Public Input No. 24-NFPA 915-2025 [Global Input]

Proposal to include Mental Health Disabilities and / or Health Emergency Considerations in NFPA 915

The NFPA 915 standard on remote inspections is significant in ensuring safety and compliance through innovative means.

I am proposing 2 separate issues:

1. I am proposing to expand the NFPA 915 scope to address the needs of individuals with mental health disabilities.

2. I am proposing to expand the NFPA 915 scope to address the needs for remote inspections during pandemic outbreaks or health emergencies, such as the COVID-19 pandemic.

Substantiation:

1. Mental Health Disabilities:

- **Rationale:** Many individuals with mental health disabilities, such as depression and anxiety, may find traditional in-person inspections challenging. Remote video inspections can provide a less stressful alternative, ensuring compliance without compromising mental well-being.
- **Recommendations:**
    - Include mental health considerations in the planning and execution of remote inspections.
    - Suggest training for inspectors on how to interact sensitively and effectively with individuals experiencing mental health issues.
    - Develop guidelines to accommodate individuals with mental health disabilities during remote inspections.
    - **2. Health Emergency Considerations:**
        - **Rationale:** Pandemic outbreaks or health emergencies, such as the COVID-19 pandemic, have highlighted the need for flexible and safe inspection methods. Remote video inspections can ensure continuity of safety standards while protecting public health.
        - **Recommendations:**
            - Establish protocols for conducting remote inspections during health emergencies.
            - Ensure that remote inspection technology is accessible and user-friendly for all individuals, including those with disabilities.
            - Provide clear communication and support for individuals undergoing remote inspections during health emergencies.
- **Conclusion:** I believe incorporating these considerations into NFPA 915 will enhance the standard's inclusivity and adaptability, ensuring that all individuals, regardless of their mental health status.and the presence of a health emergency, can participate in and

benefit from remote inspections.

I am respectfully asking to make a revision to NFPA 915, the Standard for Remote Inspections, to include provisions that accommodate individuals with mental health disabilities. As it stands, NFPA 915 provides a comprehensive framework for conducting remote virtual inspections, which has proven to be an effective and efficient method for various inspection needs.

However, I do not believe the current standard explicitly addresses the unique challenges faced by individuals with mental health disabilities. These individuals may experience significant anxiety, stress, or other mental health issues that can make in-person inspections particularly difficult. Allowing them to utilize remote virtual inspections would not only provide a more inclusive approach, but also ensure that all individuals have equal access to necessary inspections without compromising their mental well-being.

I propose the following amendments to NFPA 915:

(1) **Inclusion of Mental Health Accommodations**: **Explicitly state that individuals with mental health disabilities are eligible to request remote virtual inspections as a reasonable accommodation.**

(2) **Guidelines for Implementation**: **Develop clear guidelines for how these accommodations can be requested and implemented, ensuring that the process is straightforward and accessible.**

(3) **Training for Inspectors**: **Suggest training for inspectors on how to effectively conduct remote virtual inspections for individuals with mental health disabilities, including sensitivity training and best practices for communication.**

These changes would align NFPA 915 with the principles of inclusivity and accessibility, ensuring that all individuals, regardless of their mental health status, can benefit from the advancements in remote inspection technology.

Thank you for considering this important request. I am confident that these amendments will enhance the standard and provide much-needed support to individuals with mental health disabilities.

If you have any questions about my proposal, I would ask if you would please reach out to me for clarification.

Thank you for considering this proposal to make changes to the NFPA to include both or either of these issues.

Statement of Problem and Substantiation for Public Input

I would like to propose that the NFPA include allowing or mentioning the importance of the NFPA 915 remote inspections for people with Disabilities to include people with Mental Heatlh Disabilities.
I may be mistaken, but I thought I only saw Disabilities referring to people with physical disabilities.
I think it is important to include people with Mental Health Disabilities because many people struggle with mental health issues like depression & anxiety that require the need for remote inspections.
I also would like to propose that the NFPA mention under the NFPA 915 the importance that the remote inspections are during health emergencies, like COVID.

Submitter Information Verification

Submitter Full Name: Cynthia Lopresti

Organization:
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 03 22:51:42 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. No proposed technical changes in code language were provided via the Public Input. Accessibility considerations are addressed and enforced by other codes, laws and regulations. The submitter could review this topic with NFPA DARAC (www.nfpa.org/darac) to determine if further comment on this topic is warranted.

Public Input No. 8-NFPA 915-2024 [Section No. 1.1.1]

1.1.1*

This standard shall provide the minimum requirements for the procedures, methods, transmission, data collection, documentation, and ~~documentation~~ approvals associated with remote inspections and tests, automated inspection and testing, and distance monitoring performed in accordance with other governing laws, codes, and standards.

Statement of Problem and Substantiation for Public Input

Throughout the document it's clear that AHJ approval is required for every aspect of using and enforcing NFPA 915. The task group added this clarification to the scope to reinforce these requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 11-NFPA 915-2024 [Section No. 1.3.1]	
Public Input No. 12-NFPA 915-2024 [Section No. 1.3.2]	

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 11:31:43 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-1-NFPA 915-2025

Statement: The committee agreed with the submitter. The addition of the term "for approvals" provides context of the requirements within the standard on this topic. The PI was modified to include the word "for" to clarify that the AHJ does not have to approve the remote inspection, but that approval is a function of this process.

Public Input No. 10-NFPA 915-2024 [Section No. 1.2]

1.2* Purpose.

The purpose of this standard shall be to provide minimum requirements for performing remote inspections and tests, automated inspection and testing, and distance monitoring to deliver an equivalent or improved result than that which would be obtained with other inspection, testing, and monitoring methods.

Statement of Problem and Substantiation for Public Input

The requirements and allowances for a remote inspection or test, automated inspection and testing, and distance monitoring are included in other NFPA documents. NFPA 915 provides the requirements and allowances to perform them. Adding this term more accurately denotes the intent of the purpose statement.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 11:52:27 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-3-NFPA 915-2025
Statement: The committee agreed with the submitter, as this change provides clarification that these tests and monitoring are performed.

Public Input No. 11-NFPA 915-2024 [Section No. 1.3.1]

1.3.1*

The provisions of the standard shall apply to all types of inspections and tests, automated inspections and testing, and distance monitoring as ~~allowed~~ approved by the authority having jurisdiction.

Statement of Problem and Substantiation for Public Input

Throughout the document it's clear that AHJ approval is required for every aspect of using and enforcing NFPA 915. The task group added this clarification to the application to reinforce these requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 8-NFPA 915-2024 [Section No. 1.1.1]	Clarifies approval from the AHJ is needed.
Public Input No. 12-NFPA 915-2024 [Section No. 1.3.2]	

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 11:55:27 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-4-NFPA 915-2025
Statement: The committee agreed with the submitter. The change from "allowed" to "approved" provides clarity, as this term is defined in Chapter 3.

Public Input No. 25-NFPA 915-2025 [New Section after 1.3.2]

A.1.3.2

The authority having jurisdiction should take into consideration specific situations and/or conditions that exist at the site when determining the feasibility of remote inspections and testing, automated inspection and testing, and distance monitoring. Some examples include the following:

(1) Complex systems. The inspection or test of some complex systems might require more detail than can easily be obtained using a remote inspection or test.

(2) Poor conditions (due to low lighting, low connectivity). Certain conditions can lend themselves to having an inspection or test witnessed remotely or make it difficult to use remote inspection and testing technologies. For instance, an inspection or test required in an area with no or low lighting could use a drone or a robot equipped with its own lighting source. Other conditions could make using certain remote inspection and testing technologies prohibitive, such as in areas with low connectivity where a live inspection or test using an internet connection is not possible.

(3) Access to work. Not being able to access a work area due to height, safety concerns, the inability to shut down a process or a piece of equipment, energized equipment, and so forth, are examples of situations where remote inspections and tests could be performed using a drone, a robot, a fixed transmitting device such as a security camera, a portable transmitting device such as an industrial borescope, and so forth.

(4) Availability/understanding of technology. The authority having jurisdiction should decide if the remote inspection and testing, automated inspection and testing, and distance monitoring technology are understood well enough by both parties to be effective in obtaining the information needed.

(5) Confined/hazardous locations that need to be physically entered. Remote inspections and tests, automated inspections and tests, and distance monitoring could be effective in protecting personnel from confined or hazardous locations. However, the authority having jurisdiction should also ensure that the setup, execution, or completion of a remote inspection or test does not present additional hazards to inspection or test personnel.

(6) Mobility or other physical limitations of the inspector.

(7) Ability of the automated inspection and testing devices and equipment to comply with the applicable NFPA standard.

(8) The need to have live data transmitted to a specific location for distance monitoring of systems or equipment to ensure their readiness in the event of a fire.

(9) Any other conditions that are not conducive for a personal inspection or test such as, but not limited to, the following:

(a)Private property concerns

(b)Legality of methods employed, such as entering controlled airspace or environmentally sensitive areas

(c)Excessive travel time to the site

(d)Cost concerns

(e)Exposure to environmental health and safety concerns

(f) Cybersecurity concerns

Additional Proposed Changes

File Name	Description	Approved
NFPA_915_Section_8.2_Proposal_based_on_72-2025_Chapter_11.docx	word version	

Statement of Problem and Substantiation for Public Input

This public input is submitted on behalf of the NFPA Cybersecurity Advisory Committee (CAC) (www.nfpa.org/cac). The CAC notes that there has been consideration of the significance of cybersecurity protections as it relates to the scope of NFPA 915 and equipment in the scope of the technical committee. Important to the consideration of the suitability for remote testing and inspection, is how the data generated by these activities will be protected to ensure the integrity of the results that are delivered to the AHJs.

Submitter Information Verification

Submitter Full Name: Joshua Griffith
Organization: US Army Corps of Engineers (US
Affiliation: Cybersecurity Advisory Committee
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 06:31:32 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: FR-23-NFPA 915-2025

Statement: The committee agreed with the submitter with modification to move from 9-f to 10. Unlike actions on PI-36, PI-26, and PI-28, including cybersecurity concerns within this annex note is tied to the

application of NFPA 915. As such, adding this annex note was deemed appropriate.

Public Input No. 12-NFPA 915-2024 [Section No. 1.3.2]

1.3.2*

The authority having jurisdiction shall determine applicability of the inspection or test, automated inspection and testing, and distance monitoring categories and conditions that will be ~~allowed~~ approved .

