



Second Revision No. 23-NFPA 1225-2020 [Detail]

Insert new A.18.3 using attached Word file.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR23_A.18.3.docx	staff use
Detail_SR-23_A.18.3_PUF-AAA_NEW.docx	for balloting

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 13:09:39 EST 2020

Committee Statement

Committee Statement: Signal boosters can add noise to the receivers at a macro public safety site, such that those sites will become increasingly “deaf” to hearing low powered portable radios used by ERUs. As a result, AHJs and frequency license holder(s) need to be aware of other solutions that do not involve signal boosters.

Response SR-23-NFPA 1225-2020

Message:

[Public Comment No. 101-NFPA 1225-2020 \[Section No. 18.12\]](#)

[Public Comment No. 15-NFPA 1225-2020 \[Section No. 18.9\]](#)

[Public Comment No. 99-NFPA 1225-2020 \[Section No. 18.10\]](#)

[Public Comment No. 97-NFPA 1225-2020 \[Section No. 18.8\]](#)

[Public Comment No. 94-NFPA 1225-2020 \[Section No. 18.3\]](#)

[Public Comment No. 96-NFPA 1225-2020 \[Section No. 18.6\]](#)

[Detail SR-23]

A.18.3

There are multiple system solutions that might solve the problem of in-building RF coverage for ERUs. The choice depends on many factors, including the proximity and number of buildings with such systems, the RF noise floor in the area, the costs to agencies and building owners, and the accessibility to various agencies, such as fire, emergency medical services (EMS), and law enforcement. Ideally, the RF design professional should provide frequency license holder(s) and AHJs with an analysis of the pros and cons of the options that are most useful in the particular building, so that the AHJ and frequency license holder(s) can choose a solution. This review should be made each time a new solution is proposed for another building in the vicinity, because multiple devices can have an increasing impact on noise floor and other system parameters.

Table A.18.3 provides some information as to the pros, cons, and details of the different options available. It should be noted that not every solution shown in the table will meet all requirements of this standard.

Table A.18.3 Possible In-Building Technical Solutions

Solution	Interface to Macro Public Safety Radio System	Distribution of In-Building Signals	Pros	Cons	Notes
Passive system	Donor antenna	RF cables, antennas	Low cost; simple installation; does not add to area RF noise floor or create potential interference; can be later expanded by adding BDA	Limited applicability to smaller buildings where macro site signals are strong and path to donor antenna is not obstructed	No amplifiers; just donor antenna connected to internal antennas or radiating cable.
Portable repeater	RF via portable repeater's antenna	RF via portable repeater's antenna	No costly infrastructure required of building owners; no increase in area RF noise floor; little or no interference potential; simple solution for smaller agencies	Can cause delay in response while unit is carried into building and activated; not a good solution for EMS/law enforcement unless they are equipped with a portable repeater; might not comply with the performance requirements of this standard	A suitcase/backpack base or repeater is brought into the building along with a small antenna to communicate with ERUs inside and the IC outside.
Vehicular repeater	RF via vehicular repeater's antenna	RF via vehicular repeater's antenna	No costly infrastructure required of building owners; no increase in area RF noise floor; little or no interference potential; simple solution for smaller agencies; vehicle-mounted antenna might provide some improvement	Personnel must remember to activate the unit before leaving vehicle; not a good solution for EMS/law enforcement unless they are equipped with a vehicular repeater; might not comply with the performance requirements of this standard	A repeater or base radio mounted on a vehicle outside the building is used to communicate with ERUs inside the building and the IC outside.

Solution	Interface to Macro Public Safety Radio System	Distribution of In-Building Signals	Pros	Cons	Notes
Macro system repeater or base station in building ("fiber to the building")	Optical fiber to the building	RF cables, antennas	Reduces outside building RF pollution; eliminates donor antenna; good choice where building is far from macro site or donor antenna path is obstructed	Need fiber or other connectivity from public safety system to building repeater/base; frequency license holder and AHJ need building access to maintain equipment as part of public safety system	NA
Macro system repeater or base station in building ("fiber to the building")	Optical fiber to the building	Optical fiber DAS with RF to optical converters	Reduces outside building RF pollution; eliminates donor antenna; good choice where building is far from macro site or donor antenna path is obstructed; can be used with multiple buildings in a complex	Need fiber or other connectivity from public safety system to building repeater/base; frequency license holder and AHJ need building access to maintain equipment as part of public safety system	This type of distribution is a good solution in a large building complex where an outside public safety base/repeater alone cannot sufficiently penetrate the buildings (e.g., large shopping centers, multi-use office spaces, college campuses).
Normally off in-building system [called "auxiliary radio communications system (ARCS)" in New York City, NY]	Can be self-contained (i.e., no connection to public safety system). If connected to public safety system can be RF via donor antenna, or via optical fiber to building	RF cables, antennas; can also be via optical fiber DAS with RF to optical converters	Doesn't add to RF noise floor until activated by the emergency response personnel; can have close spacing of systems without interference	EMS/law enforcement will need access devices and usage training; can delay initial response until system is activated; cannot receive or transmit on the public safety system unless connected to public safety system dispatch; needs to be tested often to be certain system will operate when needed	This system provides a complete self-contained in-building communications system with its own base or repeater station and command console on the main floor. The system is normally not on and must be first activated by a key, token, or passcode. It could be activated by dispatch if the method is secure.
BDA system	Donor antenna	RF cables, antennas	Good signals in all building areas if system properly designed and maintained	The system must be carefully set up to eliminate self-oscillation and excessive RF noise; multiple closely spaced systems increase noise floor; increased possibility of interference to public safety system; must have good path between donor antenna and	Many countries require written authorization from the frequency license holder(s) and must comply with the rules of the radio licensing authority. It can be used in buildings where RF losses in RF distribution cables are not excessive.

Solution	Interface to Macro Public Safety Radio System	Distribution of In-Building Signals	Pros	Cons	Notes
				public safety system site	
BDA system	Donor antenna	Optical fiber DAS with RF to optical converters	Good signals in all building areas if the system is properly designed and maintained; can be used with multiple buildings in a complex	System must be carefully set up to eliminate self-oscillation and excessive RF noise; multiple closely spaced systems increase noise floor; increased possibility of interference to public safety system; must have good path between donor antenna and public safety system site	Many countries require written authorization from the frequency license holder and must comply with the rules of the radio licensing authority. It can be used in larger buildings where RF losses are too great to use RF distribution.

NA: Not applicable.



Second Revision No. 24-NFPA 1225-2020 [Section No. 12.1.3 [Excluding any Sub-Sections]]

Chapters 12 through 23 shall apply to publicly and privately owned communications systems that include, but are not limited to, the following:

- (1) Computer aided dispatching systems
- (2) Telephone systems
- (3) 9-1-1 systems
- (4) Next Generation 9-1-1 systems
- (5) Multi-line telephone systems (MLTS) used to access the Enhanced 9-1-1 systems
- (6) Telematics
- (7) Emergency response facility alerting systems
- (8) Public and private alarm reporting systems
- (9) One-way and two-way radio systems
- (10) Nationwide public safety broadband network (NPSBN).

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 13:56:13 EST 2020

Committee Statement

Committee Statement: Inclusion of the nationwide public safety broadband network ensures that public safety broadband communications meet the same in-building standards as other technologies.

Response: SR-24-NFPA 1225-2020

Message:

Public Comment No. 54-NFPA 1225-2020 [Section No. 12.1.3 [Excluding any Sub-Sections]]



Second Revision No. 25-NFPA 1225-2020 [Section No. 12.8.8]

12.8.8 Energy Storage Systems (ESS) Uninterruptible Power Supply (UPS) Systems .

12.8.8.1*

In addition to the required engine-driven generators, ~~an ESS~~ a UPS that complies with the requirements of 12.8.8 and *NFPA 70* shall be provided.

12.8.8.2

The ~~ESS~~ UPS shall provide conditioned, uninterrupted power to telecommunications equipment, two-way radio systems, IT equipment, and other sensitive electronic equipment determined by the AHJ to be essential to the operation of the emergency communication systems.

12.8.8.3*

The ~~ESS~~ UPS shall be sized to carry the connected load for the length of time required to transfer operations to the alternate communications center as determined by the AHJ in connection with the CEMP, but in no case less than 15 minutes (Class 0.25.)

12.8.8.4

The ~~ESS~~ UPS shall provide performance equivalent to Type O or Type U stored emergency power supply system (SEPSS) as specified in Table 4.2.2 of NFPA 111.

12.8.8.5

The ~~ESS~~ UPS shall meet the SEPSS requirement for Level 1 as defined by NFPA 111.

12.8.8.6

Each ~~ESS~~ UPS shall be provided with a bypass switch that maintains the power connection during switchover and that is capable of isolating all ~~ESS~~ UPS components while allowing power to flow from the source to the load.

12.8.8.7

The following ~~ESS~~ UPS conditions shall be annunciated in the operations room:

- (1) Source power failure, overvoltage, and undervoltage
- (2) High and low battery voltage
- (3) ~~ESS~~ UPS in bypass mode

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 13:59:30 EST 2020

Committee Statement

Committee Statement: A UPS is a distinct type of ESS and has very different performance requirements, including a separate UL listing standard. A UPS is listed to UL 1776, and an ESS is listed to UL 9540. In the context of this section, the proper operation of the emergency services communications center requires a UPS, not an ESS, which may or may not have the proper protective switching and filtering characteristics.

Response Message: SR-25-NFPA 1225-2020

[Public Comment No. 33-NFPA 1225-2020 \[Section No. 12.8.8\]](#)



Second Revision No. 63-NFPA 1225-2020 [Section No. 12.11.2.5]

12.11.2.5

Remote communications facilities shall be evaluated for wildland interface hazards in accordance with ~~NFPA 1144~~ [NFPA 1140](#) .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Thu Nov 19 11:13:07 EST 2020

Committee Statement

Committee Statement: NFPA 1144 has been consolidated into NFPA 1140.

Response Message: SR-63-NFPA 1225-2020



Second Revision No. 66-NFPA 1225-2020 [Section No. 14.6.2]

14.6.2

Lightning protection shall be in accordance with Section ~~12.9~~ [12.10](#) .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Sun Dec 06 21:04:59 EST 2020

Committee Statement

Committee Statement: Referenced section corrected.

Response Message: SR-66-NFPA 1225-2020



Second Revision No. 26-NFPA 1225-2020 [Section No. 15.4.2.2]

15.4.2.2

The initial recipient of the call shall remain on the line until ~~it is certain that the transfer is completed~~ the receiving agency answers the call .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 14:21:38 EST 2020

Committee Statement

Committee Statement: The best practice is to remain on the line to ensure contact with the receiving agency is made.

Response Message: SR-26-NFPA 1225-2020

Public Comment No. 13-NFPA 1225-2020 [Section No. 15.4.2.2]



Second Revision No. 27-NFPA 1225-2020 [Section No. 15.4.4.1]

15.4.4.1

The following types of calls where there is an imminent threat to life shall be included in the highest prioritization level:

- (1) Trauma (e.g., penetrating chest injury)
- (2) Neurologic emergencies (e.g., stroke, seizure)
- (3) Cardiac-related events
- (4) Unconscious/unresponsive patients
- (5) Allergic reactions
- (6) Patient not breathing
- (7) Choking
- (8) Other calls as determined by the AHJ

15.4.4.2

The following types of calls where significant property loss/damage is likely or actively occurring shall be included in the highest prioritization level:

- (1) Fire involving or potentially extending to a structure(s)
- (2) Explosion
- (3) Other calls as determined by the AHJ

15.4.4.3

Where the communications center employs a call prioritization system, the use of selected categories, groups, or codes from that system, as approved by the AHJ, shall be included in the highest prioritization level, in conjunction with 15.4.4.1 and 15.4.4.2 .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 14:26:03 EST 2020

Committee Statement

Committee Statement: The defined types of calls lack specificity and could inappropriately include calls as 'highest priority' when they might not be. The inclusion of call prioritization systems permits flexibility.

Response SR-27-NFPA 1225-2020

Message:

Public Comment No. 25-NFPA 1225-2020 [Sections 15.4.4.1, 15.4.4.2]



Second Revision No. 28-NFPA 1225-2020 [Section No. 15.4.4.4]

15.4.4.5

The following types of mitigating circumstances shall be exempted from the requirements of 15.4.4:

- (1) Language translation
- (2) TTY/TDD
- (3)* Incomplete location

A.15.4.4.5(3)

Each agency has access to different technology and location tools and references. In many cases, additional location interrogation or questioning is required by the call taker. Scenarios to consider when determining whether incomplete location information is a mitigating circumstance can include the following:

- (a) The caller does not know or cannot provide the full address.
 - (b) The caller does not know or cannot provide the full address, but the call taker received the call with a Phase 2 location.
 - (c) The call comes in as Phase 1 (cell tower address), and the call taker has to rebid to get a Phase 2 location.
 - (d) The call taker must use technology tools to find a location (e.g., search engines, third-party location services, CAD history, motor vehicle database).
 - (e) The caller says "hold on" while looking for an address.
 - (f) The caller can provide a common business name but does not have the physical address.
 - (g) The caller needs guidance or direction in finding an address.
 - (h) The location interrogation takes longer than a specified time frame (e.g., automatic exemption after specific time frame).
- (4) SMS message to 9-1-1
 - (5) Calls received from outside the normal area of responsibility and/or service area
 - (6) Calls requiring use of a PSAP registry or similar tool to determine the appropriate PSAP and/or transfer location
 - (7) Calls received during a significant disaster that severely and significantly depletes available resources, impacts local infrastructure, and could result in changes to normal dispatcher procedures (disaster mode)

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR-28_A.15.4.4.4_3_.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 14:57:30 EST 2020

Committee Statement

Committee Statement: The new annex material provides guidance on what constitutes "incomplete location."

