Committee Statement

Committee Statement: Retinal scanners currently exist in some legacy government systems, but are not commercially available for new installation. Iris verification is a newer technology than retinal verification systems. A task group is established to review iris verification technology and provide recommendations for the Second Draft Meeting.

Response Message: FR-17-NFPA 730-2024

First Revision No. 16-NFPA 730-2024 [Section No. E.4.2.3.2.5]

E.4.2.3.2.5 Retinal Verification Systems.

Retinal verification systems use the pattern of blood vessels within the retina of the eye, which is unique in everyone, as a means of identifying a person. The user looks into an eyepiece that scans the retina with a safe low-level infrared light. The infrared light reflected back is converted into digital data that is compared to information stored in a computer. The limitation in retinal verification systems is that retinal patterns are not stable and can be altered by injury, illness, alcohol, or drugs. There also may be resistance on the part of a person to look into the device. Retinal scanners for access control have largely been deprecated and are no longer readily commercially available.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 15:17:44 EDT 2024

Committee Statement

Committee Statement: Retinal scanners currently exist in some legacy government systems, but are not commercially available for new installation. The revision acknowledges that such systems may still exist somewhere, but updates the standard to not mislead that such a technology is still a viable option for current access control systems.

Response Message: FR-16-NFPA 730-2024

Public Input No. 5-NFPA 730-2023 [Section No. E.4.2.3.2.5]

First Revision No. 15-NFPA 730-2024 [Section No. E.4.3.1.2]

E.4.3.1.2

A signal generator attached to the monitor can be adjusted to project a pattern of light or dark rectangles, or windows, which can be adjusted in size and location on the screen. The windows can be focused on a fixed object to be protected, such as a safe or a doorknob. When the image of an intruder or moving object enters the monitored window, the difference in contrast is detected and triggers an alarm. Such technology is largely deprecated and not applicable to contemporary installations.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 15:07:56 EDT 2024

Committee Statement

Committee Statement: Signal generator technology may not be applicable to contemporary installations, however, it may still be in use and the information provided is useful to the user.

Response Message: FR-15-NFPA 730-2024

First Revision No. 18-NFPA 730-2024 [Section No. E.4.3.2.1]

E.4.3.2.1 Equipment.

Video surveillance equipment should ~~provide appropriate resolution equal to or greater than the manufacturer's resolution specified in a marking on the equipment or in the literature packaged with the video equipment. Video surveillance equipment should~~ be listed for its purpose and comply with Section 889 of the John S . McCain National Defense Authorization Act (NDAA) for Year 2019, which prohibits the purchase of covered telecommunications equipment and services from vendors who sell products containing spyware .

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 15:33:01 EDT 2024

Committee Statement

Committee Statement: This revision removes language that is unclear and appears to attempt to state that resolution of the camera should be proven to be as good or better than what the manufacturer listed on the literature. This should not be a necessary exercise. The revision adds language to update what should be a base requirement for VSS equipment selection; specifically, that it be listed for it's application and additionally that it meet U.S. government recommended supply chain best practice for not procuring equipment from manufacturers incriminated with having potential back doors to foreign governments.

Response Message: FR-18-NFPA 730-2024

Public Input No. 13-NFPA 730-2023 [Section No. E.4.3.2.1]

First Revision No. 19-NFPA 730-2024 [Section No. E.4.3.2.2.4]

E.4.3.2.2.4

The signal can be recorded ~~by a video recorder~~ for playback and analysis at a later time. ~~Many recorders have a time-lapse mode for quick playback of lengthy periods of tape coverage. This system is often used in conjunction with a date-time generator that can project a continuous image of the date and time in the corner of the monitor screen.~~

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Thu May 23 15:38:54 EDT 2024

Committee Statement

Committee Statement: This revision removed text that referenced deprecated information on the use of VCRs in conjunction with a matrix/controller for a VSS recording device. The language was clarified to refer to recording without specifying the recording device.

Response Message: FR-19-NFPA 730-2024

Public Input No. 14-NFPA 730-2023 [Section No. E.4.3.2.2.4]

First Revision No. 7-NFPA 730-2024 [Sections G.1, G.2]

G.1 Referenced Publications.

The documents or portions thereof listed in this annex are referenced within the informational sections of this guide and are not advisory in nature unless also listed in Chapter 2 for other reasons.

G.1.1 NFPA Publications.

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

NFPA 70®, *National Electrical Code®*, ~~2023~~ 2026 edition.

NFPA 80, *Standard for Fire Doors and Other Opening Protectives*, ~~2022~~ 2025 edition.

NFPA 101®, *Life Safety Code®*, ~~2021~~ 2024 edition.