Statement of Problem and Substantiation for Public Input

Throughout the document it's clear that AHJ approval is required for every aspect of using and enforcing NFPA 915. The task group added this clarification to the application to reinforce these requirements.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 8-NFPA 915-2024 [Section No. 1.1.1]	Clarifies that approval by the AHJ is required
Public Input No. 11-NFPA 915-2024 [Section No. 1.3.1]	Clarifies that approval by the AHJ is required

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 11:59:09 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-5-NFPA 915-2025

Statement: The committee agreed with the task group input. Throughout the document AHJ approval is required for every aspect of using and enforcing NFPA 915, and is defined in Chapter 3. The task group added this clarification to the application to reinforce these requirements.

Public Input No. 31-NFPA 915-2025 [Section No. 3.3]

3.3 General Definitions.

3.3.1 Automated Inspection and Testing.

The performance of inspections and tests at a distant location from the system or component being inspected or tested through the use of electronic devices or equipment installed for the purpose.[**13,** 2022]

3.3.2* Building Systems.

An assembly or set of units made up of components that provide services to spaces in a building. [**914,** 2023]

3.3.3* Buildings.

Structures, usually enclosed by walls and a roof, constructed to provide support or shelter for an intended occupancy. [**ASCE/SEI** 7:1.2.1]

3.3.4 Construction.

Work or operations necessary or incidental to land clearing, grading, excavation, and filling; or erection, demolition, assembling, installing, or equipping of buildings or structures; or alterations incidental thereto, or to the finished product of construction operations. [**5000,** 2024]

3.3.5 Construction Documents.

Documents that consist of scaled design drawings and specifications for the purpose of construction of new facilities or modification to existing facilities. [**1,** 2024]

3.3.6 Contractor.

One who contracts on predetermined terms to provide labor and materials and who is responsible for performance of a construction job in accordance with construction documents. [**5000,** 2024]

3.3.7 Contractor of Work.

An individual or company responsible to provide labor and materials and for the performance of an installation in accordance with the construction documents, codes, installation standards, and manufacturer's specifications for the work to be remotely inspected.

3.3.8* Data.

Factual information acquired in digital or nondigital format that can be transmitted, stored, or used as a basis for reasoning, discussion, or calculations.

3.3.9* Data Device.

Any device that collects and stores data and/or transmits data to and from a remote location.

3.3.10 Data-Sensing Device.

Any device which senses input from the physical environment and outputs it as usable data.

3.3.11 Distance Monitoring.

The monitoring of various conditions of a system or component from a distant location from the system or component through the use of electronic devices, meters, or equipment installed for the purpose. [**13,** 2022]

3.3.12 Entity Performing Remote Inspection or Test.

An individual or company responsible for the collection and/or transmitting of the data acquired from the inspection or test.

3.3.13 Equivalency.

An alternative means of providing an equal or greater degree of safety than that afforded by strict conformance to prescribed codes and standards. [**5000,** 2024]

3.3.14* Inspection.

For the purposes of this standard, the examination or witnessing of a product, process, installation, or test to determine conformity with approved documents, including, but not limited to, construction documents and applicable codes, standards, and manufacturer's specifications.

3.3.15 Inspection Area.

That portion of a structure or site where an organized or formal evaluation will take place.

3.3.16 Permit.

A document issued by the AHJ for the purpose of authorizing performance of a specified activity. [**1,** 2024]

3.3.17 Property Owner.

Any person, agent, firm, entity, or corporation having a legal or equitable interest in a property, building, or structure.

3.3.18 Qualified.

A competent and capable person who has demonstrated the skills, knowledge, and/or training for a given field acceptable to the AHJ.

3.3.19* Remote Inspection.

The use of audio/visual devices and/or other technologies to perform an inspection or witness a test for the purpose of remote verification.

3.3.20 Remote Inspection or Test Plan.

A procedure that describes the remote inspection or test and outcomes and describes responsibilities to parties involved in the process.

3.3.21 Test.

A procedure intended to establish the operational status or performance of a system or component. [**3,** 2021]

3.3.22 Unmanned Aircraft.

An aircraft operated without the possibility of direct human intervention from within or on the aircraft. [**14 CFR Part 107,** 2016]

3.3.23 Cybersecurity.

The protection of network-connected equipment and systems from unauthorized access, data theft, hardware or software damage, or other cyber threats that could compromise system confidentiality, functionality and reliability.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. The inclusion of a definition for cybersecurity is critical to standardize its meaning in the context of NFPA 915. Cybersecurity threats pose risks to the confidentiality, functionality, and reliability of network-connected systems used in remote inspections and monitoring. Without explicit recognition, the standard cannot address these risks effectively.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	

Public Input No. 33-NFPA 915-2025 [Section No. 8.2]
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]
Public Input No. 36-NFPA 915-2025 [Chapter 4]
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]
Public Input No. 36-NFPA 915-2025 [Chapter 4]
Public Input No. 37-NFPA 915-2025 [Chapter A]

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 19:47:09 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: See FR-16.

Public Input No. 32-NFPA 915-2025 [Section No. 3.3]

3.3 General Definitions.

3.3.1 Automated Inspection and Testing.

The performance of inspections and tests at a distant location from the system or component being inspected or tested through the use of electronic devices or equipment installed for the purpose.[**13,** 2022]

3.3.2* Building Systems.

An assembly or set of units made up of components that provide services to spaces in a building. [**914,** 2023]

3.3.3* Buildings.

Structures, usually enclosed by walls and a roof, constructed to provide support or shelter for an intended occupancy. [**ASCE/SEI** 7:1.2.1]

3.3.4 Construction.

Work or operations necessary or incidental to land clearing, grading, excavation, and filling; or erection, demolition, assembling, installing, or equipping of buildings or structures; or alterations incidental thereto, or to the finished product of construction operations. [**5000,** 2024]

3.3.5 Construction Documents.

Documents that consist of scaled design drawings and specifications for the purpose of construction of new facilities or modification to existing facilities. [**1,** 2024]

3.3.6 Contractor.

One who contracts on predetermined terms to provide labor and materials and who is responsible for performance of a construction job in accordance with construction documents. [**5000,** 2024]

3.3.7 Contractor of Work.

An individual or company responsible to provide labor and materials and for the performance of an installation in accordance with the construction documents, codes, installation standards, and manufacturer's specifications for the work to be remotely inspected.

3.3.8* Data.

Factual information acquired in digital or nondigital format that can be transmitted, stored, or used as a basis for reasoning, discussion, or calculations.

3.3.9* Data Device.

Any device that collects and stores data and/or transmits data to and from a remote location.

3.3.10 Data-Sensing Device.

Any device which senses input from the physical environment and outputs it as usable data.

3.3.11 Distance Monitoring.

The monitoring of various conditions of a system or component from a distant location from the system or component through the use of electronic devices, meters, or equipment installed for the purpose. [**13,** 2022]

3.3.12 Entity Performing Remote Inspection or Test.

An individual or company responsible for the collection and/or transmitting of the data acquired from the inspection or test.

3.3.13 Equivalency.

An alternative means of providing an equal or greater degree of safety than that afforded by strict conformance to prescribed codes and standards. [**5000,** 2024]

3.3.14* Inspection.

For the purposes of this standard, the examination or witnessing of a product, process, installation, or test to determine conformity with approved documents, including, but not limited to, construction documents and applicable codes, standards, and manufacturer's specifications.

3.3.15 Inspection Area.

That portion of a structure or site where an organized or formal evaluation will take place.

3.3.16 Permit.

A document issued by the AHJ for the purpose of authorizing performance of a specified activity. [**1,** 2024]

3.3.17 Property Owner.

Any person, agent, firm, entity, or corporation having a legal or equitable interest in a property, building, or structure.

3.3.18 Qualified.

A competent and capable person who has demonstrated the skills, knowledge, and/or training for a given field acceptable to the AHJ.

3.3.19* Remote Inspection.

The use of audio/visual devices and/or other technologies to perform an inspection or witness a test for the purpose of remote verification.

3.3.20 Remote Inspection or Test Plan.

A procedure that describes the remote inspection or test and outcomes and describes responsibilities to parties involved in the process.

3.3.21 Test.

A procedure intended to establish the operational status or performance of a system or component. [**3,** 2021]

3.3.22 Unmanned Aircraft.

An aircraft operated without the possibility of direct human intervention from within or on the aircraft. [**14 CFR Part 107,** 2016]

3.3.24 Cybersecurity Risk Assessment.

A structured evaluation to identify cybersecurity vulnerabilities and risks in network-connected systems, aligned with frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, or ISA/IEC 62443.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. A structured evaluation ensures systematic identification and mitigation of vulnerabilities. Using recognized frameworks (NIST, ISO/IEC 27001, ISA/IEC 62443) provides proven methodologies for enhancing resilience, addressing both regulatory requirements and practical security measures.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	

Public Input No. 33-NFPA 915-2025 [Section No. 8.2]
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]
Public Input No. 36-NFPA 915-2025 [Chapter 4]
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]
Public Input No. 36-NFPA 915-2025 [Chapter 4]
Public Input No. 37-NFPA 915-2025 [Chapter A]

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 11:46:22 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee resolved these PI's at the request of the task group. The definition created for cybersecurity removes the need to include these additional terms. The committee welcomes Public Comment on this topic.

Public Input No. 34-NFPA 915-2025 [Section No. 3.3]

3.3 General Definitions.

3.3.1 Automated Inspection and Testing.

The performance of inspections and tests at a distant location from the system or component being inspected or tested through the use of electronic devices or equipment installed for the purpose.[**13,** 2022]

3.3.2* Building Systems.

An assembly or set of units made up of components that provide services to spaces in a building. [**914,** 2023]

3.3.3* Buildings.

Structures, usually enclosed by walls and a roof, constructed to provide support or shelter for an intended occupancy. [**ASCE/SEI** 7:1.2.1]

3.3.4 Construction.

Work or operations necessary or incidental to land clearing, grading, excavation, and filling; or erection, demolition, assembling, installing, or equipping of buildings or structures; or alterations incidental thereto, or to the finished product of construction operations. [**5000,** 2024]

3.3.5 Construction Documents.

Documents that consist of scaled design drawings and specifications for the purpose of construction of new facilities or modification to existing facilities. [**1,** 2024]

3.3.6 Contractor.

One who contracts on predetermined terms to provide labor and materials and who is responsible for performance of a construction job in accordance with construction documents. [**5000,** 2024]

3.3.7 Contractor of Work.

An individual or company responsible to provide labor and materials and for the performance of an installation in accordance with the construction documents, codes, installation standards, and manufacturer's specifications for the work to be remotely inspected.

3.3.8* Data.

Factual information acquired in digital or nondigital format that can be transmitted, stored, or used as a basis for reasoning, discussion, or calculations.

3.3.9* Data Device.

Any device that collects and stores data and/or transmits data to and from a remote location.

3.3.10 Data-Sensing Device.

Any device which senses input from the physical environment and outputs it as usable data.