Response Message: SR-28-NFPA 1225-2020

[Public Comment No. 14-NFPA 1225-2020 \[Section No. 15.4.4.4\]](#)



Second Revision No. 29-NFPA 1225-2020 [Section No. 17.1.1.5.1]

17.1.1.5.1

The secondary dispatch circuit shall be provided with one of, or a combination of, the following:

- (1) A wired circuit
- (2)* A designated radio channel, with the following provision:
 - (a)* If radio is used for both the primary and secondary dispatch circuits, the following shall apply:
 - i. The primary dispatch circuit shall comply with 17.1.1.4
 - ii. The secondary dispatch circuit shall consist of a separate radio system operating on a separate channel with a separate receiver for the secondary circuit at each ERF.
- (3) An approved dedicated telephone circuit, with the following provision:
 - (a)* Where a telephone dispatch circuit is used as a primary dispatch circuit, a telephone circuit shall not be used as the required secondary dispatch circuit in conjunction with the following:
 - i. The dispatch signal circuit path for the secondary dispatch circuit specified in 17.1.1.5.1(3)(a) shall be separate and independent of the dispatch signal circuit path of the primary dispatch circuit from the dispatch console to separate control/relay switching equipment connection ports at the ERF.
 - ii. A telephone connection through a public-switched telephone network via a regular dial-up modem and nondedicated telephone line shall not be considered to be an approved dispatch circuit.
- (4) An Internet-connected device, with the following provision:
 - (a) Where ~~an~~ a wired or wireless Internet-connected device is used as a secondary dispatch circuit, a mechanism shall be in place to confirm to the AHJ that alerting messaging has been received by the device at the ERF or ERU.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR29_17.1.1.5.1.docx	staff use

Submitter Information Verification

Committee: PUF-AAA
Submittal Date: Tue Nov 10 15:34:15 EST 2020

Committee Statement

Committee Statement: The revised text ensures that public safety broadband communications meet the same in-building standards as other technologies.
Response Message: SR-29-NFPA 1225-2020

[Public Comment No. 53-NFPA 1225-2020 \[Section No. 17.1.1.5.1\]](#)



Second Revision No. 30-NFPA 1225-2020 [Section No. 17.6.2.4]

17.6.2.4

Commercial networks used ~~to~~ for secondary alerting systems; shall have the ability to prioritize alerting messaging above nonemergency traffic.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 15:47:41 EST 2020

Committee Statement

Committee Statement: The grammar is corrected to clarify the requirement.

Response Message: SR-30-NFPA 1225-2020



Second Revision No. 48-NFPA 1225-2020 [Section No. 18.1]

18.1 General.

18.1.1

All system components shall be designed, installed, tested, inspected, and maintained in accordance with the manufacturers' published instructions and the requirements of Chapter 18.

18.1.2

The requirements of other chapters shall not apply to in-building emergency responder communications enhancement systems except where specifically referenced.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 19:29:17 EST 2020

Committee Statement

Committee Statement: The migration of communications enhancement systems from NFPA 72 to NFPA 1221 has caused confusion whether the requirements in other chapters are applicable to these systems. The new text clarifies the committee's intent that only Chapter 18 is applicable.

Response: SR-48-NFPA 1225-2020

Message:



Second Revision No. 9-NFPA 1225-2020 [Section No. 18.2]

18.2 Approval.

18.2.1*

Where ~~a~~ an in-building emergency responder communications enhancement system is used, the design of the system shall be approved by the AHJ and the frequency license holder(s) .

A.18.2.1

In many countries, the frequency license holder(s) is legally responsible for retransmission on the frequencies to which the licensee is licensed by the licensing authority of the country of jurisdiction. Therefore, the frequency license holder(s) must be able to review and approve every ERCES design prior to the commencement of any ERCES installation. The purpose of the initial review is to determine if the design, equipment selection, and overall solution will properly operate and not cause interference on the public safety land mobile radio system. For example, in the United States, this is covered in 47 CFR, *Federal Communications Commission* .

The design submitted for approval should consist of the following, as appropriate for the design :

- (1) ~~Local off-air~~ DAQ signal source level measurements in a format acceptable to the AHJ [e.g., DAQ, bit error rate (BER), signal to interference noise ratio (SINR)]
- (2) Local code requirements and statement of compliance
- (3) Building site plan, building floor plans, and elevation plans
- (4) Donor RF link path profiles, link budgets, azimuths, and distances
- (5) Donor antenna mounting details and donor antenna cable installation details
- (6) Grounding and surge suppression details
- (7) ~~Riser block and level~~ Backbone and distribution antenna cable diagrams
- (8) Device locations on floor plans
- (9) Pathway survivability design as applicable
- (10) Primary and backup power distribution design and wiring
- (11) Backup power calculations
- (12) Monitoring system design including ~~FACP~~ fire alarm control unit (FACU) interfaces and annunciators
- (13) Donor/DAS antenna isolation calculations
- (14) ~~Signal coverage prediction (i.e., heat)~~ Pre-installation predictive DAQ or signal coverage maps on floor plans
- (15) Designer qualifications
- (16) Installer qualifications
- (17) Test grids on floor plans, or walk plan if approved by AHJ
- (18) ~~Manufacturers~~ Manufacturers' specification sheets (i.e., cut sheets) for all equipment and cable

18.2.2

The design of the system shall be performed by a RF system designer.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR-9_18.2.docx	staff use

Submitter Information Verification

Committee: PUF-AAA
Submittal Date: Mon Nov 09 12:54:02 EST 2020

Committee Statement

Committee Statement: The frequency license holder(s) should be included in the system design approval process, since they have the legal responsibility for the use of the frequency(s).
Response Message: SR-9-NFPA 1225-2020

Public Comment No. 19-NFPA 1225-2020 [Section No. A.18.2]
Public Comment No. 93-NFPA 1225-2020 [Section No. 18.2]



Second Revision No. 10-NFPA 1225-2020 [Section No. 18.3.2]

18.3.2* Oscillation Detection and Control.

~~Bi-directional amplifiers (BDAs)~~ Signal boosters used in emergency responder ~~radio coverage~~ communications enhancement systems shall have built-in oscillation detection and control circuitry to reduce gain and maintain operation.

A.18.3.2

Mandating oscillation detection and control does not ensure the equipment will maintain operation to the best extent possible during an emergency. If a signal booster shuts down during oscillation that could leave emergency personnel stranded without communications coverage during an emergency. Oscillation is caused by the reduction in isolation between the inside and outdoor donor antennas. An event such as fire or earth movement can cause damage to the building, thereby reducing the isolation between the inside antennas and the outside donor antenna. If the signal booster were to reduce gain until oscillation is no longer present, there would be some level of communications coverage.

18.3.2.1

When a signal booster detects oscillation, a supervisory signal shall be transmitted.

18.3.2.2

In the event of uncorrectable oscillation, the system shall be permitted to shut down.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 14:39:59 EST 2020

Committee Statement

Committee Statement: The text is revised to clarify signal booster oscillation protection operation in order to limit the ability of the signal booster to shut down, thereby leaving first responders without any radio communications capability.

Response SR-10-NFPA 1225-2020

Message:

Public Comment No. 107-NFPA 1225-2020 [Section No. 18.3.2]

Public Comment No. 16-NFPA 1225-2020 [Section No. 18.3.2]



Second Revision No. 11-NFPA 1225-2020 [Section No. 18.3.4]

18.3.4 Radio- Communication Antenna Density.

18.3.4.1*

In-building ~~two-way~~ emergency responder communication enhancement systems shall be ~~engineered~~ designed to minimize the near-far effect.

A.18.3.4.1

Near-far problems arise when a ~~passive~~ distributed antenna system (DAS) is not designed correctly, ~~and is~~ These problems are caused ~~when by~~ a transmission from a portable radio that is ~~really close (i.e., near) to~~ near a DAS antenna, ~~and it overpowers~~ overpowering the uplink amplifier. When this occurs, the ~~near portable radio uses up the available gain of the bi-directional amplifier (BDA)~~ strong signal forces the amplifier into a reduced gain situation, so that another transmission that is happening at the same time Other portables transmitting simultaneously on a different frequency channel(s), far away from a radio that is further away from a DAS antenna (i.e., far radio) would not be amplified as much. The near-far problem can be an issue with an improperly design class A channelized or ~~Class B broadband BDAs~~ the antenna system, will not be provided the gain necessary to achieve adequate uplink communications.

18.3.4.2

In-building ~~two-way~~ emergency responder communication enhancement system designs shall include a sufficient number of distribution antennas (density) to address reduced gain conditions.

18.3.4.3

Where an in-building ~~two-way~~ emergency responder communication enhancement system is required and such system, components, or equipment has a negative impact on the normal operations of the facility at which it is installed, the AHJ shall have the authority to accept an automatically activated responder system.

Supplemental Information

<u>File Name</u>	<u>Description</u> <u>Approved</u>
1225_PUF_SR11_18.3.4.docx	STAFF USE

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 14:46:21 EST 2020

Committee Statement

Committee Statement: The text is revised to use updated terminology. The annex material is revised to more clearly explain the near-far effect.

Response Message: SR-11-NFPA 1225-2020

Public Comment No. 17-NFPA 1225-2020 [Section No. 18.3.4]



Second Revision No. 12-NFPA 1225-2020 [Section No. 18.4]

18.4* Lightning Protection.

Systems shall have lightning protection that complies with ~~NFPA 780~~ 18.4.1 through 18.4.4.

18.4.1

The donor antenna coaxial cable(s) shall be protected by antenna discharge units in accordance with Article 820 of *NFPA 70*.

18.4.2

The antenna discharge units shall be listed to UL 497C, *Standard for Protectors for Coaxial Communications Circuits*.

18.4.3

Each donor antenna coaxial cable(s) shall be provided with a listed antenna discharge unit in accordance with Article 820 of *NFPA 70*.

18.4.4

The antenna, antenna mast, and antenna discharge unit(s) shall be grounded in accordance with Article 820 of *NFPA 70*.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 15:04:38 EST 2020

Committee Statement

Committee Statement: The Committee revises the text to specify the correct NFPA standard that provides lightning protection for In-Building Emergency Responder Communications Enhancement Systems. This change is needed because the scope of NFPA 780 covers lightning protection of the structure and not the equipment inside the structure. Specifically, 1.1.2 of NFPA 780 states the document shall address lightning protection of the structure but not the equipment or installation requirements for electric generating, transmission, and distribution systems except as given in Chapter 9 and Chapter 12. Chapter 9 details requirements for Wind Turbines and Chapter 12 details requirements for Solar Arrays. The problem is many buildings are not required to have NFPA 780 compliant lightning protection systems. The cost to protect an entire building in accordance with NFPA 780 can be many times the cost of an In-Building Emergency Responder Communications Enhancement System.

Response Message: SR-12-NFPA 1225-2020

Public Comment No. 102-NFPA 1225-2020 [Section No. 18.4]



Second Revision No. 2-NFPA 1225-2020 [Section No. 18.6.1]

18.6.1*

No in-building emergency responder communications enhancement system capable of operating on frequencies or causing interference to frequencies assigned to the jurisdiction by the licensing authority of the country of jurisdiction shall be installed without prior coordination and approval of the AHJ and the frequency license holder(s).

A.18.6.1

Frequencies and modulation technologies utilized by emergency services are assigned by the licensing authority of the country of jurisdiction. In the US, for example, the FCC assigns frequencies that may be utilized by emergency services. Typically, these are thought of in the VHF, UHF, and 700/800 MHz bands. More recently, the US government created a nationwide public safety broadband network for use by emergency services. As more jurisdictions utilize non-traditional broadband networks for emergency service operations the need to have those capabilities as a part of the in-building emergency responder communications enhancement system will be important for incident operations. It is important to understand that to enhance coverage of any commercial carrier broadband signal, prior coordination and approval must be obtained from the frequency license holder of those frequencies.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 10:56:45 EST 2020

Committee Statement

Committee Statement: The NPSBN is one of several frequencies and modulation technologies that may be available for use by public safety agencies within a jurisdiction.

