Public Input No. 11-NFPA 730-2023 [Global Input]

This guide does not seem to adequately address security measures designed to prevent arson; premises which are fire-safe may not be fire-secure. Specific guidance on security safeguards designed to prevent disabling of fire suppression equipment might be helpful here.

Statement of Problem and Substantiation for Public Input

Arson is the main point at which fire protection and security meet, as fire protection systems that are vulnerable to sabotage will not perform their job effectively unless the fire is accidental.

Submitter Information Verification

Submitter Full Name: Jonah Cummings
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Wed Oct 25 02:10:18 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: The submission did not include proposed language and justification. NFPA 730 is a guide for all threats within the physical campus. The technical committee encourages the submitter to provide proposed text for the body of the guide and include technical justification. NFPA 1330 discusses arson or fire threats.

Public Input No. 6-NFPA 730-2023 [Section No. 2.2]

2.2 NFPA Publications.

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

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

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

~~NFPA 731~~ NFPA 601, *Standard for Security Services in Fire Loss Prevention*, 2020 edition.

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

Statement of Problem and Substantiation for Public Input

Adding NFPA 601 as a reference is important because often the same personnel who provide premises security also provide security services in fire loss prevention. Additionally, NFPA 601 authorizes the replacement or supplementation of fire loss security personnel with automated systems in some cases, linking it to this guide.

Adjusting the italics to be consistent between standards helps ensure readability.

Submitter Information Verification

Submitter Full Name: Jonah Cummings
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Wed Oct 25 00:32:11 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: NFPA 601 is not referenced in the body of the document. The Manual of Style does not permit references in Section 2.2 that are not referenced in the body of the standard.

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

2.3.2 UL Publications.

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

UL 294, *Access Control System Units*, ~~2018~~ 2017, revised 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.

Statement of Problem and Substantiation for Public Input

Update the standards to the most current publication dates.

Related Public Inputs for This Document

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

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL Solutions
Street Address:
City:
State:
Zip:
Submittal Date: Fri Dec 29 13:09:12 EST 2023
Committee: PMM-AAA

Committee Statement

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

Public Input No. 9-NFPA 730-2023 [Section No. 3.3.11]

3.3.11 Deterrent.

Any physical ~~or psychological~~ device or method that ~~discourages action~~ allows more time for an act to be detected .

Statement of Problem and Substantiation for Public Input

In the security industry, Deter, Detect, and Delay are used as technical terms. They are part of a security framework developed by the Sandia national laboratory. Within that framework, deterrence is designed to buy time for detection, and often delays an attacker after detection, similar to how fire-resistance of an item allows both more time for a fire to be detected, and more time for response personnel to arrive before it has grown.

If the original definition is a better fit for the standard, I would suggest a word other than deterrent, such as disincentive.

Submitter Information Verification

Submitter Full Name: Jonah Cummings
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Wed Oct 25 01:00:46 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: Insufficient information was provided to revise the definition of 'deterrent.' The current definition stands on its own and assumes that an action is not occurring and doesn't need to be detected. 'Deterrent' within NFPA 730 is not only a technical term as part of the security framework developed by Sandia, but it is also an action that can be taken.

Public Input No. 22-NFPA 730-2023 [New Section after 6.5.2]

TITLE OF NEW CONTENT

Type your content here ...

A. 6.1.1 Equipment A critical part of an access or egress control system is the lock hardware that holds a door closed and opens or releases when initiated. Like many components of an integrated system, the locking mechanism can have various forms and functionalities, depending on the particular applications.

The NFPA 101 Life Safety Code includes requirements for a means of egress system to be provided that includes a continuous and unobstructed path of egress travel from any occupied point in a building, structure or facility to a public way. However, there are specific situations in which these model codes allow access control equipment that limit the immediate and unobstructed egress travel under strict provisions.