3.3.11 Distance Monitoring.

The monitoring of various conditions of a system or component from a distant location from the system or component through the use of electronic devices, meters, or equipment installed for the purpose. [**13,** 2022]

3.3.12 Entity Performing Remote Inspection or Test.

An individual or company responsible for the collection and/or transmitting of the data acquired from the inspection or test.

3.3.13 Equivalency.

An alternative means of providing an equal or greater degree of safety than that afforded by strict conformance to prescribed codes and standards. [**5000,** 2024]

3.3.14* Inspection.

For the purposes of this standard, the examination or witnessing of a product, process, installation, or test to determine conformity with approved documents, including, but not limited to, construction documents and applicable codes, standards, and manufacturer's specifications.

3.3.15 Inspection Area.

That portion of a structure or site where an organized or formal evaluation will take place.

3.3.16 Permit.

A document issued by the AHJ for the purpose of authorizing performance of a specified activity. [**1,** 2024]

3.3.17 Property Owner.

Any person, agent, firm, entity, or corporation having a legal or equitable interest in a property, building, or structure.

3.3.18 Qualified.

A competent and capable person who has demonstrated the skills, knowledge, and/or training for a given field acceptable to the AHJ.

3.3.19* Remote Inspection.

The use of audio/visual devices and/or other technologies to perform an inspection or witness a test for the purpose of remote verification.

3.3.20 Remote Inspection or Test Plan.

A procedure that describes the remote inspection or test and outcomes and describes responsibilities to parties involved in the process.

3.3.21 Test.

A procedure intended to establish the operational status or performance of a system or component. [**3,** 2021]

3.3.22 Unmanned Aircraft.

An aircraft operated without the possibility of direct human intervention from within or on the aircraft. [**14 CFR Part 107,** 2016]

3.3.25 Network Connected Equipment.

System components, utilized exclusively for remote inspections, automated inspections, distance monitoring and tests, that connect to the internet or external systems through wired or wireless pathways using various protocols.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. Network-connected equipment refers to individual components that operate as part of remote inspection, automated testing, or distance monitoring systems. These components, such as sensors, cameras, or communication devices, connect to external systems or the internet. Defining this term ensures clear delineation of responsibilities for ensuring the cybersecurity of each piece of equipment. This is essential because vulnerabilities at the equipment level, such as unsecured firmware or unprotected communication ports, can serve as entry points for cyber threats, compromising the entire system's functionality and integrity.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 37-NFPA 915-2025 [Chapter A]	

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 12:02:57 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee resolved these PI's at the request of the task group. The definition created for cybersecurity removes the need to include these additional terms. The committee welcomes Public Comment on this topic.

Public Input No. 35-NFPA 915-2025 [Section No. 3.3]

3.3 General Definitions.

3.3.1 Automated Inspection and Testing.

The performance of inspections and tests at a distant location from the system or component being inspected or tested through the use of electronic devices or equipment installed for the purpose.[**13,** 2022]

3.3.2* Building Systems.

An assembly or set of units made up of components that provide services to spaces in a building. [**914,** 2023]

3.3.3* Buildings.

Structures, usually enclosed by walls and a roof, constructed to provide support or shelter for an intended occupancy. [**ASCE/SEI** 7:1.2.1]

3.3.4 Construction.

Work or operations necessary or incidental to land clearing, grading, excavation, and filling; or erection, demolition, assembling, installing, or equipping of buildings or structures; or alterations incidental thereto, or to the finished product of construction operations. [**5000,** 2024]

3.3.5 Construction Documents.

Documents that consist of scaled design drawings and specifications for the purpose of construction of new facilities or modification to existing facilities. [**1,** 2024]

3.3.6 Contractor.

One who contracts on predetermined terms to provide labor and materials and who is responsible for performance of a construction job in accordance with construction documents. [**5000,** 2024]

3.3.7 Contractor of Work.

An individual or company responsible to provide labor and materials and for the performance of an installation in accordance with the construction documents, codes, installation standards, and manufacturer's specifications for the work to be remotely inspected.

3.3.8* Data.

Factual information acquired in digital or nondigital format that can be transmitted, stored, or used as a basis for reasoning, discussion, or calculations.

3.3.9* Data Device.

Any device that collects and stores data and/or transmits data to and from a remote location.

3.3.10 Data-Sensing Device.

Any device which senses input from the physical environment and outputs it as usable data.

3.3.11 Distance Monitoring.

The monitoring of various conditions of a system or component from a distant location from the system or component through the use of electronic devices, meters, or equipment installed for the purpose. [**13,** 2022]

3.3.12 Entity Performing Remote Inspection or Test.

An individual or company responsible for the collection and/or transmitting of the data acquired from the inspection or test.

3.3.13 Equivalency.

An alternative means of providing an equal or greater degree of safety than that afforded by strict conformance to prescribed codes and standards. [**5000,** 2024]

3.3.14* Inspection.

For the purposes of this standard, the examination or witnessing of a product, process, installation, or test to determine conformity with approved documents, including, but not limited to, construction documents and applicable codes, standards, and manufacturer's specifications.

3.3.15 Inspection Area.

That portion of a structure or site where an organized or formal evaluation will take place.

3.3.16 Permit.

A document issued by the AHJ for the purpose of authorizing performance of a specified activity. [**1,** 2024]

3.3.17 Property Owner.

Any person, agent, firm, entity, or corporation having a legal or equitable interest in a property, building, or structure.

3.3.18 Qualified.

A competent and capable person who has demonstrated the skills, knowledge, and/or training for a given field acceptable to the AHJ.

3.3.19* Remote Inspection.

The use of audio/visual devices and/or other technologies to perform an inspection or witness a test for the purpose of remote verification.

3.3.20 Remote Inspection or Test Plan.

A procedure that describes the remote inspection or test and outcomes and describes responsibilities to parties involved in the process.

3.3.21 Test.

A procedure intended to establish the operational status or performance of a system or component. [**3,** 2021]

3.3.22 Unmanned Aircraft.

An aircraft operated without the possibility of direct human intervention from within or on the aircraft. [**14 CFR Part 107,** 2016]

3.3.26 **Network Connected Systems.**

A group of devices used while performing remote inspections, automated inspections, distance monitoring and tests that are linked together through a network, allowing them to communicate and exchange data.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. Network-connected systems represent a collection of interconnected devices functioning together to perform remote inspections and monitoring. Defining this term highlights the importance of addressing not only individual equipment vulnerabilities but also systemic risks such as insecure data exchange, unmonitored connectivity points, or weak inter-device protocols. Systems-level cybersecurity measures ensure the seamless and secure operation of interconnected devices, reducing the risk of cascading failures that could disrupt inspections or compromise safety.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 37-NFPA 915-2025 [Chapter A]	

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 12:06:36 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee resolved these PI's at the request of the task group. The definition created for cybersecurity removes the need to include these additional terms. The committee welcomes Public Comment on this topic.

Public Input No. 29-NFPA 915-2025 [New Section after 3.3.2]

3.3.2* Automated Test

A self-acting test, performed with little or no direct human control, by a device designed for the purpose.

A.3.3.2 Automated Test.

An automated test is sometimes initiated by human action, such as the pressing of a button or turning a key, but the process of performing the test itself is, by definition, automated and requires little or no human action. However, in some cases, even the initiation can happen automatically via an electronic signal generated by a control panel or similar piece of equipment.

Statement of Problem and Substantiation for Public Input

The term "automated test" is different that the phrase "automated inspection and testing" and can be different from that of a traditional test, and therefore needs to be defined separately. An automated test does not necessarily have to be conducted "at a distant location" as defined in the phrase "automated inspection and testing". Additionally, an automated test may not be able to be witnessed as the test my happen instantaneously inside a device, be validated via an algorithm or similar method, or involve tasks not able to be visualized. In many cases, what is being witnessed is the results of an automated test, not the test itself. The standard to clarify these differences and this definition is a good first step.

Submitter Information Verification

Submitter Full Name: Jason Webb
Organization: Jason Webb & Associates
Affiliation: Potter Electric Signal
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 10:30:36 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. Currently, this term is not used within the document in the language as presented in the Public Input. There are several variations of this term currently within the document, which the committee determined would create confusion if this new definition was inserted.

Public Input No. 13-NFPA 915-2024 [Section No. 3.3.12]

3.3.12 Entity Performing Remote ~~Inspection~~ Inspections or ~~Test~~ Tests .

An individual or company responsible for the collection and/or transmitting of the data acquired from the ~~inspection~~ inspections or ~~test~~ tests .

Statement of Problem and Substantiation for Public Input

Making these two terms plural correlates with the title of section 4.3.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 14:25:36 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-6-NFPA 915-2025
Statement: The committed agreed to this change to correlate the definition with the title of section 4.3.

Public Input No. 14-NFPA 915-2024 [Section No. 3.3.14]

3.3.14* Inspection.

For the purposes of this standard, the examination or witnessing of a product, process, installation, or test to determine conformity with approved documents, including, but not limited to, construction documents and applicable codes, standards, and manufacturer's published specifications.

Statement of Problem and Substantiation for Public Input

Adding this term clarifies that the specifications must be published so they can be found for compliance with the standard.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 14:29:58 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-7-NFPA 915-2025
Statement: The committee agreed with the submitter with modification. The addition of the word "published instructions" provides clarity on industry-specific usage of this term, which is more commonly used and understood.

Public Input No. 5-NFPA 915-2024 [Section No. 3.3.18]

3.3.18 Qualified.

A competent and capable person who has ~~demonstrated~~ acquired the skills, knowledge, ~~and/or training~~ and training for a given field acceptable to the AHJ.

Statement of Problem and Substantiation for Public Input

The word demonstrated in the original version refers to someone who has to perform an action to validate the skill. No direction is provided on who observes this demonstration. By definition, “acquired” best acknowledges recognition of a skill. A recommendation to remove the word “or”. Leaving it as written with the word “or” in the sentence, the “and” is negated.

Submitter Information Verification

Submitter Full Name:	Kenneth Schneider
Organization:	UA - ITF
Affiliation:	United Assn. of Journeymen & Apprentices of the Plumbing & Pipe Fitting Industry
Street Address:	
City:	
State:	
Zip:	
Submittal Date:	Wed Jun 05 09:43:02 EDT 2024
Committee:	REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. The current definition changing "demonstrated" to "acquired" does not provide clarity to this definition within NFPA 915. The committee welcomes Public Comment on this topic for review during the Second Draft meeting.

Public Input No. 36-NFPA 915-2025 [Chapter 4]

Chapter 4 General Requirements

4.1 Responsibility of the Property Owner or Designated Representative.

It shall be acceptable for the owner to delegate the responsibility for remote inspection or test activities to a designated representative.