Response Message: SR-2-NFPA 1225-2020

Public Comment No. 42-NFPA 1225-2020 [Section No. 18.6.1]



Second Revision No. 4-NFPA 1225-2020 [Section No. 18.6.2]

18.6.2

The building owner or authorized agent shall suspend and correct equipment installations that degrade the performance of the public safety ~~radio~~ communications system or ~~public safety radio~~ emergency responder communications enhancement system.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 11:15:16 EST 2020

Committee Statement

Committee Statement: The Committee creates a second revision to make the language to align with other terms uses within the standard by inserting the term communications it allows for the use of NPSBN as well as other commercial carriers.

Response SR-4-NFPA 1225-2020

Message:

Public Comment No. 43-NFPA 1225-2020 [Section No. 18.6.2]



Second Revision No. 6-NFPA 1225-2020 [Section No. 18.6.3]

18.6.3*

Systems that share infrastructure with non-public safety services shall ensure that the coverage and performance of the public safety communications channels are not degraded below the level of performance identified in Sections 18.8 and 18.9, regardless of the amount of traffic carried by the non-public safety services.

A.18.6.3

Use of shared commercial and public safety systems on the same in-building communications enhancement system infrastructure should be evaluated to ensure that systems and technology provide optimized operational capabilities. Multiple DAS systems, whether combined or not, need to be designed and configured to avoid interference with each other and with other building RF systems.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 12:01:38 EST 2020

Committee Statement

Committee Statement: New annex material is added to ensure that all stakeholders carefully evaluate combining commercial and public safety technologies within in-building communications enhancement systems.

Response Message: SR-6-NFPA 1225-2020

Public Comment No. 31-NFPA 1225-2020 [New Section after A.18.4]



Second Revision No. 7-NFPA 1225-2020 [Section No. 18.7.2]

18.7.2*

~~A renewable permit or written~~ Written authorization by the frequency license holder shall be ~~issued for the public safety radio~~ required upon initial installation and prior to activation of the emergency responder communications enhancement system where required by the AHJ.

A.18.7.2

Written consent from the radio frequency licensing authority could be required in some areas. An example of where the radio frequency licensing authority could require express written consent is through the FCC in the United States. The FCC rule Title 47, CFR, Part 90.219(b) states, in part, the following:

Authority to operate. Private land mobile radio service (PLMRS) licensees for stations operating on assigned channels higher than 150 MHz may operate signal boosters, limited to the service band for which they are authorized, as needed anywhere within the PLMRS stations' service contour, but may not extend the stations' service contour.

(1) PLMRS licensees may also consent to operation of signal boosters by non-licensees (such as a building owner or a signal booster installation contractor) within their service contour and across their applicable frequencies, but must maintain a reasonable level of control over these operations in order to resolve interference problems.

(a) Non-licensees seeking to operate signal boosters must obtain the express consent of the licensee(s) of the frequencies for which the device or system is intended to amplify. The consent must be maintained in a recordable format that can be presented to an FCC representative or other relevant licensee investigating interference.

(b) Consent is not required from third party (unintended) licensees whose signals are incidentally retransmitted. However, signal booster operation is on a non-interference basis and operations may be required to cease or alter the operating parameters due to a request from an FCC representative or a licensee's request to resolve interference.

18.7.3

Where required by the AHJ, a renewable permit shall be issued for the operation of an emergency responder communications enhancement system.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 12:24:19 EST 2020

Committee Statement

Committee Statement: Renewable permits and written authorization are two different components of the existing requirement and needed different treatment. When written authorization from the frequency license holder(s) is required by authority granting the license, it shall be obtained before activating the ERCES.

Response Message: SR-7-NFPA 1225-2020

Message:

Public Comment No. 45-NFPA 1225-2020 [Section No. 18.7.2]

[Public Comment No. 98-NFPA 1225-2020 \[Section No. 18.7\]](#)



Second Revision No. 13-NFPA 1225-2020 [Section No. 18.9]

18.9* Signal Strength and Quality .

A.18.9

Many radio systems are in use by public safety agencies in the United States. A number of them have different operational characteristics. A prescribed signal strength measurement might not produce usable voice communications for all systems { [e.g., VHF, UHF, 700/800 MHz, analog, P-25, 4 slot time division multiple access (TDMA) , 2 slot TDMA, etc.}] . Requiring the AHJ to provide operational parameters required for usable voice communications for the systems in use eliminates possible confusion regarding the specified value, as determined by the AHJ. A better indicator of proper system performance and coverage is to use the DAQ audio quality measurement system whether the signals are either analog or digital.

18.9.1* Inbound Downlink .

A minimum inbound downlink signal strength shall be sufficient to provide usable voice communications, as specified by the AHJ, shall be provided a minimum of DAQ 3.0 for voice communications using either narrowband, analog, or digital P25 signals or wideband LTE digital signals throughout the coverage area. (See A.20.3.10 .)

A.18.9.1

~~Inbound (or downlink) is commonly referred to as~~ Downlink refers to the signal from the base station to the portable. ~~Although DAQ 3.0 is required as a minimum, it is recommended that systems be designed for DAQ 3.4 to provide a safety factor .~~

~~18.9.1.2~~

~~The inbound signal level shall be sufficient to provide a minimum of DAQ 3.0 for either analog or digital signals.~~

18.9.2* Outbound Uplink .

The uplink signal shall be sufficient to provide a minimum of DAQ 3.0 for voice communications using either narrowband, analog, or digital P25 signals or widespread LTE digital signals. (See A.20.3.10 .)

A.18.9.2

~~Outbound (or uplink) is commonly referred to as~~ Uplink refers to the signal from the portable to the base station.

~~18.9.2.1~~

~~A minimum outbound strength sufficient to provide usable voice communications, as specified by the AHJ, shall be provided throughout the coverage area.~~

~~18.9.2.2~~

~~The outbound signal level shall be sufficient to provide a minimum of DAQ 3.0 for either analog or digital signals.~~

18.9.3* Noise Floor.

If the design of the in-building emergency responder communications enhancement system (ERCES) requires the use of a signal booster, then the maximum uplink RF noise (noise crown) created by any signal booster or signal booster-based ERCES shall not raise the noise floor at the public safety communications site closest to the ERCES or any receiving site within the public safety communications network that the ERCES is intended to operate with.

A.18.9.3

Receiver noise floor testing can be accomplished by first noting the idle noise on all channels involved within the public safety communications system at the public safety communications site closest to the ERCES with the signal booster system off. This can be done by using a spectrum analyzer with the resolution bandwidth set to be equal or less than the noise bandwidth of the receiver used at the site. Note: Use 10 kHz for 12.5 kHz narrowband systems, and use 10 kHz for 25 kHz systems at 800 MHz in the US.

The spectrum analyzer's input should be connected to the public safety communications site receiver multi-coupler so that it is exposed to the same noise environment as the site receivers. Note that this setup would be the same regardless if the public safety communications system is a trunked or conventional system.

The signal booster systems should then be powered on and idle noise levels at the closest public safety communications site to the ERCES should be noted. If the noise level(s) is raised by 1 dB or more at the nearest public safety communications site when the signal booster is active, then an attenuator or gain change should be executed at the signal booster site until the noise power drops back to the idle level noted when the signal booster was inoperative.

An additional 3 dB of attenuation or gain reduction should be added to the signal booster installation once the noise level has been reduced to the idle level measurement made. This should be done to provide a safety factor. This step should be performed prior to the signal booster activation authorized by the AHJ and the frequency license holder(s).

The setting(s) of the ERCES gain should be documented on the as-built documents.

If an LTE network is the source of the signal, the LTE service provider should deliver the noise requirements and measuring process to the integrator or installation company. Measuring should be conducted during quieter times for the public safety communications system as determined by the AHJ and the frequency license holder(s). The test should be conducted for a period of 5 minutes, and the average noise over that period should be used for the noise level at the site.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR13_18.9.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 15:25:13 EST 2020

Committee Statement

Committee Statement: The revisions in 18.9.1 and 18.9.2 replace the terms Inbound and Outbound with Downlink and Uplink and add absolute signal strength value for analog and digital systems.

The new section, 18.9.3, provides additional detail to be measurable, repeatable, and

enforceable. The amount of increase in the noise floor is defined, as well as where it should be measured. The Committee also added Annex material to guide AHJs and others as to how and when to measure the noise floor.

Response SR-13-NFPA 1225-2020

Message:

[Public Comment No. 122-NFPA 1225-2020 \[Section No. 18.9\]](#)

[Public Comment No. 32-NFPA 1225-2020 \[New Section after 18.9.2.2\]](#)



Second Revision No. 5-NFPA 1225-2020 [Section No. 18.11]

18.11* Frequencies.

The in-building emergency responder communications enhancement system: shall be capable of transmitting on all radio frequencies, as required by the AHJ ~~assigned to the jurisdiction~~, and be capable of using any modulation technology in current use by the public safety agencies in the jurisdiction.

A.18.11

Newer transmission technologies, such as LTE and 5G, will dramatically change the capability of public safety communications systems.

18.11.1 List of Assigned Frequencies.

The AHJ and the frequency license holder(s) shall each maintain a list of all ~~inbound/outbound~~ downlink/uplink frequency pairs for distribution to system designers.

18.11.2* Frequency Changes.

18.11.2.1

Systems shall be upgradeable to allow for instances where the jurisdiction changes or adds system frequencies to maintain ~~radio~~ communication system coverage as it was originally designed.

18.11.2.2

Where frequency changes occur and systems are upgraded, they shall comply with 18.6.1.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 11:20:54 EST 2020

Committee Statement

Committee Statement: The Committee revises the language to accomplish three objectives:

1. Add annex to clarify modulation technologies may include but are not limited to LTE or 5G
2. To ensure the frequency license holder(s) are include in the processes involving frequencies
3. Replace the terms inbound and outbound with common industry terms downlink and uplink

Response Message: SR-5-NFPA 1225-2020

[Public Comment No. 50-NFPA 1225-2020 \[Section No. 18.10\]](#)

[Public Comment No. 51-NFPA 1225-2020 \[Section No. 18.11.2\]](#)

[Public Comment No. 47-NFPA 1225-2020 \[Section No. 18.8\]](#)

[Public Comment No. 100-NFPA 1225-2020 \[Section No. 18.11\]](#)

[Public Comment No. 44-NFPA 1225-2020 \[Section No. 18.6.3\]](#)

[Public Comment No. 123-NFPA 1225-2020 \[Section No. 18.11.1\]](#)



Second Revision No. 64-NFPA 1225-2020 [Section No. 18.12.1.1]

18.12.1.1

RF-emitting devices and cabling used in the installation of the ~~public safety~~ in-building emergency responder communications enhancement system shall be approved by the AHJ.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Fri Nov 20 17:58:26 EST 2020

Committee Statement

Committee Statement: This revision was developed by NFPA staff for editorial purposes, in accordance with 4.4.9.6.2 and 4.4.9.6.3 of the Regulations Governing the Development of NFPA Standards (nfpa.org/regs).

The section is revised to use consistent terminology.

Response Message: SR-64-NFPA 1225-2020



Second Revision No. 8-NFPA 1225-2020 [Section No. 18.12.2]

18.12.2 Active RF-Emitting Devices.

Active RF-emitting devices shall meet the following requirements in addition to any other requirements determined by the AHJ or the frequency license holder(s) :

- (1) Active RF-emitting devices that have a transmitted power output sufficient to require certification of the frequency licensing authority shall have the certification of the radio frequency licensing authority prior to installation.
- (2) All active RF-emitting devices shall be compatible ~~with both analog and digital communications~~ for their intended use , as required ~~to be used~~ by the radio frequency licensing authority, the frequency license holder(s), and the AHJ, simultaneously at the time of installation.
- (3) Written authorization shall be obtained from the frequency license holder(s) prior to the initial activation of any RF-emitting devices required to be certified by the frequency licensing authority.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 12:41:10 EST 2020

Committee Statement

Committee Statement: The committee creates a second revision to align the terminology within the section with other sections of the standard. Additionally, the committee determined that modifications needed to be made in item (2) to clarify that RF emitting devices must be compatible for their intended use. Furthermore, the committee determined that the testing requirements for broadband communication did not belong in this section of the standard.

The installation of an in-building emergency responder communications enhancement system (ERCES) is not a simple plug and play solution. The activation of in-building Active RF Emitting Devices which are certifiable can have a significant impact on the entire public safety land mobile radio (LMR) system network if not properly designed and installed. A portion of that design is knowing the critical aspects of the LMR system that the ERCES installation is trying to enhance. Equally important to the design is knowing the location of other nearby ERCES installations operating in other buildings. The failure to know and factor into the design of a system this critical information will create interference on the LMR system thereby placing the safety of the first responders at risk. Requiring written authorization from the frequency license holder(s) before turning up an ERCES assures that the all the critical factors associated with the local LMR system have been factored into the installation in order to reduce system interference.