NFPA 731, *Standard for the Installation of Premises Security Systems*, ~~2023~~ 2026 edition.

NFPA 1550, *Standard for Emergency Responder Health and Safety*, 2024 edition.

~~NFPA 1561 , *Standard on Emergency Services Incident Management System and Command Safety* , 2020 edition.~~

NFPA 3000, *Standard for an Active Shooter/Hostile Event Response (ASHER) Program*, 2024 edition.

G.1.2 Other Publications.

G.1.2.1 ASTM Publications.

ASTM International, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959.

ASTM F567, *Standard Practice for the Installation of Chain-Link Fence,*~~2014~~ 2023 .

ASTM F1090-15 , *Standard Classification for Bank and Mercantile Vault Construction,*~~2015~~ 2016 .

ASTM F1233-21 , *Standard Test Method for Security Glazing Materials and Systems,*~~2008, reapproved 2013~~ 2021 .

ASTM F1247-89(2018) , *Standard Specification for Intrusion Resistant Generic Vault Structures,* 1989, ~~reapproved 2011~~ revised 2018 .

G.1.2.2 BHMA Publications.

Builders Hardware Manufacturers Association, 355 Lexington Avenue, 15th Floor, New York, NY 10017.

ANSI/BHMA A156.1, *Butts and Hinges,*~~2016~~ 2021 .

ANSI/BHMA A156.2, ~~*Bored and Preassembled*~~ *Locks and Latches,*~~2017~~ 2022 .

ANSI/BHMA A156.4, *Door Control*~~*s*~~ — ~~*Closers*~~ *Closers* , 2019.

ANSI/BHMA A156.5, ~~*Auxiliary Locks and Associated Products*~~ *Cylinders and Input Devices for Locks* , 2020.

ANSI/BHMA A156.12, *Interconnected Locks*~~ *and Latches* ,2018~~ 2022 .

ANSI/BHMA A156.13, *Mortise Locks*~~ *and Latches Series 1000* ,2017~~ 2022 .

ANSI/BHMA A156.16, *Auxiliary Hardware,*~~2018~~ 2023 .

ANSI/BHMA A156.17, *Self-Closing Hinges and Pivots,* 2019.

ANSI/BHMA A156.23, *Electromagnetic Locks,* 2017.

ANSI/BHMA A156.24, *Delayed Egress Locking Systems,*~~2018~~ 2022 .

ANSI/BHMA A156.25, *Electrified Locking Devices,*~~2018~~ 2021 .

ANSI/BHMA A156.26, *Continuous Hinges,* 2017.

ANSI/BHMA A156.28, ~~*Recommended Practice for*~~ *Master Keying*~~ *Systems* ,2018~~ 2023 .

ANSI/BHMA A156.30, *High Security Cylinders,* 2020.

ANSI/BHMA A156.31, *Electric Strikes and Frame Mounted Actuators,* 2019.

G.1.2.3 FEMA Publications.

Federal Emergency Management Agency, ~~U.S.~~ US Department of Homeland Security, 500 C Street, SW, Washington, DC ~~20472~~ 20024 .

FEMA 428/BIPS-07 , *Primer ~~for~~ to Design Safe Schools Projects in Case of Terrorist Attacks and School Shootings* , ~~December 2003~~ January 2012 .

G.1.2.4 IEEE Publications.

IEEE~~, 3 Park Avenue, 17th Floor, New York, NY 10016-5997~~ Operations Center, 445 Hoes Lane, Piscataway, NJ 08854-4141 .

ANSI/IEEE C2-2023 , *National Electrical Safety Code*, ~~2012, with 2013 interpretation~~ 2022 .

G.1.2.5 IESNA Publications.

Illuminating Engineering Society, 120 Wall Street, Floor 17, New York, NY 10005-4001.

IES ~~G-1~~ G-1-22 , ~~*Guideline*~~ *Guide for Security Lighting for People, Property, and ~~Public Spaces~~ Critical Infrastructure* ,~~2003~~ 2022 .

G.1.2.6 SDI Publications.

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

ANSI/SDI A250.4, *Test Procedure and Acceptance Criteria for Physical Endurance for Steel Doors, Frames and ~~Hardware Reinforcing~~ Frame Anchors* ,~~2011~~ 2022 .

ANSI/SDI A250.8, ~~*Recommended*~~ *Specifications for Standard Steel ~~Door~~ Doors & Frames,*~~2003, reaffirmed 2008~~ 2017 .

G.1.2.7 UL Publications.

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

UL 294, *Access Control System Units*, ~~2013, revised 2018~~ 2023 .

UL 437, *Key Locks*, ~~2017~~ 2013, revised 2023 .