4.1.1 Access.

The property owner or designated representative shall provide access to appropriate locations as necessary for remote inspection or test.

4.1.2*

The property owner or designated representative shall also provide appropriate safeguards to prevent the unauthorized recording of video, images, or audio of sensitive or classified subject(s).

4.1.3* Notification.

4.1.3.1

The property owner or designated representative shall notify all applicable parties regarding the remote inspection or test.

4.1.3.2

The property owner or designated representative shall be responsible to obtain any required permissions from all applicable parties regarding the remote inspection or test.

4.1.4

The owner or designated representative shall comply with AHJ requirements for remote inspections and tests as applicable.

4.2 Responsibility of the Contractor of Work.

4.2.1 Permission from the Property Owner.

The contractor of work shall obtain permission from the property owner or designated representative to plan and perform a remote inspection or test.

4.2.2

The contractor of work shall be responsible for providing a qualified entity to perform the remote inspections and tests.

4.2.3

The contractor of work shall comply with AHJ requirements for remote inspections and tests as applicable.

4.3* Responsibility of the Entity Performing Remote Inspections and Tests.

4.3.1* Permission from the Property Owner.

The entity performing the remote inspection or test shall have permission from the property owner or designated representative to access the property and conduct a remote inspection or test.

4.3.2

The entity performing remote inspections and tests shall comply with AHJ requirements for remote inspections and tests as indicated in 4.4.1.

4.3.2.1

It shall be the responsibility of the entity performing remote inspections and tests to ensure the accuracy, quality, verification, authentication, and usability of data or information collected.

4.3.2.2

The entity performing remote inspections and tests shall be qualified.

4.3.2.3*

A written inspection or test plan shall be submitted to and approved by the AHJ unless exempt by the AHJ.

4.3.2.3.1

The inspection or test plan shall be submitted in a manner acceptable to the AHJ.

4.3.2.3.2*

The inspection or test plan shall include pertinent administrative information necessary for the AHJ to approve the use of the remote inspection or test process.

4.3.2.3.3*

The inspection or test plan shall include the procedure in which the remote inspection or test will be performed.

4.3.3 Identification of Participants.

4.3.3.1

It shall be the responsibility of the entity performing remote inspections and tests to identify all personnel participating in the remote inspection or test by providing all of the following:

(1) Name of each individual

(2) Company, organization, or affiliation for each individual

(3) Role each individual is performing as part of the work being done or remote inspection or test being performed

4.3.3.2

The identification of participants shall be documented within the remote inspection or test video and/or audio format transmitted to the AHJ.

4.4 Responsibility of the AHJ.

4.4.1*

The AHJ shall be responsible for providing the following criteria related to remote inspections or tests:

(1) Suitability of performing the inspection or test remotely

(2) Limitations

(3) Documentation

(4) Technology

(5) Submission format

(6) Scheduling requirements

(7) Modifications

(8) Record retention

4.4.2 Remote Inspection or Test Results.

The AHJ shall approve the results of the remote inspection or test.

4.4.3

Where other governing laws, codes, or standards establish success or failure criteria, they shall be the basis for the criteria described in 4.4.2.

4.4.4

The AHJ shall determine the appropriate time frame to provide remote inspection or test results to the responsible party.

4.5 Safety.

Remote inspection or test activities shall be conducted in accordance with applicable safety regulations.

4.6 Permits or Approvals.

Where required, the property owner or designated representative shall have in place appropriate permits or approvals for the work to be remotely inspected.

4.7 Supporting Documents.

4.7.1

All plans, specifications, drawings, details, and records shall be made available for the remote inspection or test as required.

4.7.2

Documents shall be made available in either hard copy or digital format at the discretion of the AHJ.

4.8 Cybersecurity Compliance

All network-connected systems and equipment used for remote inspections, automated inspections, distance monitoring and tests shall comply with the cybersecurity provisions outlined in Section 8.2.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. Mandating compliance ensures that systems used in remote inspections are secure, reducing risks of unauthorized access, operational disruptions, and data breaches. Cybersecurity failures in these systems can compromise inspection integrity and safety.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 37-NFPA 915-2025 [Chapter A]	

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 12:09:27 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee determined that cybersecurity requirements should be consolidated in one location. Given this, these inputs have been resolved.

Public Input No. 30-NFPA 915-2025 [Section No. 4.4]

4.4 Responsibility of the AHJ.

4.4.1*

The AHJ shall be responsible for providing the following criteria related to remote inspections or tests:

(1) Suitability of performing the inspection or test remotely

(2) Limitations

(3) Documentation

(4) Technology

(5) Submission format

(6) Scheduling requirements

(7) Modifications

(8) Record retention

4.4.2 Remote Inspection or Test Results.

~~The AHJ shall approve the results of the remote inspection or test.~~

~~4.4.3~~ –

Where other governing laws, codes, or standards establish success or failure criteria of the inspection or test being conducted remotely , they shall be the basis for ~~the criteria described in 4.4.2 .~~ approval by the AHJ.

4.4.4 3

The AHJ shall determine the appropriate time frame to provide remote inspection or test results to the responsible party.

Statement of Problem and Substantiation for Public Input

4.4.2 is worded in a way that could be interpreted as requiring the AHJ to approve results regardless of whether or not they are satisfactory. It can just be deleted in its entirety as 4.4.1 already requires that the AHJ must establish what inspections and tests they will allow to be performed remotely. The following section (4.4.3 in the '24 edition) is an important pointer to codes and standards that already establish pass/fail criteria, but needed to be reworded with the deletion of 4.4.2.

Submitter Information Verification

Submitter Full Name: Jason Webb
Organization: Jason Webb & Associates
Affiliation: Potter Electric Signal
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 12:37:21 EST 2025

Committee: REI-AAA

Committee Statement

Resolution: FR-10-NFPA 915-2025

Statement: The committee agreed with the submitter, as the removal of 4.4.2 provides clarity that the AHJ is not required to provide approval. The change in the existing 4.4.3 (now 4.4.2) relocates the basis for the approval by the AHJ to be applied where relevant codes, standards or regulations provide the relevant pass/fail criteria.

Public Input No. 26-NFPA 915-2025 [New Section after 4.4.1]

A4.4.1

The following criteria examples are to assist the AHJ in determining the acceptable remote inspection or test criteria for their jurisdiction:

(1) Suitability of the inspection or test, which could include the expected success of the inspection or test; the available site and task safety available, or lack thereof; and size/scope of the work to be inspected

(2) Limitations, which could include weather, trained personnel, privacy constraints, cellular/ WIFI connections, and any constraints that will affect safety, health, and the environment

(3) Acceptance criteria, which could include upper and lower limits of data results in accordance with codes, standards, or best practices

(4) Inspection or test requirements, which could include supervision, inspector qualifications, insurance, contracts, and other risk management requirements

(5) Documentation, which could include the allowance or disallowance of electronic reports, photography, and video

(6) Technology, including the allowable standard for remote testing equipment and systems

(7) Submission format, including electronic data, cloud storage, handwritten reports, and paper reporting

(8) Scheduling requirements, including times, dates, and weather conditions

(9) Dissemination of modifications and current practices to the AHJ required criteria

(10) Acceptance criteria for cybersecurity protection for testing and inspection data including data storage, data transmission, data integrity, and data access.

Additional Proposed Changes

File Name	Description	Approved
.1736163473454		

Statement of Problem and Substantiation for Public Input

This public input is submitted on behalf of the NFPA Cybersecurity Advisory Committee (CAC) (www.nfpa.org/cac). The NFPA CAC notes that there has been consideration of the significance of cybersecurity protections as it relates to the scope of NFPA 915 and equipment in the scope of the technical committee. Important to the consideration of the suitability for remote testing and inspection, is how the data generated by these activities will be protected to ensure the integrity of the results that are delivered to the AHJs.

Submitter Information Verification

Submitter Full Name: Joshua Griffith
Organization: US Army Corps of Engineers (US
Affiliation: Cybersecurity Advisory Committee

Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 06:36:02 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee determined that cybersecurity requirements should be consolidated in one location. Given this, these inputs have been resolved.

Public Input No. 23-NFPA 915-2025 [New Section after 4.7.2]

TITLE OF NEW CONTENT

4.8 Artificial Intelligence (AI)

4.8.1 Artificial Intelligence (AI) shall be permitted to aid in the identification of detectable anomalies during the evaluation of Remote Inspection and Testing.

4.8.1.1 All identified anomalies or off-normal results shall be reviewed by an authorized individual.

4.8.2 Final Verification of AI generated results is required to be verified by an authorized individual.

Statement of Problem and Substantiation for Public Input

The AI TG (TG !) determined that conditions and limitations should be considered in the current scope of NFPA 915.
The submitted text is an attempt to start to put "guardrails" on the use of AI technology in the Standard.
Annex Language should also be added regarding the following topics:
1. fire sprinkler water supply results
2. photo/video/data evaluation
3. QA/QC of reports
4. verification of previous reported anomalies being tracked or repaired
5. building code review
6. installation review

Submitter Information Verification

Submitter Full Name: Wayne Moore
Organization: NFPA 915 TG 1 Chairman
Affiliation: NFPA 915 Task Group
Street Address:
City:
State:
Zip:
Submittal Date: Fri Jan 03 10:25:51 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: FR-11-NFPA 915-2025

Statement: The committee agreed with the submitter with modification. Currently, no known AI requirements are provided within NFPA codes and standards. The inclusion of the provided requirements pertaining to artificial intelligence (AI), where approved by the AHJ, allow this technology to be considered for use within NFPA 915. This technology is becoming more prevalent in all areas of digital life, including fire protection. These requirements, as provided, create a framework for the use of this evolving technology within the document. As this technology is currently in a state of constant change, Public Comment is welcome on this topic to consider relevant updates during the Second Draft meeting. these requirements provide a basic framework for consideration and utilization

of this tool, where appropriate.

Public Input No. 2-NFPA 915-2024 [Section No. 5.2.2]

5.2.2* Structure.

The type of structure**, in accordance with NFPA 220 or a building code,** shall be verified and/or documented at the time of the remote inspection or test.

Statement of Problem and Substantiation for Public Input

The Annex Section A.5.2.2 Because the type of structure could vary, please see NFPA 220 for applicable building types, currently points the user to check NFPA 220. We would like to make things consistent and having NFPA 220 added into the section as opposed to it being in the annex. This addition would be beneficial to the user and to the AHJ knowing to look in NFPA 220 or a building code for structure type directly in the main section.

Submitter Information Verification

Submitter Full Name: Joseph Duval Jr
Organization: Connecticut Office of State Fire Marshal
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jun 04 08:19:40 EDT 2024
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. As NFPA 915 addresses the remote inspection process, and not the building construction types, the inclusion of NFPA 220 in the prescriptive language is not warranted. The annex note for A.5.2.2 is provided for reference for guidance only.