Response SR-8-NFPA 1225-2020

Message:

[Public Comment No. 52-NFPA 1225-2020 \[Section No. 18.12.2\]](#)

[Public Comment No. 109-NFPA 1225-2020 \[Section No. 18.12.2\]](#)



Second Revision No. 14-NFPA 1225-2020 [New Section after 18.12.3.1]

18.12.3.2

Mechanical protection of work and raceways for coaxial cables shall comply with Article 820 of NFPA 70 .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 16:01:30 EST 2020

Committee Statement

Committee Statement: The new text clarifies that the mechanical protection of backbone cables, backbone cable components, and distribution antenna cables is required where they are subject to physical damage. All cable does not need to be in conduit, only cables in areas subject to physical damage.

Response Message: SR-14-NFPA 1225-2020

Public Comment No. 105-NFPA 1225-2020 [New Section after 18.12.3.1]



Second Revision No. 15-NFPA 1225-2020 [Section No. 18.12.3.2]

~~18.12.3.3~~

~~The backbone cables shall be connected to the antenna distribution, radiating, or copper cables using coupler or splitter devices of a value determined by the overall design.~~

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 16:04:47 EST 2020

Committee Statement

Committee Statement: The Committee deletes this section because it is not necessary. The types of cables, couplers, and splitters are determined by the RF system designer.

Response Message: SR-15-NFPA 1225-2020

Public Comment No. 30-NFPA 1225-2020 [Section No. 18.12.3.2]

Public Comment No. 103-NFPA 1225-2020 [Section No. 18.12.3.2]



Second Revision No. 16-NFPA 1225-2020 [Sections 18.12.3.3, 18.12.3.4, 18.12.3.5, 18.12.3.6]

18.12.3.3

Backbone cables and backbone cable components installed in buildings that are fully protected by an automatic sprinkler system in accordance with NFPA 13 shall ~~be installed in metal raceways~~ not be required to have a fire resistance rating .

18.12.3.4*

Backbone cables and backbone cable components installed in nonsprinklered buildings ~~or, in buildings that are partially protected by a sprinkler system, or in high-rise buildings~~ shall be protected from attack by fire in accordance with one of the following:

- (1) ~~Listed with a~~ Use a cable with a listed fire-resistance rating in accordance with the following:
 - (a) Where the primary structural frame of a building is required to have a fire-resistance rating of 2 hours or more or is classified as heavy timber construction, the minimum fire-resistance rating shall be 2 hours.
 - (b) Where the primary structural frame of a building is required to have a fire-resistance rating of less than 2 hours, the minimum fire resistance rating shall be 1 hour.
 - (c) Where the primary structural frame of a building does not require a fire-resistance rating, a fire resistance rating shall not be required.
- (2) ~~Protected by an assembly having~~ A protected enclosure or area shall have a fire-resistance rating in accordance with the following:
 - (a) Where the primary structural frame of a building is required to have a fire-resistance rating of 2 hours or more or is classified as heavy timber construction, the minimum fire-resistance rating shall be 2 hours.
 - (b) Where the primary structural frame of a building is required to have a fire-resistance rating of less than 2 hours, the minimum fire resistance rating shall be 1 hour.
 - (c) Where the primary structural frame of a building does not require a fire-resistance rating, a fire resistance rating shall not be required.

18.12.3.5

Where backbone cables and distribution antenna cables are run in a fire-resistant enclosure or protected area , both of the following shall apply, except as permitted in 18.12.3.6 :

- (1) The connection between the backbone cable and the distribution antenna cables shall be made within an enclosure or protected area identified in 18.12.3.4.
- (2) Passage of the distribution antenna ~~distribution~~ cable in and out of the enclosure or protected area shall be fire-stopped to an equivalent rating of the enclosure or protected area .

18.12.3.6

If both the backbone cables and the backbone cable components are fire rated in accordance with 18.12.3.4, the connection of the distribution antenna ~~distribution~~ cable shall not be required to be made within an enclosure or protected area .

Supplemental Information

File Name

Description Approved

1225_PUF_SR16_18.12.3.3-18.12.3.6.docx staff use

Submitter Information Verification

Committee: PUF-AAA**Submittal Date:** Mon Nov 09 16:08:29 EST 2020

Committee Statement

Committee Statement: The issue of backbone cable survivability from fire was thoroughly discussed during the SD meeting because the ability to transmit clear and understandable radio frequency (RF) voice messages inside buildings during emergency conditions is a safety concern for emergency responders. The Committee creates a second revision, so backbone cables and backbone cable components are protected from the attack by fire with reasonable requirements that are consistent with the structural integrity of the building in which they are installed.

Section 18.12.3.3 was revised for the following reasons:

- Backbone cables are not protected from attack by fire when installed in metal conduit. Metal conduit only provides physical protection of the cable.
- Installing backbone cables in conduit adds unnecessary cost to the installation of the system without improving the performance or solving a known problem that is occurring in the field.

Section 18.12.3.4 was revised for the following reasons:

- There needs to be a specified fire-resistance rating for backbone cables as it relates to the structural frame rating of the building.
- Backbone cables and backbone cable components shall have the same level of protection from attack by fire if they are installed in a fire rated enclosure or if the cable itself has a fire-resistant rating.
- Previous editions of NFPA standards provided language that stated contained language that said, "Where a two-way radio communications enhancement system is used in lieu of a two-way in-building wired emergency communications system, it shall have a pathway survivability of Level 1, Level 2 or Level 3." Wired two-way in-building emergency communications systems were required in high-rise structures, not all structures. This proposed change continues to require pathway survivability for high rise structures while understanding that other types of building structures may not need the same level of survivability. This proposed modification is to clarify the intent of protecting the backbone cable and backbone cable components while balancing the cost associated with these systems.
- The findings of a NFPA Fire Protection Research Foundation (FPRF) literature review titled Temperature Rating of Two-Way Radio Communications Enhancement Systems. This report concluded that technical data does not exist as it relates to temperatures at which critical voice messages being transmitted by the public safety responders on an ERCES system backbone cables/connectors will be impacted from fire to the point where the voice messages are no longer intelligible. Therefore, there was never any technical substation to require a two-hour survivability requirement for the types of cables used within an ERCES.
- The performance of an ERCES backbone cables ability to propagate radio frequency when exposed to heat conditions is much different than standard AC/DC type fire alarm cables and therefore ERCES cable cannot be looked at in the same concept.
- A new project request has been sent to FPRF to perform actual fire testing to determine

the impact of temperature RF cables and connectors.

Section 18.12.3.4(2), 18.12.3.5 and 18.12.3.6 were revised to replace the term “assembly” with “enclosure or protected area” because the term is used in NFPA 72 to describe how to protect cables without a fire-resistance rating from attack by fire.

Response SR-16-NFPA 1225-2020

Message:

[Public Comment No. 1-NFPA 1225-2020 \[Section No. 18.12.3.4\]](#)

[Public Comment No. 3-NFPA 1225-2020 \[Section No. 18.12.3.3\]](#)

[Public Comment No. 104-NFPA 1225-2020 \[Sections 18.12.3.3, 18.12.3.4, 18.12.3.5, 18.12.3.6\]](#)



Second Revision No. 17-NFPA 1225-2020 [Section No. 18.14]

18.14 System Monitoring.

18.14.1 Fire Alarm System.

18.14.1.1

The system shall include automatic supervisory signals for malfunctions of the in-building emergency responder communications enhancement system that are annunciated by the fire alarm system in accordance with *NFPA 72*.

18.14.1.2

The system shall comply with all of the following:

- (1) Monitoring for integrity of the system shall comply with Chapter 10 of *NFPA 72*.
- (2) System supervisory signals shall include the following:

(a)* ~~Donor antenna~~ Signal source malfunction

A.18.14.1.2(2)(a)

The signal source for an in-building emergency responder communications enhancement system is critical to keep the system operational. Loss or reduction of the RF signal from the public safety radio communications system to the in-building communications enhancement system can take multiple forms, depending on the nature of the signal source. In systems that use a RF link between the two sites, the disconnection of the antenna coax, a short in the coax, a damaged coax, or a misdirected donor antenna can cause a degradation of RF signals such that the in-building system will not work correctly. If the source of the signal is a fiber optic cable between the sites, then damage to that cable can cause loss of signal as well.

- (b) Active RF-emitting device failure
- (c) Low-battery capacity indication when 70 percent of the 12-hour operating capacity has been depleted
- (d) Active system component failure
- (3) Power supply supervisory signals shall include the following for each RF-emitting device and active system components:
 - (a) Loss of normal ac power
 - (b) Failure of battery charger
- (4) The communications link between the fire alarm system and the in-building emergency responder communications enhancement system shall be monitored for integrity.
- (5) Where approved by the AHJ, a single supervisory input to the fire alarm system to monitor all system supervisory signals shall be permitted.

18.14.2 Dedicated Annunciation.

18.14.2.1

A dedicated annunciator shall be provided within the fire command center to annunciate the status of all RF-emitting devices and active system component locations. ~~This device shall provide visual and labeled indications of the following for each system component and RF-emitting device:~~

- ~~Normal ac power~~
- ~~Loss of normal ac power~~
- ~~Battery charger failure~~
- ~~Low-battery capacity (i.e., to 70 percent depletion)~~
- ~~Donor antenna malfunction~~
- ~~Active RF-emitting device malfunction~~
- ~~Active system component malfunction~~

18.14.2.2

~~This device~~ The annunciator shall provide visual and labeled indications of the following for each system component and RF-emitting device:

- (1) Normal ac power
- (2) Loss of normal ac power
- (3) Battery charger failure
- (4) Low-battery capacity (i.e., to 70 percent depletion)
- (5) ~~Donor antenna~~ Signal source malfunction *[See A.18.14.1.2(2)(a).]*
- (6) Active RF-emitting device malfunction
- (7) Active system component malfunction

18.14.2.3

The communications link between this device and the in-building emergency responder communications enhancement system shall be monitored for integrity.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR17_18.14.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 16:18:49 EST 2020

Committee Statement

Committee Statement: The Committee creates a second revision to clarify that different RF design solutions, other than a signal booster with a donor antenna, may be utilized to solve the lack of communications coverage within a building. Therefore, the term donor antenna was changed to signal source in order to provide for other types of solutions that may be installed. Additionally, the committee determined that annex language would be needed to help explain the various components of a signal source.

Response Message: SR-17-NFPA 1225-2020

Public Comment No. 110-NFPA 1225-2020 [Section No. 18.14]





Second Revision No. 18-NFPA 1225-2020 [Section No. 18.15]

18.15 Technical Criteria.

18.15.1

The AHJ and the frequency license holder(s) shall maintain a document ~~of containing~~ technical information specific to its requirements for the installation of emergency responder communications enhancement systems .

18.15.2

The document shall include relevant information from the frequency license holder(s).

18.15.3

~~Technical~~ The AHJ technical information documents shall be ~~kept in a secure place~~ accessible to ~~maintenance personnel but not accessible to the public~~ emergency responder communications enhancement system design personnel .

18.15.4

~~Technical~~ The AHJ technical information documents shall contain, ~~as a minimum but not be limited to~~ , the following:

- (1) Frequencies and other modulation technologies required for the in-building emergency responder communications enhancement system and the point of contact for the ~~frequencies'~~ frequency license holder(s)
- (2) Location and effective radiated power (ERP) of public safety radio sites used by the ~~public safety radio~~ emergency responder communications enhancement system
- (3) Maximum propagation delay — in microseconds
- (4) Other supporting technical information necessary to direct system design

18.15.5

Where required, system design and installation documents, specifications, test results, and other records necessary to document the operation of the emergency responder communications enhancement system shall be provided.

18.15.6

The documents shall be in a format and location approved by the AHJ.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR18_18.15.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Mon Nov 09 16:38:52 EST 2020

Committee Statement

Committee The text is revised to ensure that the frequency license holder(s) are involved in the
Statement: development.

In addition, the revised text identifies that the information must be available and provided to system designers. Furthermore, the second revision clarifies that the AHJ needs to identify not just frequencies but also other modulation technologies that may be required in their jurisdiction. Many jurisdictions post their requirements on their websites and other public formats therefore the phrase "but not accessible to the public" has been removed.

Sections 18.15.5 and 18.5.6 provide language by which an AHJ can require as-built documentation and specify the location and format of the documents.

Response SR-18-NFPA 1225-2020
Message:

[Public Comment No. 4-NFPA 1225-2020 \[Section No. 18.15.2\]](#)

[Public Comment No. 111-NFPA 1225-2020 \[Section No. 18.15\]](#)

[Public Comment No. 5-NFPA 1225-2020 \[Section No. 18.15.3\]](#)



Second Revision No. 19-NFPA 1225-2020 [Section No. 20.3.10.1.3]

20.3.10.1.3

All systems initial acceptance testing documentation shall include a listing of the following:

- (1) All system equipment utilized
- (2) Manufacturer's data sheets
- (3) Installation, testing, and maintenance documentation
- (4) As-built drawings showing all equipment locations
- (5) Written documentation acceptable to the AHJ of the initial system testing, including system performance measurements at all locations covered by the installed system
- (6) Secondary power calculations
- (7) List of assigned frequencies
- (8) ~~System~~ Where signal boosters are used, system isolation test results
- (9) ~~Off-air measured~~ Measured signal source levels ~~from the donor antenna~~
- (10) Identification of the type of signal source
- (11) The settings of all frequency channels or bands subbands, channel/band gains, and filter bandwidths, and all configurable parameters of automatic gain control (AGC) modes used during the installation and testing

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR19_20.3.10.1.3.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 10:07:27 EST 2020

Committee Statement

Committee Statement: The revision clarifies that the type of signal source should be identified and measured.