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

UL 608, *Burglary Resistant Vault Doors and Modular Panels*, 2004, revised ~~2017~~ 2022 .

UL 634, *Connectors and Switches for Use with Burglar-Alarm Systems*, 2007, revised ~~2015~~ 2020 .

UL 636, *Holdup Alarm Units and Systems*, ~~1996, revised 2013~~ 2018 .

UL 639, *Intrusion-Detection Units*, 2007, revised ~~2018~~ 2019 .

UL 681, *Installation and Classification of Burglar and Holdup Alarm Systems*, 2014, revised 2021 .

UL 687, *Burglary-Resistant Safes*, ~~2011, revised 2015~~ 2020 .

UL 752, *Bullet-Resisting Equipment*, ~~2005, revised 2015~~ 2023 .

UL 768, *Combination Locks*, 2006, revised ~~2018~~ 2023 .

UL 972, *Burglary Resisting Glazing Material*, 2006, revised ~~2015~~ 2020 .

UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, 2011, revised 2020.

UL 2058, *Outline of Investigation for High-Security Electronic Locks*, 2005, revised 2013 .

UL 2610, *Commercial Premises Security Alarm Units and Systems*, ~~2018~~ 2021 , revised ~~2020~~ 2023 .

G.1.2.8 ~~U.S.~~ US Government Publications.

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

Americans with Disabilities Act of 1990, 42 U.S.C. § 12101 et seq.

John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019, 2018.

S/N 027-000-0132-7, ~~U.S.~~ US Department of Justice, *Vulnerability Assessment of Federal Facilities*, 1995.

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

G.2 Informational References.

The following documents or portions thereof are listed here as informational resources only. They are not directly referenced in this guide.

Academic Institution Accreditation Requirements, Wilmington, DE: SafePlace Corporation, 2003.

America's Crime Fears Threaten Retail Sales for 1995, Boston, MA: America's Research Group, 1995.

Atlas, R. *21st Century Security and CPTED — Designing for Critical Infrastructure Protection and Crime Prevention*, second edition. Boca Raton, FL: CRC Press, 2013.

Bates, N. *Checklist for Security Assessments — Hotels and Motels*. Sudbury, MA: Liability Consultants Inc., 1993.

Berlonghi, A. E. *Special Event Security Management, Loss Prevention, and Emergency Services*. Mansfield, OH: Bookmasters, Inc., 1996.

Brashear, J. P., and J. W. Jones. "Risk Analysis and Management for Critical Asset Protection (RAMCAP Plus)." In *Wiley Handbook of Science and Technology for Homeland Security*, John Wiley & Sons, 2010.

Chemical Accident Prevention: Site Security. Washington, DC: ~~U.S.~~ US Environmental Protection Agency, Office of Solid Waste and Emergency Management, Chemical Emergency Preparedness and Prevention Office, 2000.

Crime Awareness and Campus Security Act of 1990. ~~U.S.~~ US Public Law 101-542, Title II. Nov. 1990:104 (2384–2387).

The Expanding Role of Crime Prevention Through Environmental Design in Premises Liability. NIJ Research in Brief. Washington, DC: ~~U.S.~~ US Department of Justice, 1996.

Fannin, J. C. "A Discussion of Modern Security," *Proceedings of the Annual Conference of the Risk and Insurance Management Society*, Chicago, IL, April 2003.

FIPS ~~140-2~~ 140-3 , National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules,*~~May 2001~~ March 2019 .

Floyd, William R., *Security Surveys: Guidelines for Evaluating Security,* Alexandria, VA: ASIS International, 2007.

Fourth Annual Survey of Restaurant and Fast Food Employees. Minneapolis: National Computer Systems, 1999.

General Security Risk Assessment Guidelines. Alexandria, VA: American Society for Industrial Security International, 2003.

GSAM, *General Service Administration Acquisition Manual/Regulation (GASM/R)* , ~~9/19/2008~~ 2/15/2024 .

Guidelines for the Safety and Security of Health Care and Community Service Workers. San Francisco: California State Department of Industrial Relations. Division of Occupational Safety and Health, 1993.

Guidelines for Preventing Workplace Violence ~~Prevention Programs for Health Care Workers in Institutional and Community Settings~~ for Healthcare and Social Workers . Washington, DC: Department of Labor. Occupational Safety and Health Administration, ~~1993~~ 2016 .

Higher Education Amendments of 1998 Act. ~~U.S.~~ US Public Law 105-244, Oct. 1998:104 (2384–2387).

Hyatt, James A., Ready to Respond: Case Studies in Campus Safety and Security, Washington, D.C.: National Association of College and University Business Officers, 2010.