Public Input No. 3-NFPA 915-2024 [Section No. 5.3]

5.3* Occupancy Type.

Where required **in accordance with a life safety or building code** , the type of occupancy shall be verified and documented at the time of the remote inspection or test.

Statement of Problem and Substantiation for Public Input

The Annex Section A.5.3 the type of occupancy could be a one- or two-family dwelling, an apartment, or a health care facility, among others. See NFPA 101, NFPA 5000, or applicable life safety or building codes for occupancy types, currently points the user to check applicable life safety or building code for occupancy. We would like to make things consistent and having life safety or building code added into the section as opposed to it being in the annex. This addition would be beneficial to the user and to the AHJ knowing to look in life safety or building code for occupancy type directly in main section.

Submitter Information Verification

Submitter Full Name: Joseph Duval Jr
Organization: Connecticut Office of State Fire Marshal
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jun 04 08:24:31 EDT 2024
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. As NFPA 915 addresses the remote inspection process, and not the life safety or building code requirements, the reference to these classification of documents within the prescriptive language is not warranted. The annex note for A.5.3 provides reference to relevant NFPA documents for guidance only.

Public Input No. 4-NFPA 915-2024 [Section No. 5.5]

5.5 Timestamp Requirements.

5.5.1* Inspection or Test Date.

The date that the remote inspection or test is performed shall be verified**, timestamped,** _ and documented by the owner, or their designee, and provided to the AHJ.

5.5.2* Inspection or Test Local Time.

The time of day that the remote inspection or test is performed shall be verified**, timestamped,** and documented by the owner, or their designee, and provided to the AHJ.

Statement of Problem and Substantiation for Public Input

The word timestamped should be added to these sections. Merriam Webster dictionary defines timestamp as b: an indication of the date and time recorded as part of a digital signal or file (such as an email, digital photograph, radio broadcast, or text message) indicating the time of creation, transmission, etc. The addition of this word will allow the inspection to be timestamped with the date and time to prove when the inspection took place. This would be beneficial to the AHJ during the inspection and after the inspection for record keeping.

Submitter Information Verification

Submitter Full Name: Joseph Duval Jr
Organization: Connecticut Office of State Fire Marshal
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jun 04 08:29:22 EDT 2024
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter, as adding this term is implied by the section, and therefore redundant. By the use of the word “verified”, it is implied that timestamped is achieved.

Public Input No. 28-NFPA 915-2025 [New Section after 6.1.2]

6. 1 .3 _ Cybersecurity Capability for Devices

Data collection and _ transmission d evices shall _ meet the cybersecurity requirements of _ S ection 8.2.

Statement of Problem and Substantiation for Public Input

This public input is submitted on behalf of the NFPA Cybersecurity Advisory Committee (CAC) (www.nfpa.org/cac). The NFPA CAC notes that there has been consideration of the significance of cybersecurity protections as it relates to the scope of NFPA 915 and equipment in the scope of the technical committee. Important to the consideration of the suitability for remote testing and inspection, is how the data generated by these activities will be protected to ensure the integrity of the results that are delivered to the AHJs.

Submitter Information Verification

Submitter Full Name: Joshua Griffith
Organization: US Army Corps of Engineers (US
Affiliation: Cybersecurity Advisory Committee
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 06:47:51 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee determined that cybersecurity requirements should be consolidated in one location. Given this, this input has been resolved.

Public Input No. 17-NFPA 915-2024 [New Section after 7.1.2]

7.1.3 Approvals

Data shall be in accordance with applicable standards or other approved format.

Statement of Problem and Substantiation for Public Input

Not only should the use of a specific data collection format be approved by the AHJ, but the data itself should be in a format as required by a standard or approved by the AHJ.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 14:44:17 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-12-NFPA 915-2025
Statement: The committee agreed with the submitter. The inclusion of this requirement provides a specific reference to the data collected, which had been missing from the existing text. The data itself should be in a format as required by a standard or approved by the AHJ.

Public Input No. 27-NFPA 915-2025 [Section No. 8.2]

8.2* Cybersecurity.

8.2 Cybersecurity. ~~(Reserved)~~

8.2.1 * Application

Where required by governing laws, codes, or standards, or other parts of this standard, cybersecurity shall be provided in accordance with Chapter 8 for equipment software, system support tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance. [72:11.1.1]

A.8.2.1

Cybersecurity is not required for every system or application; it is only required when other sections of this standard, authorities, or regulations mandate that cybersecurity be incorporated into the system(s). Generally, there are greater cybersecurity concerns when systems are connected to external networks. [72:A.11.1.1]

8.2.2 * Network Connectable Equipment Software Development and Production Environments.

Development and production environments used to develop and manufacture network connectable equipment shall employ cybersecurity safeguards that are consistent with one or more of the following :

(1) NIST 's "The NIST Cybersecurity Framework 2.0"

(2) ISO/IEC 27001 , *Information security management systems*

(3) ANSI/ISA/IEC 62443-4-1: *Security for industrial automation and control systems - Part 4-1*

(4) IASME Consortium Cyber Essentials

(5) Other equivalent standards acceptable to a nationally recognized testing laboratory (NTRL)

(6) * Other applicable laws and regulations

[72:11.2]

A.8.2.2

The security practices for the design, development, production, and service of network connectable equipment includes the overall cybersecurity posture of the manufacturing company itself. For example, it does not matter how well a system is designed or deployed from a cybersecurity perspective if the manufacturer does not adequately secure its own development, manufacturing, and patch/update distribution systems. Threat actors can compromise products by installing covert back doors during initial development, or during the development and distribution of software updates. [72:A.11.2]

8.2.3 * Security Levels for Network Connectable Equipment.

All interfaces used to communicate with network connectable equipment shall be protected in accordance with the following:

(1) For non-internet protocol wired interfaces one of the following:

(a) Security Level 1 (SL1) in accordance with ANSI/ISA/IEC 62443-4-2, *Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components*

(b) Security Level 1 (SL1) in accordance with ANSI/ISA/IEC 62443-3-3, *Security for Industrial Automation and Control Systems, Part 3-3: System Security Requirements and Security Levels*

(c) Security Level 1 (SL1) in accordance with CAN/UL 2900-2-3, *Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems*

(d) Comparable level associated with Section 8.2.3(4)

(2) For non-internet protocol wireless interfaces or internet protocol wired and wireless interfaces that do not connect to publicly accessible networks, one of the following:

(a) Security Level 2 (SL2) in accordance with ANSI/ISA/IEC 62443-4-2

(b) Security Level 2 (SL2) in accordance with ANSI/ISA/IEC 62443-~~3-3~~

(c) Security Level 2 (SL2) in accordance with CAN/UL 2900-2-3

(d) Comparable level associated with Section 8.2.3 (4)

(3) For internet protocol wired or wireless interfaces that connect to publicly accessible networks, one of the following:

(a) Security Level 3 (SL3) in accordance with ANSI/ISA/IEC 62443-4-2

(b) Security Level 3 (SL3) in accordance with ANSI/ISA/IEC 62443-~~3-3~~

(c) Security Level 3 (SL3) in accordance with CAN/UL 2900-2-3

(d) Comparable level associated with Section 8.2.3 (4)

[72:11.3]

A.8.2.3

In general, there could be overlap in what this section requires and the end user's IT department's requirements. That overlap could require additional coordination in the case of Class N networks or internet communications, as IT departments could have more stringent requirements and certifications than listed in this Code. In those instances, IT compliance beyond this Code could be required for the owner. **[72:A.11.3]**

An example of a Security Level 1 (SL1) system consists of a fire alarm system with notification appliances and initiating devices that are connected using a

proprietary protocol two-wire interface and that is not connected to the internet. **[72:A.11.3]**

An example of a Security Level 2 (SL2) system consists of a signaling system with devices connected to a control unit using internet protocol communications on a dedicated network that does not connect to the internet. **[72:A.11.3]**

An example of a Security Level 3 (SL3) system consists of internet gateway module for off-premises transmission of signals from a fire alarm system with notification appliances and initiating devices that are connected using a proprietary protocol two-wire interface. In this case the gateway is SL3, and the remainder of the system is SL1. **[72:A.11.3]**

8.2.4 * _ Interconnecting Conductors, Cables, or Other Physical Pathways.

Interconnecting conductors, cables, or other physical pathways for use in Security Level 2 or higher applications in locations accessible to the public shall be protected by metal raceways or metal armored cables. **[72:11.4]**

A.8.2.4

An assumption is often made that attacks are launched remotely from the internet. However, there are many examples of attackers gaining access to a facility to enable an attack. For example, a system that has no networking capability, with only an RS-232 serial port can be connected to an RS-232-to-Ethernet adapter. This could be intended benignly, as a way of enabling remote monitoring or remote service, but it is a risk that should be considered, nonetheless. **[72:A.11.4]**

The protection by metal raceways or metal armored cables of interconnecting conductors, cables, or other physical pathways is also recommended for use in Security Level 1 applications. For improved physical security in systems where control units and data access points are not installed in restricted areas, using security tamper switches to produce a tamper signal for notification when an enclosure is opened should be considered. Tamper resistant fasteners can be employed on junction box covers to provide additional physical protection. **[72:A.11.4]**

8.2.5 _ Unused Physical Data Ports.

All unused physical data ports shall be protected _ in at least one of the following ways :

(1) Physically protected from unauthorized access

(2) Administratively disabled

(3) Configured to require a token-based authentication, certificate-based authentication, password, or other method that is consistent with the security requirements of the system

[72:11.6]

8.2.6 * _ Data Connections to External Networks.