Response Message: SR-19-NFPA 1225-2020 The Committee did not include the proposed (12) because 18.7.1 permits the AHJ to require propagation displays, also known as heat maps.

Public Comment No. 114-NFPA 1225-2020 [Section No. 20.3.10.1.3]



Second Revision No. 20-NFPA 1225-2020 [Section No. 20.3.10.2.1]

20.3.10.2.1

All systems that are connected to fire alarm systems that are not monitored for alarm, supervisory, and trouble conditions off site as defined by *NFPA 72* shall be visually inspected weekly for the following conditions:

- (1) Normal ac power
- (2) Loss of normal ac power
- (3) Battery charger failure
- (4) Low battery capacity
- (5) ~~Donor antenna~~ Signal source malfunction
- (6) Active RF-emitting device malfunction
- (7) Active system component malfunction
- (8) Loss of communication with the fire alarm control panel

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 10:15:46 EST 2020

Committee Statement

Committee Statement: The revision aligns item (5) with terminology used in the second revision on Section 18.14 (SR-17).

Response Message: SR-20-NFPA 1225-2020

[Public Comment No. 115-NFPA 1225-2020 \[Section No. 20.3.10.2.1\]](#)



Second Revision No. 21-NFPA 1225-2020 [Section No. 20.3.10.2.2]

20.3.10.2.2

All systems that are connected to fire alarm systems that are monitored for alarm, supervisory, and trouble conditions off site as defined by *NFPA 72* shall be visually inspected semiannually for the following conditions:

- (1) Normal ac power
- (2) Loss of normal ac power
- (3) Battery charger failure
- (4) Low battery capacity
- (5) ~~Donor antenna~~ Signal source malfunction
- (6) Active RF-emitting device malfunction
- (7) Active system component malfunction
- (8) Loss of communication with the fire alarm control panel
- (9) Signs of physical damage to components that could affect proper system operation

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 10:18:22 EST 2020

Committee Statement

Committee Statement: The revision aligns item (5) with terminology used in the second revision on Section 18.14 (SR-17).

Response Message: SR-21-NFPA 1225-2020

[Public Comment No. 116-NFPA 1225-2020 \[Section No. 20.3.10.2.2\]](#)



Second Revision No. 22-NFPA 1225-2020 [Section No. 20.3.10.2.3.2]

20.3.10.2.3.2

~~Operational Annual operational~~ tests shall include ~~at least one quantitative test of 20 percent of the system's coverage areas to ensure continuity of the system. the following:~~

- (1) At least one quantitative DAQ test shall be in accordance with 18.9.1 and 18.9.2 on each floor. Where the floor area exceeds 128,000 ft² (11,900 m²), additional quantitative tests shall be performed.
- (2)* Signal boosters shall be tested to verify that the gain is the same as it was during the initial installation and acceptance or set to optimize the performance of the system.

A.20.3.10.2.3.2(2)

If, during testing, it is found that the link budget, system design parameters, internal construction conditions, or nearby development have changed, the system should be modified to maintain the optimum performance of the system.

- (3) Backup batteries and power supplies shall be tested under load for a period of 1 hour.
- (4) Other active components shall be checked to verify operation within the manufacturer's published specifications.
- (5) All required supervisory monitoring signals shall be tested.
- (6) A spectrum analyzer or other suitable test equipment shall be utilized to ensure spurious oscillations are not being generated by the subject signal booster.
- (7) Where a donor antenna is used, isolation in accordance with Section 18.10 shall be verified.
- (8) An inspection shall be made to evaluate if the building structural changes or alternations that have been made impact the communications coverage of the system as required in Section 18.8.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR22_20.3.10.2.3.2.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 10:38:59 EST 2020

Committee Statement

Committee Statement: The revision addresses issues associated with tracking what 20% of the systems coverage area was tested during the last test. The method for tracking what was tested and by whom does not exist and there is no clear direction on where that information would be kept for easy access by the AHJ. Waiting 5 years to conduct any type of quantitative test certainly places significant concern on the ability of the system to operate for the first responders during an emergency. Therefore, providing direction for conducting

a quantitative test on each floor allows for a baseline indication of how the system is currently working on an annual basis. A complete system quantitative test would then be conducted at the 5-year interval. The reference to 128,000 square feet is currently within the annex of this document. Furthermore, the other items within this public comment seeks to add clarity to all the provisions of an annual operational test of the Emergency Responder Communication Enhancement System. The Committee adds new item 8 to address building's changes that impact communications system performance.

Response SR-22-NFPA 1225-2020

Message:

[Public Comment No. 6-NFPA 1225-2020 \[Section No. 20.3.10.2.3.1\]](#)

[Public Comment No. 108-NFPA 1225-2020 \[Section No. 20.3.10.2.3.2\]](#)

[Public Comment No. 22-NFPA 1225-2020 \[Section No. 20.3.10.2.3.2\]](#)

[Public Comment No. 117-NFPA 1225-2020 \[Section No. 20.3.10.2.3.2\]](#)



Second Revision No. 31-NFPA 1225-2020 [Section No. 22.1.3]

22.1.3

~~The plan shall include the items required by 22.1.4 through 22.1.14 :~~

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 15:56:01 EST 2020

Committee Statement

Committee Statement: The requirement is deleted because it was unnecessary. All of the requirements in the chapter must be followed.

Response SR-31-NFPA 1225-2020

Message:

[Public Comment No. 74-NFPA 1225-2020 \[Section No. 22.1.3\]](#)



Second Revision No. 32-NFPA 1225-2020 [Section No. 22.1.6.1]

22.1.5.1

The education requirements shall include at least annual training for all staff who access computer-based systems, ~~so that they can understand and prevent phishing attacks, understand virus prevention best practices with regard to passwords and other access control mechanisms, and understand HIPAA compliance procedures.~~ to include all of the following:

- (1) Information on resisting phishing attacks
- (2) Virus prevention
- (3) Dangers of the use of thumb drives
- (4) Security issues with browsing the Internet from network computers
- (5) Construction of strong passwords or use of other access control mechanisms
- (6) Confidentiality of medical and personal information

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 15:59:30 EST 2020

Committee Statement

Committee Statement: The list is reordered and converted to a numbered list for ease of use. The revision also adds some new items as a result of recent cyber developments.

Response Message: SR-32-NFPA 1225-2020

Public Comment No. 59-NFPA 1225-2020 [Section No. 22.1.6.1]



Second Revision No. 33-NFPA 1225-2020 [Section No. 22.1.6.2]

22.1.5.2

The plan shall include procedures for personnel to notify the AHJ-appointed security officer within 24 hours of discovery of suspected or actual cyber breaches so that remedial measures can be taken.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:06:29 EST 2020

Committee Statement

Committee Statement: Recent cyber events have shown that rapid intervention is needed to contain damage.

Response Message: SR-33-NFPA 1225-2020

[Public Comment No. 60-NFPA 1225-2020 \[Section No. 22.1.6.2\]](#)



Second Revision No. 34-NFPA 1225-2020 [Section No. 22.1.7]

22.1.6*

The communications center shall implement control provisions for access to physical premises, access to ~~radio subscriber units of subscribers~~ into the radio system, and personnel access to ~~various~~ authorized portions of the communications center networks and computers.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:08:48 EST 2020

Committee Statement

Committee Statement: The revision clarified that we were talking about control provisions for subscribers and access to communications center networks and computers.

Response Message: SR-34-NFPA 1225-2020

[Public Comment No. 61-NFPA 1225-2020 \[Section No. 22.1.7\]](#)



Second Revision No. 35-NFPA 1225-2020 [Section No. 22.1.9.1]

22.1.8.1

The AHJ shall have specific guidelines outlining employee use of AHJ computers, Web access from AHJ computers, and use of thumb drives with AHJ systems.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:17:55 EST 2020

Committee Statement

Committee Statement: The revision clarifies which computers require guidance for employee use.

Response Message: SR-35-NFPA 1225-2020

[Public Comment No. 62-NFPA 1225-2020 \[Section No. 22.1.9.1\]](#)



Second Revision No. 36-NFPA 1225-2020 [Section No. 22.1.9.2]

22.1.8.2

These guidelines shall be ~~both~~ all of the following:

- (1) Explained to all new employees
- (2) Reviewed annually as part of employee refresher training in compliance with 22.1.5
- (3) Explained to any outside third-party contractors who could work upon or use the AHJ computers and networks

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:19:34 EST 2020

Committee Statement

Committee Statement: Training of 3rd parties is added because there have been recent instances of contractor access causing cyber attacks on systems owned by the client using the contractor.

Response Message: SR-36-NFPA 1225-2020

Message:

[Public Comment No. 63-NFPA 1225-2020 \[Section No. 22.1.9.2\]](#)



Second Revision No. 37-NFPA 1225-2020 [Section No. 22.1.9.4 [Excluding any Sub-Sections]]

Communications center networks or computers shall have virus protection software installed and updated in accordance with a frequency determined by the AHJ .

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:21:28 EST 2020

Committee Statement

Committee Statement: The revised text requires the AHJ to consider how often to update software. Outdated software is the source of many cyber attacks.

Response Message: SR-37-NFPA 1225-2020

Public Comment No. 64-NFPA 1225-2020 [Section No. 22.1.9.4 [Excluding any Sub-Sections]]



Second Revision No. 38-NFPA 1225-2020 [Section No. 22.1.9.4.1]

22.1.8.4.1*

The AHJ shall have a procedure to ~~deal with~~ securely receive videos, pictures, text messages, and emails that come into the communications center electronically from the public.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:23:50 EST 2020

Committee Statement

Committee Statement: The revised text clarifies the need to safely accept electronic files.

Response Message: SR-38-NFPA 1225-2020

Public Comment No. 65-NFPA 1225-2020 [Section No. 22.1.9.4.1]



Second Revision No. 39-NFPA 1225-2020 [Section No. 22.1.10]

22.1.9*

The AHJ shall have a software patch management policy that details, at minimum, the frequency of patch updating and the major software to be updated.

A.22.1.9

A common approach to gaining unauthorized access to systems is to leverage a known vulnerability within a software system, which is why it becomes important to ensure that the system is properly maintained throughout its life cycle with up-to-date software versions and patches that close vulnerabilities and bugs. To help prevent existing vulnerabilities from being exploited, it is important to regularly patch an IT infrastructure. Because patch application can sometimes negatively affect the performance of critical communications land mobile radio systems, security patches should be tested in a controlled environment prior to production rollout. Common software attacks can be divided into several ~~flavors~~ categories :

- (1) *Buffer overflows* — an input is returned that is much larger than the variable that holds it and literally overwrites a portion of system memory.
- (2) *SQL injection* — an input is returned that will be used in an embedded structured query language (SQL) statement. The input includes additional SQL such as “OR 1=1” that return more than the intended data.
- (3) *Authentication errors* — applications accept incorrect user authentication or pass authentication credentials in clear text, which can be easily sniffed and reused.
- (4) *Privilege errors* — applications give administrative privileges to regular user logins without requiring additional authentication.
- (5) *Abort errors* — applications encounter processing errors that cause them to abort, but they leave the user logged in with the enhanced service login privileges in which they were running.

It is therefore important to find an enterprise backup solution that has been tested against the information system.

22.1.9.1

The communications center shall implement the AHJ's software patch management policy provisions to ensure that all software is maintained with all updates released and recommended by the system manufacturer to facilitate improved security ~~and in accordance with the AHJ's patch management policy~~ .

22.1.9.2

The radio systems used by the AHJ shall implement the AHJ's software patch management policy provisions to ensure that all software is maintained with all updates released and recommended by the system manufacturer to facilitate improved security.

22.1.9.3

The AHJ shall consider whether firmware updates are necessary.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:29:18 EST 2020

Committee Statement

Committee Statement: This revision clarifies that the frequency of updating needs to be specified. Modern radio systems are firmware and/or software driven and require patches/updates, as well.

Response Message: SR-39-NFPA 1225-2020

Message:

[Public Comment No. 66-NFPA 1225-2020 \[Section No. 22.1.10\]](#)



Second Revision No. 47-NFPA 1225-2020 [Section No. 22.4]

22.4* Cyber Security Measures.

New public safety computer systems or communications networks or upgrades to existing systems or networks shall be designed and implemented using a security-by-design process to incorporate cyber security measures as part of the system.

A.22.4

Security-by-design is a concept in data security wherein software and hardware components and systems have been designed to inherently have security built in from the beginning, as opposed to depending upon security through add-on software, devices, or modifications to the original design.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 19:21:43 EST 2020

Committee Statement

Committee Statement: Annex material is added to provide guidance on the term, security-by-design.