The factors that must also be considered for installation and in accordance with applicable fire and life safety codes include:

- Integration with fire detection and suppression or other life safety systems that release locked doors upon their activation, allowing immediate emergency egress
- Fail safe features to release locks in the event of a loss of power
- Fail secure features that intentionally maintain locked positions
- Emergency planning and preparedness with staff training and required drills
- Limitations on the delay time for delayed-egress doors
- Special signage requirements
- Security and resistance to unauthorized entry may also be considerations

Locks and locking systems can be tested for compliance with different end product standards. Each end product standard defines the scope of the application and includes construction and test compliance criteria for evaluation and certification.

Typical end uses for the locks and locking systems include integration into access control systems, fire rated door assemblies, special locking arrangements, panic hardware, controlled exit panic devices and burglary resistant electric locks. Locks and locking systems used in these applications can take different forms depending on the design of a product or system. Some of these devices are purely mechanical and others may include electronics to control or provide delayed release or audible alarm functions. Certified locks are investigated for safety from electric shock and mechanical hazards and depending on the product type may also be tested for burglary resistance and/or fire resistance.

An end user or AHJ can see various configurations of equipment incorporated into a system and the equipment may have different forms to suit a specific application. A very common scenario is the use of UL 294 certified access control systems units controlling locks certified to UL 1034.

Other prevalent applications include special locking arrangements that have dedicated system component equipment and certified locks connected to control a request to exit (REX) system. For this application, the REX system certification is specific to the system components submitted for investigation.

The various permutations of locking hardware and systems applications (see table) allows for the use of the devices in accordance with model building and life safety codes, with the common element of safety by design.

The table below summarizes the applicable standards for various locking devices and systems that are typically used on means of egress or controlled access areas.

Standard	**Category Title**	**Helpful Notes**	**Typical door hardware / lock form factor**
UL 294, Standard for Access Control System Units	Access Control System Units*	Sec. 34.2 applies to Single point locking devices	Autonomous access control lock
UL 294	Special Locking Arrangements	UL 294, Sec. 68 applies to Controlled and Delayed Egress Equipment and Systems Operation	Require to Exit (REX) devices / systems and controlled or delayed egress locks
UL 1034, Standard for Burglary-Resistant Electric Locking Mechanisms	Burglary Resistant Electric Locking Mechanisms	Performance based for static force, dynamic force, and endurance test factors	Electromagnetic locks, Electric Dead bolts, Electric Door Strikes, Electrically operated door locking mechanisms,
UL 305, Standard for Panic Hardware	Panic or Fire Exit Hardware	Generally mechanical devices only (no electronics)	Panic Hardware, Fire Exit Hardware
UL 294 and UL 305,	Controlled Exit Panic Devices	UL 294, and UL 305 apply	Electromechanical locking/latching mechanisms
UL 634, Standard for Panic Hardware	Connectors and Switches for use in Burglar Alarm Systems	Includes Electric Power Transfers, Door Loops, and Door Position Switches	Electric Hinge and flexible connectors intended for burglar alarm applications
UL 10C, Standard for Positive Pressure Fire Tests of Door Assemblies	Positive Pressure Fire Test of Door Assemblies	Also, UL 305 for Card readers and components for use with locks sold separately	Electric Cylindrical Locks and Mortise Locks; Electrically Controlled Single-Point Locks or Latches; Electromagnetic locks ; Fire Exit Hardware; Electrified Hinge; Electric strikes; Miscellaneous Fire Door Accessories, Positive Pressure Tested; Accessories for use with Single-

			point locks and latches and fire exit hardware

Statement of Problem and Substantiation for Public Input

This Public Input adding an Annex Note will provide additional guidance on the testing and certification standards for various access control and egress locking systems to guide AHJs in acceptance of products intended for use in these applications.

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL Solutions
Street Address:
City:
State:
Zip:
Submittal Date: Fri Dec 29 13:30:58 EST 2023
Committee: PMM-AAA

Committee Statement

Resolution: The proposed revision is included in NFPA 731 and is not appropriate for inclusion in NFPA 730.