When any data connection is made from the system to an external network, the

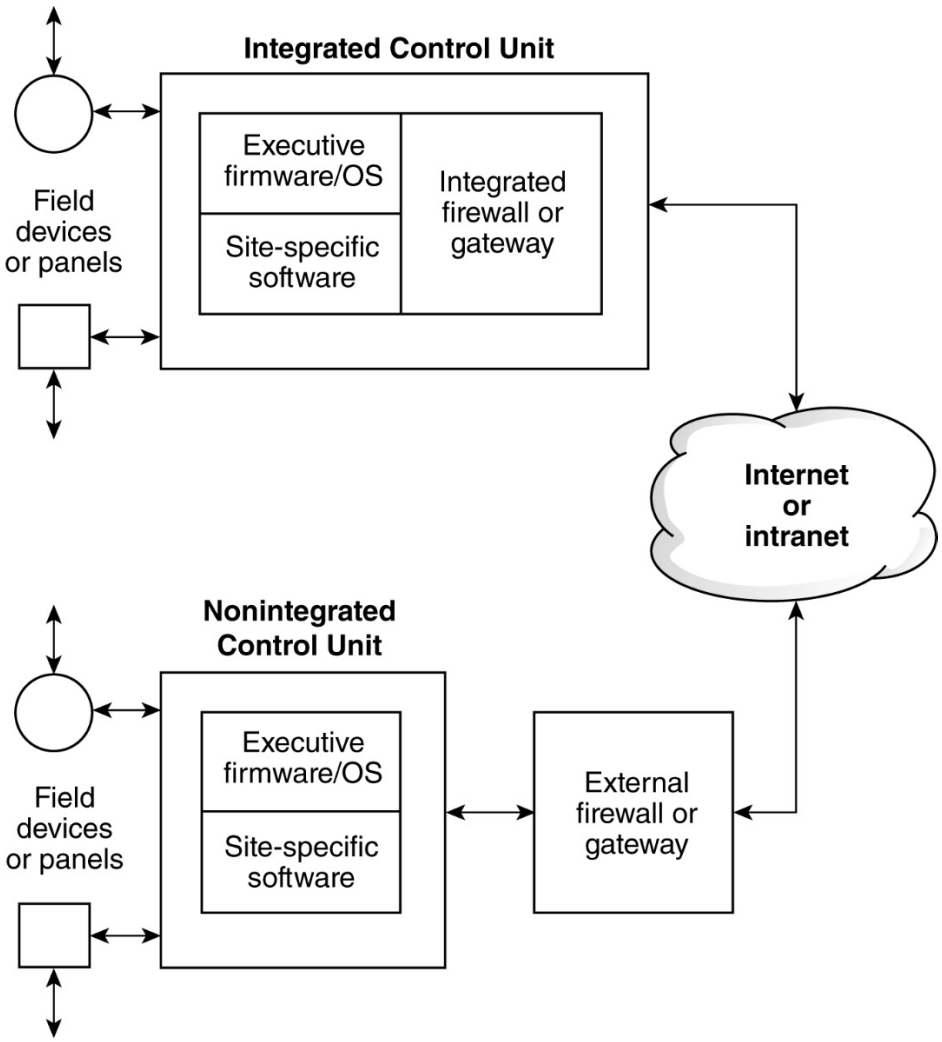
connection shall be protected by a gateway or firewall that ensures that only trusted traffic is allowed to pass. **[72:11.7]**

A.8.2.6

Figure A.8.2.6 depicts typical system typical firewall/gateway operation. Such functionality, when deployed, could take the form of physical hardware, firmware, or both. The firewall/gateway might be physically integrated into the control unit, as shown in the integrated control unit graphic, or a separate device/service that interacts with the control unit, as shown in the nonintegrated control unit.

Many networks have additional protections, such as multiple firewalls. **[72:A.11.7]**

Figure A.8.2.6 System Typical Firewall/Gateway Operation. **[72:Figure A.11.7]**



8.2.7 Network Connectable Equipment Cybersecurity Software Updates.

8.2.7.1

At least quarterly, the equipment manufacturer(s) shall do the following until the equipment is no longer supported by the manufacturer:

(1) Evaluate all relevant cybersecurity threats

(2) Determine if a software update is required to maintain the cybersecurity level achieved in compliance with 8.2.2

[72:11.8]

8.2.7.2

The system installer shall provide the name and contact information of the system owner or their representative to the equipment manufacturer(s) at the time of system acceptance testing. [72:11.8.2]

8.2.7.3 * _

The equipment manufacturer(s) shall notify the system owner or their representative of all required software security updates required to maintain the cybersecurity level achieved in compliance with 8.2.2, 8.2.3, and 8.2.4. [72:11.8.3]

A. 8.2.7.3

As security vulnerabilities are discovered, existing systems could be affected. It is important for manufacturers to provide solutions when vulnerabilities are discovered. Likewise, it is important to carefully manage the update and patch management infrastructure to ensure that corrections are available, have not been modified or spoofed, and are applied successfully. [72:A.11.8.3]

8.2.7.4 _

Software for network connectable devices shall be maintained by installing software security updates as required by the equipment manufacturer(s) to maintain the cybersecurity level achieved in compliance with 8.2.2, 8.2.3, and 8.2.4. [72:11.8.4]

8.2.7.5 _

Software security updates that are deemed necessary by the equipment manufacturer(s) for compliance with Section 8.2.4 shall be installed at least annually. [72:11.8.5]

8.2.7.6 _

Cybersecurity software changes to systems or system components shall be permitted to be made by remote access.

8.2.8 _ Notification of Termination of Cybersecurity Update Support.

The manufacturer shall notify the system owner or their representative of the termination of cybersecurity software update support required by 8.2.7 for any element of the system. [72:11.9]

8.2.9 _ Cybersecurity for System Support Tools.

A system support tool and the support tool interfaces shall comply with the requirements of Sections 8.2.2 through 8.2.8. [72:11.10]

8.2.10 _ Evidence of Compliance.

8.2.10.1 _

Evidence of cybersecurity compliance shall include one or more of the following:

(1) Certification of compliance by a nationally recognized testing laboratory

(2) Manufacturer certification for the specific type and brand of system provided by the manufacturer

(3) An assessment or certification program acceptable to the authority having jurisdiction

[72:11.11.1]

8.2.10.2

The validity of cybersecurity certificates shall be verified annually by the person testing the system. [72:11.11.2]

8.2.10.3

The validity of the equipment manufacturer's contact information for the system owner shall be verified annually by the person testing the system. [72:11.11.3]

8.2.11 Documentation.

The standards used and security levels employed in complying with Chapter 8 shall be identified in the system documentation. [72:11.12]

Additional Proposed Changes

File Name	Description	Approved
NFPA_915_Section_8.2_Proposal_based_on_72-2025_Chapter_11.docx	word file includes figure	

Statement of Problem and Substantiation for Public Input

This public input is submitted on behalf of the NFPA Cybersecurity Advisory Committee (CAC) (www.nfpa.org/cac). The CAC notes that there has been consideration of the significance of cybersecurity protections as it relates to the scope of NFPA 915 and equipment in the scope of the technical committee. The CAC recommends consideration of using the cybersecurity chapter from NFPA 72 2025 Chapter 11 as a template for the reserved cybersecurity Section 8.2.

NFPA 72 2025 Edition has taken a proactive approach to providing cybersecurity requirements for systems within its scope. It is reasonable for equipment that enables remote inspections and tests, or automated inspections and tests, to conform to cybersecurity standards that are consistent with the equipment being tested or inspected.
The intent is that cybersecurity requirements in 915, are triggered when required by other applicable laws, codes, standards, or specific sections of 915 that might directly reference section 8.2. In this way, cybersecurity requirements do not apply by sole virtue of including 8.2 in 915. There will be some other trigger, but once triggered, 915 will provide acceptable requirements to guide manufacturers, owners, and AHJs. On example of such a law is California IoT Security Law (SB-327)45. This law requires manufacturers of connected devices, often referred to as Internet of Things (IoT) devices, to provide reasonable security features for those devices and prevent hackers from modifying them. It also requires either a unique password for each device or a user-set password before the first use. More information on this law can be found by searching for "Bloomberg Law, Professional Perspective, California's New IoT Cybersecurity Law: A Guide for Business".
Part of the reason for this proposal is to establish the discussion within the relevant technical committees of what cybersecurity requirements are suitable for 915, and provide a vetted example of the cybersecurity requirements that can apply to some of the common equipment inside the scope of both documents, and provide the committee(s) a broad enough proposal that a task group(s) working between the first and second draft can provide alternate proposals that may be considered without the concern of it being new material.

Note, referenced figure is in the word file since it's unable to be put into terra.

Submitter Information Verification

Submitter Full Name: Joshua Griffith
Organization: US Army Corps of Engineers (US
Affiliation: Cybersecurity Advisory Committee
Street Address:
City:
State:
Zip:
Submittal Date: Mon Jan 06 06:38:59 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee resolved this PI based on the actions taken via PI-33.

Public Input No. 33-NFPA 915-2025 [Section No. 8.2]

8.2* Cybersecurity. - ~~(Reserved)~~

This section establishes cybersecurity requirements of network-connected systems and equipment used for remote inspections, automated inspections, distance monitoring and tests. The purpose of these requirements is to ensure the systems are protected against unauthorized access, data theft, and other cyber threats that could compromise their confidentiality, integrity, functionality, or reliability.

8.2.1* Cybersecurity Requirements

Network-connected systems shall follow the requirements of recognized cybersecurity frameworks and standards acceptable to the AHJ.

8.2.2 Cybersecurity Risk Assessment

A cybersecurity risk assessment shall be conducted as part of the remote inspection and test program for network-connected equipment, following the guidelines of the NIST SP 800-30, Rev.1, Guide for Conducting Risk Assessments, or other equivalent standards acceptable to the authority having jurisdiction (AHJ). The risk assessment shall identify potential vulnerabilities within data pathways, system interfaces, and connectivity points. Each system shall incorporate appropriate security controls to achieve required cybersecurity safeguards in accordance with 8.2.3.

8.2.3 Security Controls for Network-Connected Systems

All network-connected systems shall incorporate cybersecurity controls in accordance with the risk assessment and one or more of the following:

(1) ANSI/ISA/IEC 62443, Security for Industrial Automation and Control Systems Series

(2) Other standards acceptable to the AHJ

(3) Center for Internet Security (CIS) Controls

(4) NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations

(5) ISO/IEC 27001, Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements

(6) CAN/UL 2900-2-3, Software Cybersecurity for Network Connectable Products

8.2.4 Cybersecurity Testing for Network-Connected Systems

Testing for network-connected systems shall confirm the functionality of access controls, network pathway protections, and other safeguards that align with the system's designated security controls outlined in 8.2.3

8.2.5 Authorized Access

Only authorized personnel or authorized systems shall perform remote inspection and test activities on network-connected equipment. Access control measures shall include limiting access to essential personnel, maintaining access logs that record the date, identity, and purpose of access, and regularly reviewing and updating access credentials to ensure only current personnel have authorized access.

8.2.5.1 Network Connected Systems Maintenance Plan

A plan detailing the requirements of the regular maintenance of network connected systems shall be provided to the Authority Having Jurisdiction (AHJ). The plan shall include:

(1) patch and update review frequency.

(2) log review frequency.

(3) methods of maintaining an accurately connected equipment inventory with the status of all equipment.

(4) methods of maintaining the registry of authorized personnel and authorized systems.

(5) frequency of required audits.

8.2.6 Documentation of Cybersecurity Compliance

Remote inspection and test program documentation for network connected systems shall include:

(1) evidence of cybersecurity compliance,

(2) audit results and remedial action,

(3) a history of system changes including connected equipment, software, updates, and patches,

(4) terminations of cybersecurity provisions,

(5) documentation of cybersecurity incidents and responses.