Response Message: SR-47-NFPA 1225-2020

[Public Comment No. 81-NFPA 1225-2020 \[New Section after 3.3.111.2\]](#)



Second Revision No. 46-NFPA 1225-2020 [Section No. A.15.4.3]

A.15.4.3

PSAPs, 9-1-1 authorities, and responder agencies should look at the processing times in a comprehensive manner. Transfers, especially multiple transfers, have the impact of making compliance with the overall processing time standard nearly impossible. Given the life safety implications for critical incidents, PSAPs should make every effort to reduce/eliminate transfers, thereby reducing the amount of time required to answer, process, transfer, and dispatch alarms. Potential strategies to reduce transfers include consolidation, either physical or virtual, CAD to CAD integrations, improved wireless call routing, and improved compliance with call answering standards. See Figure A.15.4.1(a).

Where the communications center is a secondary PSAP, every effort should be made to assess transfer performance consistent with 15.4.2 for all primary PSAPs who routinely transfer calls to the communications center. See Figure A.15.4.1(b).

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 17:06:44 EST 2020

Committee Statement

Committee Statement: Experience has shown that typical law enforcement primary PSAPs that transfer 911 calls to fire and/or EMS secondary PSAPs often fail to monitor their performance. It is incumbent upon fire and/or EMS secondary PSAPs to assess their performance and to advocate for strategies to minimize call transfer times when they exceed targets.

Response Message: SR-46-NFPA 1225-2020

Public Comment No. 24-NFPA 1225-2020 [Section No. A.15.4.3]



Second Revision No. 56-NFPA 1225-2020 [Section No. A.20.3.10]

A.20.3.10

Test Procedures. The test plan should ensure testing throughout the building. Test procedures should be as directed by the AHJ or the frequency license holder(s). The following information is provided to guide the AHJ or the frequency license holder(s) on several types of testing methods that can be used when testing an in-building emergency responder communications enhancement system.

Methods of Determining DAQ. One method of determining DAQ is conducting voice tests according to the standard ITU-T P.863 (POLQA). It can be used on narrowband, wideband, analog, digital, or LTE signals. It is graded qualitatively using a DAQ scale. A second method of determining DAQ for narrowband, analog, or P25 digital systems is quantitatively measuring a minimum signal-to-interference-plus-noise ratio (SINR) value of 18dB and a maximum BER value of 2.5 percent, or to other values provided by the licensee frequency license holder(s) and the AHJ. A third method of determining DAQ is to manually test the system using portable radios as specified by the AHJ. Manually testing the system with portable radios is typically more subjective than utilizing calibrated test equipment. The important factor of any of these test methods is to determine if there is signal strength and quality to provide a DAQ of 3.0 so that the emergency responders can communicate from within the building.

Note: Testing procedures typically are ~~done~~ performed on a grid system. A grid is overlaid onto a floor area to provide 20 grid cells. Grid cells are provided with definite minimum and maximum dimensions. For most buildings, using a minimum grid dimension of 20 ft (6.1 m) and a maximum grid dimension of 80 ft (24.4 m) will suffice to encompass the entire floor area. Where a floor exceeds 128,000 ft² (11,900 m²), which is the floor area that can be covered by the maximum grid dimension of 80 ft (24.4 m), it is recommended that the floor be subdivided into sectors each having an area less than or equal to 128,000 ft² (11,900 m²), and It is also recommended that each sector be tested individually with 20 grid cells in each sector.

Signal strength measurements should be taken at the center of each grid, where required. ~~and should be performed using standardized parameters as specified in the notes of "Measurement Parameters" of this section.~~

The ~~delivered audio quality (DAQ) scale is a universal standard~~ often cited in system designs and specifications, using the following measures:

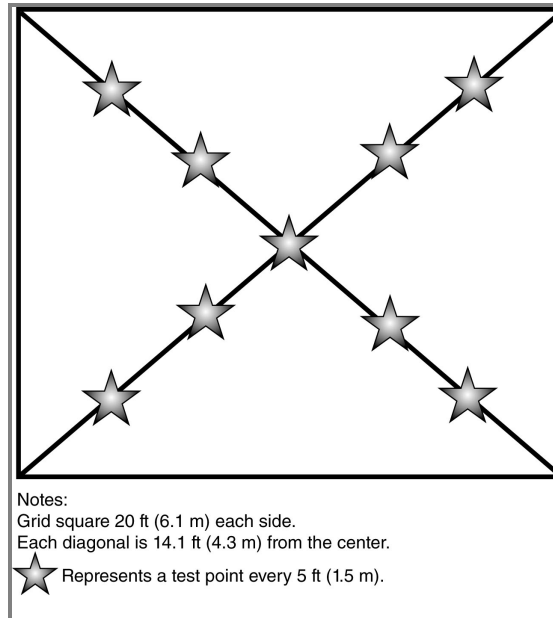
- (1) DAQ 1: Unusable, speech present but unreadable.
- (2) DAQ 2: Understandable with considerable effort. Frequent repetition due to noise/distortion.
- (3) DAQ 3: Speech understandable with slight effort. Occasional repetition required due to noise/distortion.
- (4) ~~DAQ 3.5~~ 4 : Speech understandable with repetition only rarely required. Some noise/distortion.
- (5) DAQ 4: Speech easily understood. Occasional noise/distortion.
- (6) DAQ 4.5: Speech easily understood. Infrequent noise/distortion.
- (7) DAQ 5: Speech easily understood.

The DAQ scale comes from TIA- TSB-88.1-E , *Wireless Communications Systems Performance in Noise and Interference-Limited Situations Part 1: Recommended Methods for Technology-Independent Narrowband Performance Modeling*. A DAQ test is preferred to absolute RF signal levels for two reasons: because the DAQ test is easier to administer than RF signal levels, and DAQ is useful regardless of the type of modulation or system technology used (e.g., analog, or digital, P25, LTE, or broadband). It measures what really matters — how the signal sounds to the user — regardless of manufacturer specifications or intervening transmission technology.

Initially, DAQ testing was somewhat subjective, but now it can be performed objectively, in an automated fashion, with repeatable results. One option is to use the standard test method ITU-T P.863. This international standard has been in use for over 10 years by all the major cellular carriers. ITU-T P.863, called POLQA, is available from three vendors and comprises a suite of hardware and software tools that allow for the rapid, repeatable, objective, and automated testing in two directions of both narrow and wide band radio communications systems.

Testing can be performed for POLQA. First, an "X" is drawn across the grid square and 13 equally spaced locations are identified along the "X." (See [Figure A.20.3.10](#)). Then, the DAQ is measured at all 13 locations for both uplink and downlink communications, and the results from each location are averaged. The average result for uplink and the average result for downlink become the DAQ values for that grid square.

Figure A.20.3.10 POLQA Testing "X."



The minimum allowable DAQ for each grid cell typically is three square is 3.0. Not more than two nonadjacent grid cells squares should be allowed to fail the test. In the event that three of the areas fail the test, or if two adjacent areas fail the test, in order to be more statistically accurate, the testing grid resolution should be doubled. This would require decreasing the size of the grids to one-half the dimension used in the failed test to a minimum of 10 ft (3 m) and a maximum of 40 ft (12.2 m). Further, to cover the same floor area, the number of grids is quadrupled to 80 grids. No more than eight nonadjacent and/or five adjacent grid cells should then be allowed to fail the test.

In the event that nine or more nonadjacent and/or six or more adjacent grid cells fail the test, consideration should be given to redesigning and reinstalling the public safety radio enhancement system to meet the minimum system design requirements. Failures should not be allowed in critical areas. Measurements should be made with the antenna held vertically at 3 ft to 4 ft (0.9 m to 1.2 m) above the floor. The DAQ readings should be recorded on small-scale drawings that are used for testing with the AHJ with an identification of the location on the floor. In addition, the gain values of all RF-emitting devices and system components should be measured and the test measurement results should be kept on file with the building owner and with the AHJ and licensee so that the measurements can be verified each year during annual tests.

SINR and BER Testing. AHJs and frequency license holder(s) can also measure signal strength and bit error rates (BER), but this might only be useful on analog and P25 digital systems. The necessary BER rates for other types of digital systems, such as DMR, could be different. Measuring BER for a LTE system has less meaning because LTE has many tools. These tools include changing data rates, advanced error detection and correction techniques, and multiple antenna techniques (MIMO), that can compensate for a changing channel environment.

Table A.1 of the TSB-88 standard provides several land mobile radio (LMR) technologies and variants that map SINR and BER to expected DAQ values. Determining DAQ for narrowband, analog, or P25 digital systems is conducted by quantitatively measuring a minimum SINR value of 18 dB and a maximum BER value of 2.5 percent or by measuring to other values, as provided by the frequency license holder(s) and the AHJ.

It has been found that, in many narrowband (12.5 kHz) analog systems, a measured signal strength of -95 dBm or greater will provide a DAQ of 3.0.

It has been found that, in many narrowband (12.5 kHz) digital P25 systems, a measured signal strength of -100 dBm or greater will provide a DAQ of 3.0.

The downlink signal can be measured with a calibrated radio, spectrum analyzer, or site monitor.

When uplink measurements are performed, they can be taken at the donor output of the BDA to the donor antenna to estimate the level arriving at the donor radio equipment or at the donor radio site equipment.

Testing procedures for BER and SINR are typically performed on a grid system.

For each floor plan, design a grid, or multiple grids, on the floor plan of each floor. The areas in each grid should be between 1000 ft^2 (93 m^2) and 4000 ft^2 (372 m^2); they should be as close to square as possible. Ideally, no side should be more than 25 percent longer than another side. Each entire floor should be completely covered. The areas across all the floors of the whole building will be approximately the same size (± 10 percent).

One test should be performed in each grid area using the parameters specified in Section 18.9. The test should be long enough and should include enough samples to provide a stable average and to account for variations of the signal, in accordance with the testing device manufacturer's instructions. The received signal strength indicator (RSSI) values should be measured with equipment that specifies 2 dB of accuracy. If SINR is used, it should be with equipment that specifies 2 dB of accuracy. If BER is used, it should include enough samples to have a high confidence (typically over 4 frames). If DAQ is used, the DAQ scale, above, should be used. Each grid area should pass or fail based on the measurements taken and the criteria for each metric.

When conducting the measurements, move around the grid area, to the extent possible, so the final value reflects as much of the area as possible. Ideally, walk an "X" pattern toward the four corners. The measurement device should use a test antenna height of 3 ft (0.9 m) to 4 ft (1.2 m), unless otherwise specified by the AHJ.

One test should be performed for each critical area, using a similar approach as the grid area tests, except for the walking pattern, which should be dependent on the area.

The percent of passing radio coverage on a floor, as required in Section 18.8, should be the percent of passing grid areas. Each floor should be graded independently of other floors and should pass or fail on its own. A floor should also fail if two adjacent grid areas fail. After a failure, floors can be retested using smaller grid areas meeting the minimum size criteria. All floors should pass for a building to pass.

In the event the building fails the test, consideration should be given to redesigning and reinstalling the emergency responder communications enhancement system to meet the minimum system design requirements. Failures should not be permitted in critical areas. All measurement results, including the DAQ readings, should be recorded on small-scale drawings that are used for testing with the AHJ, as well as the grading and the pass/fail status. In addition, the gain values of all RF-emitting devices and system components should be measured. The test measurement results should be kept on file with the building owner so that the measurements can be verified each year during annual tests.

Two Portable Testing. The purpose of this test is to ensure that the near-far performance of the system is such that a portable that is closer to one antenna on one frequency will not prevent another portable farther from its antenna from being able to use some of the energy remaining in the system to communicate.

To test the in-building radio emergency responder communications enhancement system with two portable radios, the following procedure can be used: One portable radio should be positioned no greater than 10 ft (3 m) from an indoor distribution antenna or leaky coaxial cable. The second portable radio should be positioned at a distance that represents the farthest distance possible in that location of the building from an indoor distribution antenna or radiating cable. Both portables should be simultaneously keyed up on different frequencies or talkgroups within the same radio band, and listeners or POLQA test equipment on those the two different frequencies or talkgroups should verify that the voice messages received were intelligible to DAQ 3.0. It is useful when performing these tests to use unfamiliar words, such as from the Harvard Sentences list, when determining reception intelligibility. Testing should be performed on each floor; once per band, if multiple bands are supported; and once per each

powered unit, if multiple units are used. These tests should use two frequencies specified by the AHJ. If the technology uses TDMA, the test should use two time slots on the same frequency.