Public Input No. 21-NFPA 730-2023 [Section No. 7.5.3.2]

7.5.3.2

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

(1) * ANSI/BHMA A156 Series, *Categories of Builders Hardware*, for builders' hardware

(2) UL 1034, *Burglary-Resistant Electric Locking Mechanisms*, for burglary-resistant electronic locking mechanisms

(3) UL 437, *Key Locks*, for key locks

(4) UL 768, *Combination Locks*, for combination locks

(5) UL 294, *Access Control System Units*, for access control system units

(6) UL 2058, *Outline of Investigation for High-Security Electronic Locks*, for high-security electronic locks

(7) UL 305, *Panic Hardware*, and ANSI/BHMA A156.3, *Exit Devices*, for exit panic devices

A.7.5.3.2(1)

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

Statement of Problem and Substantiation for Public Input

This Public Input adding an Annex Note will provide additional guidance on the testing and certification standards for various access control and egress locking systems to guide AHJs in acceptance of products intended for use in these applications.

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL Solutions
Street Address:
City:
State:
Zip:
Submittal Date: Fri Dec 29 13:26:41 EST 2023
Committee: PMM-AAA

Committee Statement

Resolution: The proposed text is already located in annex A.7.5.3.2(1).

Public Input No. 8-NFPA 730-2023 [Chapter 8 [Title Only]]

~~Crime Prevention Through Environmental~~ Premises Design

Statement of Problem and Substantiation for Public Input

Crime Prevention Through Environmental Design (CPTED) is a specific framework designed to reduce crime through certain environmental design principles, first developed by Oscar Newman under the name "Defensible Space".

However, long-term follow-ups on many sites designed using these principles have shown only a temporary decrease in crime, such as within the Five Oaks neighborhood that Mr. Newman used to promote CPTED to HUD officials; recommending that CPTED practices to be followed is irresponsible without further research into why those early sites did not maintain their crime prevention capabilities even though the design remained the same.

Submitter Information Verification

Submitter Full Name: Jonah Cummings
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Wed Oct 25 00:43:29 EDT 2023
Committee: PMM-AAA

Committee Statement

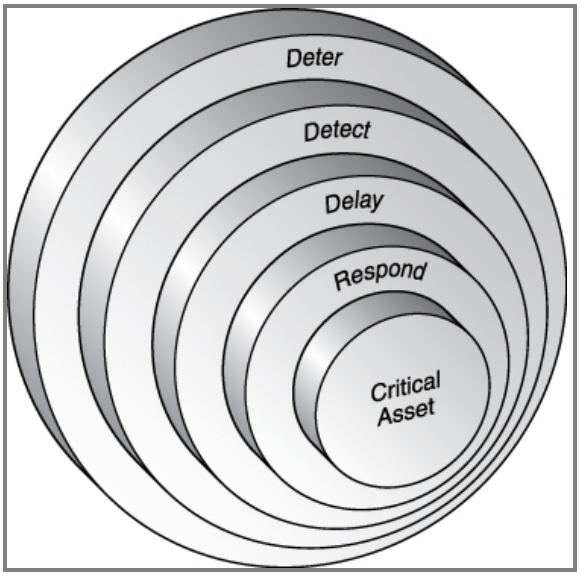
Resolution: Insufficient information or data was provided to change the title of the chapter.

Public Input No. 10-NFPA 730-2023 [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~~ This is accomplished 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:

(2) Purchase price or manufacturing cost

(3) Freight and shipping charges

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

(5) *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:

(6) Lease or rental

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

(8) *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.

(9) *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.

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

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

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

Statement of Problem and Substantiation for Public Input

This section confuses two methodologies, concentric rings of protection and Deter-Detect-Delay. The graphic is misleading, as if taken as rings it suggests that response happens after delay, when response happens at the same time as delay; the delay is what allows the response to arrive in time to interrupt the adversary. If the diagram is taken as a pyramid shape, it suggests that detection happens continuously, when it is instead a distinct event; as the diagram only adds confusion no matter how it is interpreted, it should be removed.

The "new world" sentence is inserting unnecessary opinion into the guide; if someone has committed to following the guidelines, they already see a need for secure premises.

Submitter Information Verification

Submitter Full Name: Jonah Cummings
Organization: [Not Specified]
Street Address:
City:
State:
Zip:
Submittal Date: Wed Oct 25 01:20:51 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-9-NFPA 730-2024

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.