8.2.6.1 Audits

Audits shall include records of each cybersecurity assessment, assigned security controls, and identified vulnerabilities, along with records of all software updates and patches applied to maintain system security in accordance with 8.2.3.

8.2.7 Update and Patch Management

All cybersecurity software updates and patches specified by the equipment manufacturer, or necessary to maintain the system's security, shall be installed at least annually. Each update and patch shall be recorded as part of the remote inspection and test program documentation to verify ongoing cybersecurity compliance.

8.2.8 Cybersecurity Monitoring and Incident Response

8.2.8.1 Network-connected systems shall be monitored at intervals acceptable to the AHJ, to identify cybersecurity incidents that could affect system integrity or functionality.

8.2.8.2 In the event of a cybersecurity incident, immediate response measures shall be taken to isolate and secure the affected systems, notify stakeholders, and restore system functionality. Documentation of the incident and response actions shall be included in the remote inspection and test records.

8.2.9 Documentation of Termination of Cybersecurity Support

Any termination of cybersecurity provisions shall be documented as part of the remote inspection and test records. Upon termination of cybersecurity provisions, A cybersecurity risk assessment shall be conducted per 8.2.2. Verification of new cybersecurity compliance in accordance with 8.2.1 and 8.2.6.1 shall be made to ensure that system cybersecurity measures remain up-to-date and effective.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. The scope of NFPA 915 relies solely on digital devices and network connected systems for the implementation of data transmission, collection, and storage.
Cybersecurity is crucial in today's digital world as it safeguards sensitive information like personal data, business confidentials, and government data from theft and misuse. It prevents significant financial losses due to data breaches, disruptions to business operations, and ransomware attacks.

Furthermore, strong cybersecurity practices are essential within the remote inspection and testing realm for maintaining public trust in businesses and government institutions, and for protecting critical infrastructure such as healthcare systems, energy grids, and transportation networks from cyberattacks.

Related Public Inputs for This Document

Related Input	Relationship
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 31-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]	
Public Input No. 36-NFPA 915-2025 [Chapter 4]	
Public Input No. 37-NFPA 915-2025 [Chapter A]	

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 11:49:31 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: FR-14-NFPA 915-2025

Statement: The committee agreed with the submitter with modification. The committee determined, after lengthy debate, that this material should reside within a new annex to provide visibility on technical requirements but not including specifics in a prescriptive format. This annex material provides detailed guidance and resources for consideration for users of NFPA 915 as it applies to the remote inspection and testing process. As cybersecurity is evolving, the committee welcomes Public Comment on this topic to review during the Second Draft meeting.

For new Annex B, see FR-24.

Public Input No. 38-NFPA 915-2025 [Section No. 8.2]

8.2* Cybersecurity. ~~(Reserved)~~

8.2.1 Remote software updates to a fire detection and notification system that have a potential influence on safety and on compliance with the particular system safety standard shall be performed in accordance with UL 5500.

Add to Chapter 2 if approved.

2.5 UL Publications.

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

UL5500 Remote Software Updates, 2018, revised 2023 .

Statement of Problem and Substantiation for Public Input

: Current practices for updating fire detection and notification system operating system software may include remote updates through the use of an internet connection. These remote software updates may affect life-safety function and performance and the required compliance with the applicable system/product certification standard. Requiring remote software updates are performed in accordance with UL 5500 will provide additional assurance that the updates are in compliance with manufacturer's instructions and procedures to maintain the essential life-safety functionality of the system.

UL 5500 is an overlay standard for software updates taking into account the manufacturer's recommended process. It is specific to software elements having an influence on safety and on compliance with the particular end product safety standard. UL 5500 covers hardware compatibility necessary for safety of the remote software update. UL 5500 is intended to be used in conjunction with the appropriate end product safety standard.

Submitter Information Verification

Submitter Full Name: Kelly Nicolello
Organization: UL Solutions
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 18:26:59 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: The committee did not agree with the submitter. This language is specific to software updates to fire detection and notification systems. This is outside the scope of cybersecurity requirements within NFPA 915 and may be more appropriate to other NFPA standards, including, but not limited to, NFPA 72.

Public Input No. 37-NFPA 915-2025 [Chapter A]

Annex A Explanatory Material

Annex A is not a part of the requirements of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.1.1.1

Methods for conducting remote inspections and tests can range from handheld devices to other means, including, but not limited to, unmanned aircraft systems (drones), to achieve the stated objectives of the authority having jurisdiction. Requirements for implementation of the procedures, methods, and documentation required by this standard are to be developed by the authority having jurisdiction to best respond to their specific needs. Inspections and tests of buildings, structures, systems, and premises, including underground spaces and aerial areas, can include electrical, HVAC, and fire protection, among other disciplines.

Tests can be either observed remotely (the same as an inspection) while they are happening or recorded for review by the authority having jurisdiction.

Automated inspections and tests are permitted by many of the installation standards for fire protection systems, including NFPA 13, NFPA 14, NFPA 20, NFPA 25, and *NFPA 72*. If approved for use by the authority having jurisdiction, periodic inspections and tests such as those required for water-based fire protection systems, fire alarm systems, and other mechanical and electrical systems can be performed automatically and the results recorded for review.

Distance monitoring involves installing electronic devices, meters, or equipment to observe conditions in mechanical and electrical systems that can be constantly reported to a dashboard or similar display or requested on an as needed basis.

A.1.1.2

An NFPA standard, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements, is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions of a standard are not considered a part of the requirements of a standard and are, therefore, located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA manuals of style.

A.1.2

The intent of remote inspection and testing, automated inspection and testing, and distance monitoring methods is to ensure that a facility, structure, system, site, feature, construction, or process satisfies the applicable project requirements, design, and applicable governing laws, codes, regulations, or standards. Additionally, it is the intent of this standard that these methods should supplement and facilitate inspections and tests, automated inspection and testing, and distance monitoring.

A.1.3

This standard is written to be compatible with the requirements of any jurisdiction. Requirements can be modified by any jurisdiction based on the needs, technology, and conditions.

A.1.3.1

It is the intent of this section to allow several types of inspections and tests to be conducted, including, but not limited to, routine, scheduled, and special inspections or tests. However, determining the types of inspections and tests allowed, whether they are performed in person or through automated inspection and testing methods, should be at the discretion of the authority having jurisdiction. Distance monitoring is usually performed by the owner or their representative but can also benefit the authority having jurisdiction especially for high-risk facilities where it is important to know the status of protection equipment and systems at all times.

A.1.3.2

The authority having jurisdiction should take into consideration specific situations and/or conditions that exist at the site when determining the feasibility of remote inspections and testing, automated inspection and testing, and distance monitoring. Some examples include the following:

(1) Complex systems. The inspection or test of some complex systems might require more detail than can easily be obtained using a remote inspection or test.

(2) Poor conditions (due to low lighting, low connectivity). Certain conditions can lend themselves to having an inspection or test witnessed remotely or make it difficult to use remote inspection and testing technologies. For instance, an inspection or test required in an area with no or low lighting could use a drone or a robot equipped with its own lighting source. Other conditions could make using certain remote inspection and testing technologies prohibitive, such as in areas with low connectivity where a live inspection or test using an internet connection is not possible.

(3) Access to work. Not being able to access a work area due to height, safety concerns, the inability to shut down a process or a piece of equipment, energized equipment, and so forth, are examples of situations where remote inspections and tests could be performed using a drone, a robot, a fixed transmitting device such as a security camera, a portable transmitting device such as an industrial borescope, and so forth.

(4) Availability/understanding of technology. The authority having jurisdiction should decide if the remote inspection and testing, automated inspection and testing, and distance monitoring technology are understood well enough by both parties to be effective in obtaining the information needed.

(5) Confined/hazardous locations that need to be physically entered. Remote inspections and tests, automated inspections and tests, and distance monitoring could be effective in protecting personnel from confined or hazardous locations. However, the authority having jurisdiction should also ensure that the setup, execution, or completion of a remote inspection or test does not present additional hazards to inspection or test personnel.

(6) Mobility or other physical limitations of the inspector.

(7) Ability of the automated inspection and testing devices and equipment to comply with the applicable NFPA standard.

(8) The need to have live data transmitted to a specific location for distance monitoring of systems or equipment to ensure their readiness in the event of a fire.

(9) Any other conditions that are not conducive for a personal inspection or test such as, but not limited to, the following:

(10) Private property concerns

(11) Legality of methods employed, such as entering controlled airspace or environmentally sensitive areas

(12) Excessive travel time to the site

(13) Cost concerns

(14) Exposure to environmental health and safety concerns

A.1.3.3

There is a hierarchy between ordinances and adopted codes and standards that must be considered and followed. The authority having jurisdiction should be consulted where there are conflicting requirements to determine which one takes precedence over the other.

A.1.7.1

See A.3.2.2 for an explanation of how the term *authority having jurisdiction (AHJ)* is used in a broad sense to include jurisdictions and approval agencies that could be involved in approving the provisions of this standard.

A.1.7.4

An authority having jurisdiction can perform the remote inspection or test using their own resources, including qualified personnel and approved methods and devices, as long as they meet the requirements of this standard. However, they can also allow or require a third-party entity to perform the remote inspection or test.

A.3.2.1 Approved.

The National Fire Protection Association does not approve, inspect, or certify any installations, procedures, equipment, or materials nor does it approve or evaluate testing laboratories. In determining the acceptability of installations, procedures, equipment, or materials, the "authority having jurisdiction" may base acceptance on compliance with NFPA or other appropriate standards. In the absence of such standards, said authority may require evidence of proper installation, procedure, or use. The "authority having jurisdiction" may also refer to the listings or labeling practices of an organization that is concerned with product evaluations and is thus in a position to determine compliance with appropriate standards for the current production of listed items.

A.3.2.2 Authority Having Jurisdiction (AHJ).

The phrase "authority having jurisdiction," or its acronym AHJ, is used in NFPA standards in a broad manner because jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his or her designated agent assumes the role of the authority having jurisdiction; at government installations, the commanding officer or departmental official may be the authority having jurisdiction.

A.3.2.4 Listed.

The means for identifying listed equipment may vary for each organization concerned with product evaluation; some organizations do not recognize equipment as listed unless it is also labeled. The authority having jurisdiction should utilize the system employed by the listing organization to identify a listed product.

A.3.3.2 Building Systems.

Building systems include all electrical power services; communication and security services; electrical control systems; HVAC systems; water, steam, wastewater, and drainpipes and services; fire suppression systems including water-based and non-water-based systems; oil and piped hydraulic and pneumatic systems. [**914,** 2023]

A.3.3.3 Buildings.