Measurement Parameters. ~~DAQ levels should be measured to ensure the system meets the criteria of 18.8 according to parameters as directed by the AHJ.~~

Note: ~~Downlink measurements should be made with the following standardized parameters:~~

~~Receive antennas of equal gain to the agency's standard portable radio antenna, oriented vertically, with a centerline between 3 ft to 4 ft (0.9 m to 1.2 m) above floor~~

~~Levels recorded while walking an "X" pattern, with the center of the pattern located approximately in the center of each grid area~~

~~The linear distance of each side of the "X" equal to at least 10 percent of the length of the grid's side and a minimum length of 10 ft (3 m)~~

~~Measurements sampled in averaging mode to include a minimum of one sample per each 5 ft (1.5 m) traveled recorded with not less than five samples per measurement recorded per side of the "X."~~

Antenna Measurements. To ensure that the performance has not changed over time, measuring the downlink power level (RSSI) as close as possible to each antenna is recommended. Then, annual checks can begin with a comparison of these measurements to the initial tests, as an early indicator of system degradation over time. However, all DAQ checks should still be made.

In-building Signal Leakage to Outside. Signal leaking from an in-building ERCES can create potential interference in the public safety communications system, depending on the type of solution that is installed within the building. To ensure that the amplified signals of an in-building ERCES are not leaking outside of the building and causing interference with the outdoor public safety communications network or any other RF system, signal leakage should be measured.

Regardless of what type of solution is used for the ERCES, it is important that outside leakage of an ERCES be verified to be at or below the level determined by the AHJ and the frequency license holder(s). Signal leakage parameters are especially important for an ERCES that is in the always-on position.

For example, if a signal booster has been designed to enhance the communications signal within the building, one approach is to set up a test signal on an unused frequency through the in-building ERCES via keying a portable inside the building on the test frequency. Then, a walk test should be performed around the outside perimeter of the building at ground level, not less than 3 ft (1 m) away from the building walls, to measure the test signal's power level. The test process should verify that the leaked signal at 3 ft (1 m) from the building walls is at least 15 dB below the average signal level from the public safety communications network on one or more channels of the public safety communications network, or not greater than a level determined by the frequency license holder(s).

Where the AHJ requires that the ERCES be left in the off position until activated by first responders, the signal leakage to the outside should still be measured and understood.

In some cases, the AHJ might require a certain amount of signal leakage into the area around the building to enhance the ability of first responder incident commanders on the street to talk to ERUs inside the building. It should be clearly understood that such designs could cause considerable interference to both the public safety and non-public safety communications systems in the vicinity of the location of the ERCES. Therefore, such a design decision should be thoroughly evaluated for unintended consequences.

Acceptance Test. An acceptance test of the two-way in-building wireless communication systems should be scheduled with the AHJ. Acceptance test procedures and requirements should be as directed by the AHJ.

Note: Typically, acceptance tests are required by the AHJ and frequency license holder(s) prior to building occupancy. As-built drawings should be provided including all system design parameters, other information required from the DAQ level and commissioning tests, including a full report with grid locations, DAQ measurements, and RF-emitting device or system

component gain values. The acceptance test typically entails a random test by the AHJ of radio communication in various portions of the building, especially including the critical areas. The AHJ and frequency license holder(s) can review any test documentation and ensure that the findings of the commissioning test with respect to DAQ levels and gain values are supported by the acceptance test.

If RF-emitting devices are used in in-building emergency responder communications enhancement system a spectrum analyzer ~~shall~~ should be used to ensure spurious oscillations are not generated nor are unauthorized ~~carriers~~ signals repeatedly in violation of radio licensing authority regulations. This testing should be conducted at time of installation and during subsequent inspections. Downlink and uplink spectrum should be recorded with a maximum-hold screen capture at the active system air interfaces with the system under normal load and at least one uplink carrier active on the indoor portion of the system. Measurements should be analyzed for correct gains on both uplink and downlink paths, noise floor elevation from active components, intermodulation, and other parameters determined necessary by the AHJ and frequency license holder(s). Gain values of all RF-emitting devices and system components should be measured and the results kept on file with the building owner and the AHJ. In the event that the measurement results are lost, the building owner will need to repeat the acceptance test to re-establish the gain values.

Where the two-way radio communications enhancement system is shared with other non-public safety services, the testing of the public safety system should be made under simulated heavy traffic load conditions of the non-public safety services to ensure that the DAQ values, noise floors, intermodulation, and other parameters, as described by the AHJ and frequency license holder(s) for both ~~in-bound and out-bound~~ uplink and downlink, are met for the public safety portion of the system.

Annual Tests. The AHJ and frequency license holder(s) should be notified in advance and should direct the annual test procedures and requirements.

~~Note:~~ Typically, annual tests require several items to be checked. RF-emitting devices and system components should be tested to ensure that the gain is the same as it was at initial installation and acceptance. Backup batteries and power supplies should be tested under load for 1 hour to verify that they will operate properly during a power outage.

License or Certification of Personnel. All system designs, installation, testing, and maintenance should be conducted, documented, and signed by an ~~acceptable manufacturer or person~~ RF system designer in possession of a current general radio licensing authority license, industry certification, professional electrical engineering license, or operator's license or an equivalent license issued by the frequency licensing authority of the country of jurisdiction and other certifications, as required by the AHJ.

~~Note: Many manufacturers of two-way in-building wireless communications systems provide certification programs for installing contractors. Local adopting jurisdictions could require certification of two-way~~ the installing contractors to have an in-building wireless emergency response communications enhancement system training for the installing contractors certificate issued by a nationally recognized organization or school, ~~or and~~ a certificate issued by the manufacturer of the equipment being installed.

Supplemental Information

<u>File Name</u>	<u>Description</u>	<u>Approved</u>
1225_PUF_SR56_A.20.3.10.docx	staff use	
SR-56_Figure_A-20-3-10-RF.pptx	Figure A.20.3.10 - for staff use	

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Wed Nov 11 18:08:47 EST 2020

Committee Statement

Committee There are several acceptable methods to test in-building emergency responder communications enhancement systems. Additional information has been inserted in the annex to help the AHJ better understand these testing methods. Several terms were modified to align with terminology used within the standard. Additionally, it is critical to ensure the Frequency License Holder is included in the process. Lastly, the issue of signal leakage outside the building continues to be a growing issue, so a section explaining the testing for leakage problems was included.

Response SR-56-NFPA 1225-2020

Message:

[Public Comment No. 120-NFPA 1225-2020 \[Sections A.20.3.10, A.21.5.1\]](#)

[Public Comment No. 124-NFPA 1225-2020 \[Sections A.20.3.10, A.21.5.1\]](#)



Second Revision No. 40-NFPA 1225-2020 [Section No. A.22.1]

A.22.1 

With the increasing numbers of people working from home, and the increase in ransomware attacks, the need for a comprehensive ICT security plan has never been greater.

Security issues for public safety communications systems and communications centers data systems include the following:

- (1) Security of data from outsiders
- (2) Security of data from inappropriate access and use
- (3) Modification of data by those not authorized to do so
- (4) Denial-of-service (DoS) attacks
- (5) Equipment and infrastructure failures that impede or prevent access to data

Many jurisdictions are providing public access to departmental records, some including CAD records, through web browser access. Such unprecedented live access to files presents security issues not previously considered, including but not limited to the following:

- (1) Accidental release of privileged data, such as data protected by the Health Insurance Portability and Accountability Act (HIPAA) of 1996
- (2) Deliberate or inadvertent impacts on the system that affect data availability to any of the users

Data systems give employees access to a wide variety of departmental data that were not easily available before. Agency rules and regulations should be modified to specifically address the misuse of data as a breach of the confidentiality agreement used by the agency. With the move to Internet protocol (IP)–based networks for both the core network for land mobile radio systems as well as IP-based telephony and IP-based Next Generation 9-1-1, it is important that a new holistic approach to data security be taken. “Defense in depth” is an approach in which security is not resolved purely on a technical level but is also addressed across personnel and operations in a holistic risk management methodology. Therefore it is imperative that agencies implement a layered defense that will span the entire enterprise and is not purely technology focused. These defense-in-depth strategies are outlined in Table A.22.1.

Table A.22.1 Defense-in-Depth Strategies

<u>Defense-in-Depth Strategies for</u>		
<u>People</u>	<u>Technology</u>	<u>Operations</u>
Assignment of roles and responsibilities (e.g., administrator, console, and so forth)	Defense in multiple places and layers	Continuity of operations and disaster recovery
Training of critical personnel (e.g., IA training class)	Passive attacks: encryption	Certifying and accrediting changes to the baseline (e.g., configuration management)
Personal accountability (e.g., logging)	Active attacks: firewalls	Managing the security posture (e.g., patch management)
Physical security and personnel security measures to control and monitor access to facilities and critical elements	Layered defenses (e.g., network firewall, host firewall)	Key management
	Role-based access Intrusion detection certified products	Incident response

Critical communication systems have incorporated IP backbones and commercial-off-the-shelf (COTS) technologies. These recent changes from proprietary to open systems have had the following advantages:

- (1) Frequent technology refreshes
- (2) Integration with other IT applications
- (3) Use of standard administrative skills
- (4) Better customer pricing
- (5) Improved product flexibility
- (6) Reuse of existing fiber for backhaul

With these advantages comes the security disadvantage of openness. The protocols are widely documented, and the hardware is inexpensive and widely available. To mitigate the inherent vulnerabilities, steps should be taken in a layered defense-in-depth approach to address the risks to the communications center's systems.

Additional information relating to security issues can be found in Annex F.

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR40_A.22.1.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:40:20 EST 2020

Committee Statement

Committee Statement: The revision clarifies the intent of the section.

Response Message: SR-40-NFPA 1225-2020

Public Comment No. 75-NFPA 1225-2020 [Section No. A.22.1]



Second Revision No. 41-NFPA 1225-2020 [Section No. A.22.1.9]

A.22.1.8 

Computer systems have become not only the primary resource for storing information but also the primary workhorse for users to perform their jobs; therefore they have also become a primary objective for intruders for either data gathering or destruction. This makes a computer system the end point for security, and it requires layers to be built around it to minimize the risks associated with intruders accessing the information contained within the computer or with the trusted capability placed at their disposal.

The rise of home-based workers, and the rise of ransomware attacks, has only exacerbated the risk scenarios for agencies.

Host-Based Security. Host-based security consists of a suite of software or software functionality inside a single software that protects the host computer from malicious behavior. Antivirus software is a recommended minimum application to protect workstations and servers from malicious code, and it is one that most individuals accept even for their home computers. However, it does not provide a complete solution for all the malicious behavior that can result from zero-day viruses, which are not found by antivirus software, intentional attacks through bugs, or even accidental user actions. A comprehensive host solution is necessary for ensuring proper protection from known attack vectors and unallowable behaviors to anomaly detection for incident handling and chain of events.

Firewalls. Firewalls provide protection to the information system by enforcing policies, preventing abnormal network behavior, and integrating high-performance security features, including application-aware firewall, secure socket layer (SSL) and internet protocol security (IPSec), VPN, intrusion prevention system (IPS), antivirus, anti-spam, anti-phishing, and Web-filtering services. These technologies deliver strong network and application-layer security, user-based access control, worm mitigation, malware protection, and improved employee productivity. Adaptive security appliances integrate industry-leading firewalls, unified communications security, VPN technology, intrusion prevention, and content security in a unified platform to carry out the following functions:

- (1) Stop attacks before they penetrate the network perimeter
- (2) Protect resources and data, as well as voice, video, and multimedia traffic
- (3) Control network and application activity
- (4) Reduce deployment and operational costs
- (5) Have an adaptable architecture for rapid and customized security services deployment
- (6) Provide advanced intrusion prevention services that defend against a broad range of threats
- (7) Provide highly secure remote access and unified communications to enhance mobility, collaboration, and productivity

Network Intrusion Detection Systems (NIDS). In today's communications environment, where everything is highly dynamic with new technologies and increased evolving and sophisticated threats, networks need to implement security measures that are just as dynamic and adaptive. By placing network intrusion detection system (NIDS) in line with the network configurations, the system can act as a preventative measure — placing it on the spanning (or sniffer) port of a switch allows it to act as a detection system on all traffic on the switch, even the network traffic that is not being routed outside the local area network. An enterprise NIDS solution can analyze network traffic and prevent threats from damaging a network, including the following:

- (1) Worms
- (2) Trojans
- (3) Backdoor attacks
- (4) Spyware
- (5) Port scans
- (6) VoIP attacks
- (7) Internet protocol version 6 (IPv6) attacks
- (8) DoS attacks

- (9) Buffer overflows
- (10) Statistical anomalies
- (11) Protocol anomalies
- (12) Application anomalies
- (13) Malformed traffic
- (14) Invalid headers
- (15) Blended threats
- (16) Rate-based attacks
- (17) Zero-day threats
- (18) TCP segmentation and IP fragmentation
- (19) Unauthorized use of computational resources

Cloud-Based Services. Agencies large and small are turning to cloud-based repositories for software applications and file storage. The AHJ should ensure that any use of cloud-based services includes an encrypted virtual private network (VPN) connection to the cloud to prevent sensitive data from being read, copied, or changed. Further, the AHJ should ensure that the cloud services provider has adequate backup and restoration capabilities if real-time public safety data will be put into the cloud. Agencies should be aware that in recent years several significant outages of cloud-based services have left users of such services unable to operate properly for hours to days.