ICS 705-1, Director of Central Intelligence Directive, *Physical and Technical Security Standards for Sensitive Compartmented Information Facilities,* 9/17/2010.

Lighting for Parking Facilities, RP-20, Illuminating Engineering Society, 2014.

Lighting Handbook, 10th edition. Illuminating Engineering Society, 2011.

Lodging Facility Accreditation Requirements. Wilmington, DE: SafePlace Corporation, 2003.

Meadows, R. J. “The Likelihood of Liability.” *Security Management*, 1991:35.7, pp. 60–66. Alexandria, VA: American Society for Industrial Security International.

Niemann, L. “Are You Armed Against High Dollar Judgments in Security Cases?” Austin, TX: Texas Apartment Association, National Institute of Justice, 1988.

Niemann, L. “Rape Protection for Onsite Apartment Personnel.” Austin, TX: Texas Apartment Association, 1988.

Operation Liberty Shield. Washington, DC: Department of Homeland Security, 2003.

Preventing Crime: What Works, What Doesn't, What's Promising: A Report to the United States Congress. Washington, DC: National Institute of Justice, Department of Criminology and Criminal Justice, University of Maryland, 1997.

Preventing Homicide in the Workplace. Washington, DC: ~~U.S.~~ US Department of Health and Human Services, National Institute for Occupational Safety and Health, 1993.

Recommended Lighting for Walkways and Class 1 Bikeways, IES DG-5-94, Illuminating Engineering Society of North America, 1994 (withdrawn).

SafePlace Security Vulnerability Assessment Workbook. Wilmington, DE: SafePlace Corporation, 2003.

Results of the National Campus Safety and Security Project Survey, National Association of College and University Business Officers (NACUBO.ORG) ~~http://www.nacubo.org/Documents/Initiatives/CSSPSurveryResults.pdf~~ nacubo.org/media/Nacubo/Documents/Initiatives/CSSPSurveyResults.ashx

Safety Bulletin: The Security Vulnerability Assessment. Wilmington, DE: SafePlace Corporation, 2003.

Safety Bulletin: Terrorist Threat Condition Level Change. Wilmington, DE: SafePlace Corporation, 2003.

Security and Loss Prevention for the Hotel and Motel. New York: American Hotel and Motel Association, 1985.

“Security and Protective Lighting.” *Protection of Assets Manual*. Santa Monica, CA: The Merritt Company, 1997, pp. 19.59–19.73b.

Security Principles 101: Physical & Administrative Protective Elements. Wilmington, DE: SafePlace Corporation, 2002.

Security Vulnerability Assessment: A Guide to Security Countermeasure Development. Wilmington, DE: SafePlace Corporation, 2003.

Sherwood, C. W. “Security Management for a Major Event.” Law Enforcement Bulletin. Washington, DC: Federal Bureau of Investigation, August 1998.

Site Security Survey Record. Wilmington, DE: SafePlace Corporation, 2003.

“Special Report: Are Malls Safe?” Crime Control Research Corp., *Security Law Newsletter* 14.4:1994, pp. 37–39.

Student Assistance General Provisions: Final Rule (64FR210). Washington, DC: ~~U.S.~~ US Department of Education, Nov. 1, 1999 (59060–59073).

Vulnerability Assessment Methodologies. Albuquerque, NM: Sandia National Laboratories, 2003.

~~U.S.~~ US Army Corps of Engineers, 10 South Harvard Street, Baltimore MD 21201.

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue May 21 17:12:56 EDT 2024

Committee Statement

Committee Statement:	References updated in accordance with the Reference policy. The reference to NFPA 3000 is added based its addition to Annex A.
Response Message:	FR-7-NFPA 730-2024

Public Input No. 20-NFPA 730-2023 [Section No. G.1.2.7]

Public Input No. 3-NFPA 730-2023 [Section No. G.1.2.5]

First Revision No. 8-NFPA 730-2024 [Section No. G.3]

G.3 References for Extracts in Informational Sections.

NFPA 731,*Standard for the Installation of Premises Security Systems*, ~~2023~~ 2026 edition.

NFPA 99, *Health Care Facilities Code* , 2024 edition.

~~*NFPA 5000* ® , *Building Construction and Safety Code* ® , 2021 edition.~~

Submitter Information Verification

Committee: PMM-AAA

Submittal Date: Tue May 21 17:28:55 EDT 2024

Committee Statement

Committee Statement: This revision updates extracted text in accordance with the Extract Policy. For substantiation on any changes, see the first and second draft reports for the source document. The extract from NFPA 5000 was changed to NFPA 99 as NFPA 5000 extracts from NFPA 99 for this content.

Response Message: FR-8-NFPA 730-2024