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

A.20.3.2

IES G 1, ~~*Guideline*~~ *Guide* *for Security Lighting for People, Property, and* ~~*Public Spaces*~~ *Critical 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.

Statement of Problem and Substantiation for Public Input

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

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Fri Aug 04 15:45:16 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-10-NFPA 730-2024
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.

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

E.4.2.1– Purpose

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. Electronic~~ Establishing a person's identity can be based on three methods; something known by a person (ie.. password), something possessed by a person (ie.. card or key), or some physically unique about the person (ie.. finger print). Electronic access control equipment should be listed to UL 294, *Access Control System Units*.

Statement of Problem and Substantiation for Public Input

The added test was taken from E.4.2.3.2 Biometric Systems, which provided a better description for the methods of verifying identity than the existing text. The providing for the definition for the means for establishing identity were relevant to the whole section of 4.2.3, and therefore were better placed before it than recessed within a sub-section of it. In turn, I will be proposing the elimination of the text from that section.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Wed Nov 01 16:01:34 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-11-NFPA 730-2024
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.

Public Input No. 4-NFPA 730-2023 [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. Additional legacy retina, handwriting, and voice systems may exist but have been deprecated and should not be considered for access control purposes .

Statement of Problem and Substantiation for Public Input

Relocated opening section on means of establishing identity to E.4.2.1. Provided updated text based on current industry conditions.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Mon Sep 25 15:30:12 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-12-NFPA 730-2024
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.

Public Input No. 15-NFPA 730-2023 [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.

Statement of Problem and Substantiation for Public Input

The length of time that optical finger print scanners have been available is well in excess of 10 years now, and 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.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Wed Nov 01 15:15:14 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-13-NFPA 730-2024
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.

Public Input No. 5-NFPA 730-2023 [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.

Statement of Problem and Substantiation for Public Input

Retinal scanners currently exist in some legacy government systems, but are not commercially available for new installation. The proposed update would allow for the acknowledgement 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.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Mon Sep 25 15:32:43 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-16-NFPA 730-2024
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.

Public Input No. 12-NFPA 730-2023 [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.~~

Statement of Problem and Substantiation for Public Input

This is deprecated information and not applicable to contemporary installations.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Wed Nov 01 14:35:08 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: 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.

Public Input No. 13-NFPA 730-2023 [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 should 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.

Statement of Problem and Substantiation for Public Input

The removed section 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 added section is an update to 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.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Wed Nov 01 14:38:33 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-18-NFPA 730-2024

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.

Public Input No. 14-NFPA 730-2023 [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.~~

Statement of Problem and Substantiation for Public Input

The removed text was deprecated information from the use of VCRs in conjunction with a matrix/controller for a VSS recording device.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Wed Nov 01 14:54:58 EDT 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-19-NFPA 730-2024
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.

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

G.1.2.5 IESNA Publications.

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

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

Statement of Problem and Substantiation for Public Input

A newer standard has been released and it is proposed that it be adopted.

Submitter Information Verification

Submitter Full Name: David Church
Organization: kW Mission Critical Engineering
Street Address:
City:
State:
Zip:
Submittal Date: Mon Sep 25 14:16:16 EDT 2023
Committee: PMM-AAA

Committee Statement

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

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

G.1.2.7 UL Publications.

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

UL 294, *Access Control System Units*, ~~2013~~ 2017 ,revised 2018.

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

UL 606, *Linings and Screens for Use with Burglar-Alarm Systems*, 1999, revised ~~2006~~ 2023 .

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~~ 2022 .

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~~ 2021 .

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.

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

Statement of Problem and Substantiation for Public Input

Update the standards to the most current publication dates.

Related Public Inputs for This Document

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

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL Solutions
Street Address:
City:
State:
Zip:
Submittal Date: Fri Dec 29 13:19:48 EST 2023
Committee: PMM-AAA

Committee Statement

Resolution: FR-7-NFPA 730-2024

Statement: References updated in accordance with the Reference policy. The reference to NFPA 3000 is added based its addition to Annex A.