Emergency services agencies that include law enforcement should understand that the Department of Justice has specific requirements for information security with respect to criminal records, requiring that the cloud computing service provider be certified by IARC-JAXA Information System (IJIS).

Additional sources of information on cloud computing include the following:

- (1) NIST SP 500-292, *NIST Cloud Computing Security Reference Architecture*, NIST
http://collaborate.nist.gov/wiki/cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013/cloud-computing-reference-architecture
Cloud Computing Reference Architecture, NIST www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
- (2) NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, NIST
SP 800-144. <http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf> csrc.nist.gov/publications/detail/sp/800-144/final
- (3) APCO, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement*,
APCO International. <http://psc.apcointl.org/2013/01/07/mitigating-risks-in-the-application-of-cloud-computing-in-law-enforcement-2>

Supplemental Information

<u>File Name</u>	<u>Description Approved</u>
1225_PUF_SR41_A.22.1.9.docx	staff use

Submitter Information Verification

Committee: PUF-AAA
Submission Date: Tue Nov 10 16:43:20 EST 2020

Committee Statement

Committee Statement: The cybersecurity references are updated. The need for a security plan with workers at home and ransomware risks is also addressed.

Response Message: SR-41-NFPA 1225-2020

[Public Comment No. 112-NFPA 1225-2020 \[Section No. A.22.1.9\]](#)



Second Revision No. 42-NFPA 1225-2020 [Section No. A.22.1.11.2]

A.22.1.10.2



Offsite storage of mission-critical information is highly encouraged. Loss of data can occur from malicious cyber attacks that aim to erase or modify data. Ransomware attacks have become more frequent. When a ransomware attack occurs, all data is encrypted and the agency must pay a ransom, sometimes in the thousands or millions of dollars, to regain the information. In some cases, despite a ransom being paid, the data is not returned. Data loss can occur when in case of catastrophic physical site failure is caused by a storm, flood, fire, earthquake, and so forth etc. Cloud-based storage of such information is off-site, but this adds additional risks that need to be assessed.

Frequency of backing up information will depend on the level of activity of the public safety communications center. Larger agencies should back up critical data weekly, at a minimum. In smaller agencies critical data can be backed up less frequently, such as every two weeks.

~~It might be necessary to store~~ For all agencies, it is recommended that they store at least two time periods of backup information. This should be done in case the computers and networks ~~have infected~~ some of the data before it corruption is discovered, ~~meaning that a as the latest backup can might~~ also contain malware.

~~Storing such information~~ Such backup data should be stored on media that ~~are is~~ not normally connected to the any network, which provides an “air gap;” ~~is recommended.~~

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:45:59 EST 2020

Committee Statement

Committee Statement: The revision clarifies details on the types of ransomware attacks, differentiates how often systems should be backed up by agency size, and addresses the importance of having 2 time periods of backup data.

Response Message: SR-42-NFPA 1225-2020

[Public Comment No. 76-NFPA 1225-2020 \[Section No. A.22.1.11.2\]](#)



Second Revision No. 43-NFPA 1225-2020 [Section No. A.22.1.11.4]

A.22.1.10.4



~~Ransom-ware~~ Ransomware attacks on public safety agencies are becoming more common. In some cases the request is for a ransom payment in exchange for the key to unlock the data. On some occasions, the actor threatens to expose the data publicly if the ransom is not paid.

It is important that AHJs have a ransom plan already in place to deal with the issue before it happens. Additionally, the ICT security plan should address how to resist a ransom incident in the first place, and how to mitigate it, if it should happen.

If the AHJ has a good disaster recovery plan in place with mission-critical data stored off-site and unconnected to any network, then recovery can be ~~quick~~ quicker and threat actors are not rewarded with a ransom.

If these conditions are not in place, then the AHJ will have to decide if paying a ransom is appropriate. Some entities have found services that can unlock their encrypted data so that the entity can get its information back. However, such services ~~don't~~ do not always work. It should be understood that if a ransom is paid, there is no guarantee that the data will in fact be returned, and paying such a ransom will only encourage threat actors to continue and expand the practice.

There is cyber insurance available, but AHJs should understand in detail exactly what said insurance does and does not cover. Some have found that the insurance did not pay because of misunderstanding what was covered. Again, payments to threat actors from cyber insurance only encourages more criminal behavior.

The FBI issued a specific advisory about ransomware attacks:
ic3.gov/media/2019/191002.aspx

In the US, the Treasury Department has stated that, in some cases, entities can be fined for paying ransoms.

Either local or federal law enforcement should be notified of every ransomware incident. In the US, the FBI is the lead federal agency for such notifications. See Annex F for more information. Notifying law enforcement could cause government agencies to reduce or eliminate fines for paying ransoms.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:48:19 EST 2020

Committee Statement

Committee Statement: The revision adds details on ransomware attacks, resources to help, and US Treasury implications if ransom is paid, along with a recommendation to report such attacks to law enforcement.

Response Message: SR-43-NFPA 1225-2020

Message:

Public Comment No. 77-NFPA 1225-2020 [Section No. A.22.1.11.4]



Second Revision No. 44-NFPA 1225-2020 [Section No. A.22.1.13]

A.22.1.12

A key element of ensuring that the system maintains a proper security posture is the periodic auditing of the vulnerabilities inherent in the system to ensure that new vulnerabilities are being addressed and that previously closed vulnerabilities have not resurfaced as a result of changes made to systems during normal business operations. Auditing can be done by individually scanning every asset on the system with a vulnerability management tool, or it can be done automatically by a centralized appliance that is capable of scheduled scans. Both are available from industry leaders in the field. All vulnerability management tools should be used consistently to ensure baseline security compliance.

Vulnerability management processes are used to ensure the survival in various scenarios as appropriate to the jurisdiction, including major storms, floods, earthquakes, wildfires, civil disturbances, security breaches, and ~~civil disturbances~~ ransomware attacks.

Such audits should be conducted at least every 2 to 3 years, depending on the agency size, as determined by the AHJ.

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:53:04 EST 2020

Committee Statement

Committee Statement: The revision adds ransomware attacks as a scenario, because they are becoming more common. It also adds guidance on the frequency of audits.

Response Message: SR-44-NFPA 1225-2020

Public Comment No. 78-NFPA 1225-2020 [Section No. A.22.1.13]



Second Revision No. 45-NFPA 1225-2020 [Chapter F]

Annex F Cyber Security (NFPA 1221)

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

F.1 Where to Start.

It is often difficult for agencies to decide where to start in cyber security. Here are Given the increase in personnel working from home in many agencies, the importance of improved cyber security cannot be overemphasized. Find out where to start in the following three resources:

- (1) ~~Council on Cyber~~ The Center for Internet Security's Critical Security Controls- www.counciloncyber-security.org/critical-controls (www.cisecurity.org/controls/). All agencies should strive to implement the top four controls as soon as possible because they represent the most common security threats and to implement the others as determined necessary by the AHJ. The controls are now in three levels for organizations with small, medium, or large resources.
- (2) Stop.Think.Connect. (www.dhs.gov/stopthinkconnect www.stopthinkconnect.org) is a Department of Homeland Security campaign aimed at educating end users about phishing attacks.
- (3) ~~SANS Securing the Human~~ (www.securingthehuman.org/resources) ~~is another program aimed at educating end users.~~ SANS Institute (www.sans.org/security-awareness-training/products/end-user). Many successful attacks are the result of phishing or similar techniques that lure users onto sites that infect their computers with malware and allow adversaries to steal legitimate user credentials. There are many sources, such as the SANS Institute, for end user training to educate on these issues because every network is often just one click away from a cyber disaster.

F.2 Additional Information.

F.2.1

The federal government's Cybersecurity and Infrastructure Security Agency (CISA) has a document on cyber essentials: <https://www.cisa.gov/cyber-essentials>

F.2.2

The International Association of Chiefs of Police (IACP) (www.theiacp.org/Technology/tabid/72/Default.aspx) has begun a major effort to disseminate information on cyber security and to combat cyberthreats. Go to: www.iacpcybercenter.org. Emergency services agencies with a law enforcement presence should be able to gain access to these resources. :

~~The Law Enforcement Tech Minute video: "The Current Climate in Cyber Security"~~

~~The Law Enforcement Cyber Security Center~~

F.2.3

The International Association of Fire Chiefs (IAFC) has a document "Protecting Against Cyberattacks; A Guide for Public Safety Leaders" that can be found at www.iafc.org/topics-and-tools/resources/resource/protecting-against-cyberattacks.

F.2.4

The National Institute of Standards and Technology (NIST) has been researching and issuing security standards for some time. The NIST Cybersecurity framework is a voluntary outline of best security practices: www.nist.gov/cyberframework

F.2.5

PSAPs are a vital link in the emergency alerting process from the public to ERUs. At the same time PSAPs can be a major target for disruption of emergency services. The move to Next Generation Internet Protocol (IP) based PSAPs brings new challenges and risks. Many resources exist for PSAPs. The following are just a few of these resources:

- (1) This one lists many other resources:
www.911.gov/documents_tools/Cybersecurity.html
- (2) The National Emergency Number Association's (NENA) latest version of their cyber security guidelines are useful for both legacy 9-1-1 centers and Next Generation IP 9-1-1 centers: www.nena.org/page/NG911_Security
- (3) Federal governments Cybersecurity and Infrastructure Security Agency document:
www.cisa.gov/publication/next-generation-911
- (4) The Association of Public Safety Officials (APCO) has many excellent links to cybersecurity resources: www.apcointl.org/cybersecurity/federal-cybersecurity-resources/

F.2.6

The FBI is the lead federal agency on investigating cyber security incidents. A wealth of knowledge exists on their website on preventing, reporting, and dealing with cybersecurity incidents: www.fbi.gov/investigate/cyber

F.2.3

~~The National Institute of Science and Technology (NIST) has been researching and issuing security standards for some time. Here is a partial list, with the most current first:~~

~~Preliminary Cyber Security Framework (www.nist.gov/itl/upload/preliminary-cyber-security-framework.pdf): useful mapping to previous security frameworks such as ISO 270001~~

~~Security and Privacy Controls for Federal Information Systems and Organizations (<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>)~~

~~Minimum Security Requirements for Federal Information and Information Systems (<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>)~~

~~Federal Information Security Management Act of 2002 (FISMA), Title III—Information Security (<http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>)~~

F.2.4

~~The National Emergency Number Association (NENA) has issued guidelines on cyber security that are useful for 9-1-1 centers:~~

~~*Next Generation 9-1-1 Security (NG-SEC) Audit Checklist* (https://c.ycdn.com/sites/www.nena.org/resource/resmgr/Standards/NENA_75-502.1_NG-SEC_Audit_C.pdf)~~

~~*NENA Security for Next Generation 9-1-1 Standard (NG-SEC)* (http://c.ycdn.com/sites/www.nena.org/resource/collection/2851C951-69FF-40F0-A6B8-36A714CB085D/NENA_75-001-v1_NG-Security.pdf)~~

F.2.5

~~The Association of Public Safety Communications Officials (APCO) has issued several guidelines, among them the following:~~

~~*Telephony Denial of Services (TDOS) to Public Safety Communications Phone Service Recommended Best Practices Checklist* (<http://psc.apcointl.org/2013/03/28/telephony-denial-of-services-tdos-to-public-safety-communications-phone-service>)~~

~~*APCO International and the IJIS Institute Outline Information Sharing Priorities* (<http://psc.apcointl.org/2013/08/20/apco-international-and-the-ijis-institute-outline-information-sharing-priorities>)~~

F.2.6

A cyberhealth pyramid can be found at
www.state.nj.us/njinfosecure/home/Posters/2012_Pyramid_Poster.pdf

F.2.7

The FBI's Next Generation Cyber Initiative offers information here:
www.fbi.gov/news/testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland, and a Cyber Shield Alliance offers information here:
www.isc.gov/blog/isc-bloggers/fbis-guardian-portal-expands-cyber-threat-information

Supplemental Information

<u>File Name</u>	<u>Description</u> <u>Approved</u>
1225_PUF_SR45_Annex_F.docx	staff use

Submitter Information Verification

Committee: PUF-AAA

Submittal Date: Tue Nov 10 16:58:29 EST 2020

Committee Statement

Committee Statement: The revision updates the information.

Response Message: SR-45-NFPA 1225-2020

[Public Comment No. 68-NFPA 1225-2020 \[Section No. F.2.1\]](#)

[Public Comment No. 71-NFPA 1225-2020 \[Section No. F.2.4\]](#)

[Public Comment No. 67-NFPA 1225-2020 \[Section No. F.1\]](#)

[Public Comment No. 72-NFPA 1225-2020 \[Section No. F.2.5\]](#)

[Public Comment No. 73-NFPA 1225-2020 \[Section No. F.2.6\]](#)

[Public Comment No. 69-NFPA 1225-2020 \[Section No. F.2.2\]](#)

[Public Comment No. 70-NFPA 1225-2020 \[Section No. F.2.3\]](#)