The term *building* is to be understood as if followed by the words "or portions thereof." Each portion of a building that is separated from other portions by a fire wall is considered to be a separate building.

A.3.3.8 Data.

Data can include photographic images, video, audio recordings, copies of reports, and other associated items.

A.3.3.9 Data Device.

Data devices are capable of collecting images or other forms of data and storing the data so it can be transferred to an entity at a later time or are capable of transmitting data in real time to an entity through various means. Examples include cameras, video recorders, cell phones, and other smart devices.

A.3.3.14 Inspection.

An inspection is a means to determine compliance. Examples of this include conformity to a specification or design or a process to ensure expected performance. This can take many forms. The inspection should match the approved design and installation documents, or witness a test to prove compliance with acceptance criteria. In all of these cases confirmation is required, which can either be in person by the AHJ or through the use of technologies that can provide the same result or better than an in-person inspection.

A.3.3.19 Remote Inspection.

The following are examples of remote inspections:

(1) Evaluation of objects, materials, or construction from a distance or off-site location

(2) Aerial inspections

(3) Off-site witnessing of fire system testing

A.4.1.2

Sensitive or classified subjects that the property owner should protect include, but are not limited to, personal information of patients protected by HIPAA, proprietary corporate data, and so forth.

A.4.1.3

The property owner should assume that all remote inspections and tests will consist of video, image, and audio recording, and it might be necessary for the property owner to notify the building occupants prior to a remote inspection or test to prevent unauthorized photography and sensitive information from being recorded.

A.4.3

The entity performing the remote inspection or test can be either the property owner, the contractor of work, or a third party, depending on the work being performed.

A.4.3.1

Those conducting remote inspections and tests should always assume that there is a *property owner* or designated representative. One should never assume that it is permissible to enter vacant land, public property, remote areas, or airspaces without authorization.

A.4.3.2.3

It is the intention of the committee that the written inspection or test plan augments inspection or test documentation required by other nationally recognized codes and standards. The committee also recognizes that not every remote inspection or test will require a narrative description of the anticipated remote inspection or test process. For example, a written inspection or test plan for the remote inspection or test of a hot water heater is most likely not necessary as the inspection or test of the equipment is self-explanatory. Ultimately, the AHJ will make the determination as to whether the remote inspection or test requires a written plan or not.

A.4.3.2.3.2

Administrative information should include the identification of participants, the type of inspection or test, the reason for the inspection or test, remote inspection or test method to be used, the exact location of the inspection or test, and the proposed date and time of the remote inspection or test.

A.4.3.2.3.3

A narrative description of the inspection or test process should include the preparation; equipment to be used; qualifications and licenses required; hazards identification and how the hazards will be mitigated; the inspection or test execution timeline, including major steps and phases of the inspection or test; general description of data-gathering method; and how the inspection or test will be ended and the property secured.

A.4.4.1

The following criteria examples are to assist the AHJ in determining the acceptable remote inspection or test criteria for their jurisdiction:

(1) Suitability of the inspection or test, which could include the expected success of the inspection or test; the available site and task safety available, or lack thereof; and size/scope of the work to be inspected

(2) Limitations, which could include weather, trained personnel, privacy constraints, cellular/WIFI connections, and any constraints that will affect safety, health, and the environment

(3) Acceptance criteria, which could include upper and lower limits of data results in accordance with codes, standards, or best practices

(4) Inspection or test requirements, which could include supervision, inspector qualifications, insurance, contracts, and other risk management requirements

(5) Documentation, which could include the allowance or disallowance of electronic reports, photography, and video

(6) Technology, including the allowable standard for remote testing equipment and systems

(7) Submission format, including electronic data, cloud storage, handwritten reports, and paper reporting

(8) Scheduling requirements, including times, dates, and weather conditions

(9) Dissemination of modifications and current practices to the AHJ required criteria

A.5.1

Alternatively, the contractor of work, or other approved entity, could be designated to provide this information. Other geolocation technologies, such as GPS or Bluetooth, can be considered to help validate the location.

A.5.2.1

The address should be the physical address where the inspection or test is to take place; for example, 1 Batterymarch Park, Quincy, MA 02169. If no address is provided, the use of other approved markers, such as parcel ID, plot plan designations, GIS coordinates, or other geolocation technologies could be considered.

A.5.2.2

Because the type of structure could vary, please see NFPA 220 for applicable building types.

A.5.2.3

The areas within a structure might include a floor and specific location, for example, a second floor bathroom. This area should be able to be verified via any submitted materials.

A.5.3

The type of occupancy could be a one- or two-family dwelling, an apartment, or a health care facility, among others. See NFPA *101*, *NFPA 5000*, or applicable life safety or building codes for occupancy types.

A.5.5.1

Unless modified by the AHJ, the format to record the date should be month/day/year. For example, 10/1/2019 would indicate October 1st of the year 2019.

A.5.5.2

Unless modified by the AHJ, the format to record time should be hours/minutes/meridiem. For example, 9:05 a.m. would indicate nine hours, five minutes, ante meridiem, and 9:05 p.m. would indicate nine hours, five minutes, post meridiem.

A.6.1.1

The use of data collection/transmission devices could be considered integral to performing remote inspections and tests. The entity performing the remote inspection or test should also be familiar with the data collection device that has been selected.

The technical committee recognizes the ever-changing technological landscape. The intent of this section is to allow for the consideration of other data collection/transmission devices as appropriate, as they become available and are approved by the AHJ.

Authorities such as the Federal Communications Commission (FCC) often regulate many types of devices.

A.6.1.2

See Table A.6.1.2 for guidance on both devices and formats.

Table A.6.1.2 Data Collection Capabilities by Device

Type	Live Video	Recorded Video	Live Audio (In Person)	Live Audio (Data Collection/ Transmission Device)	Recorded Audio	Recorded Digital Photography	Recorded Nondigita Photograp
Cellular telephones/ smartphones	X	X	X	X	X	X	N/A
Satellite telephones	n/a	n/a	X	X	n/a	n/a	n/a
Cellular tablets/pads	X	X	X	X	X	X	n/a
Wireless/ network-connected computers	X	X	X	X	X	X	n/a
Digital telephones	n/a	n/a	X	X	n/a	n/a	n/a
Digital audio recorders	n/a	n/a	n/a	X	X	n/a	n/a
Digital cameras	n/a	n/a	n/a	n/a	n/a	X	n/a
Digital video recorders	n/a	X	n/a	n/a	n/a	n/a	n/a
Computers	X	X	n/a	X	X	X	n/a
Analog telephones	n/a	n/a	X	X	n/a	n/a	n/a
Audio cassette recorders	n/a	n/a	n/a	n/a	n/a	n/a	X
Radios	n/a	n/a	X	n/a	n/a	n/a	n/a
Film cameras	n/a	n/a	n/a	n/a	n/a	n/a	X
Video cassette recorders	n/a	X	n/a	n/a	n/a	n/a	n/a
Wave detection technologies	n/a	n/a	n/a	n/a	n/a	n/a	X
sUAS	X	X	X	X	X	X	n/a

X: Capable.

N/A: Not applicable.

A.6.2

A wireless device is one that is connected to a wireless network, either directly or from a wireless connection, which might or might not be connected to the internet.

A.6.2.1(4)

This could include laptops or similar devices.

A.6.2.1(5)(a)

Wireless Local Area Networks (WLAN) are wireless networks that use radio waves. The backbone network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network. The range of a WLAN can be anywhere from a single room to an entire campus.

A.6.2.1(5)(b)

Wireless Personal Area Networks (WPAN) are short-range networks that use Bluetooth technology. They are commonly used to interconnect compatible devices near a central location, such as a desk. A WPAN has a typical range of about 30 ft (9.1 m). It is a wireless-type device that uses either battery or line voltage. A digital device is digitized to transmit a signal and modulated to be sent out wireless.

A.6.2.1(5)(c)

Wireless Wide Area Networks (WWAN) are created through the use of mobile phone signals typically provided and maintained by specific mobile phone (cellular) service providers. WWANs can provide a way to stay connected even when away from other forms of network access.

A.6.2.2

Authorities such as the Federal Communications Commission (FCC) often regulate many types of devices. Also, see Table A.6.1.2 for further information.

A.6.2.3

Examples of other wireless devices would be certain smart watches or glasses.

A.6.3

A digital device is one that records or transmits in a digital format via a wireless, ethernet, hard-wired, or dial-up connection. Digital devices might or might not be connected to a network or the internet.

A.6.3.3

An example of a different type of digital device not mentioned might be glasses that allow connection to a digital device or cellular network.

A.6.4

A nondigital device is one that uses physical media to transmit or record in a predetermined format that is not capable of being connected to a network.

A.6.4.1(3)

Radios are meant to include two-way radio communication devices that can span large distances.

A.6.4.1(6)

These could include radar, sonar, laser, x-ray, lidar, or other similar technologies.

A.6.5

A vehicle, for the purposes of this standard, is an apparatus that can transport humans, or be directly controlled by humans, for the purposes of conducting a remote inspection or test.

A.6.5.1.1

An example of a nonaerial manned vehicle could include, but not be limited to, an underwater sled. These devices provide access to areas within the structure that normally might or might not be accessible otherwise.

A.6.5.1.2

An example of a nonaerial unmanned vehicle could include, but not be limited to, a motorized robotic apparatus used to examine attics, crawl spaces, piping systems, tunnels, or other inaccessible areas.

A.6.5.1.3

An example of another nonaerial unmanned vehicle could include, but not be limited to, a motorized lift apparatus used to examine exterior building components and facades. These devices are not normally accessible. Additionally, while the lift itself is aerial, the base remains on ground level.

A.6.5.2.1

An example of an aerial manned vehicle could include, but not be limited to, an airplane or helicopter used to survey a large site. These devices provide access to areas above a site or a structure that are not normally accessible otherwise.

A.6.5.2.2

The most common example of an unmanned aerial vehicle are drones. While not limited solely to drones, these devices provide access to areas above a site or structure that are not normally accessible. Drones typically provide a more cost-effective and substantive aerial examination than traditional aircraft.

A.6.5.2.2.1

See 3.3.22 for the definition of unmanned aircraft.

A.6.5.2.2.1.1

For example, the AHJ includes the aviation regulatory authority having jurisdiction. In the United States, this is the FAA. Internationally, this is the applicable national civil aviation authority. [**2400:**A.1.5]

A.6.5.2.2.1.2

Small unmanned aircraft means an unmanned aircraft weighing less than 55 lb on takeoff, including everything that is on board or otherwise attached to the aircraft. The weight limit defining a small unmanned aircraft will vary from country to country and quite often will be determined by the applicable aviation authority. The current definition is based on regulations in the United States developed by the Federal Aviation Administration (FAA). 14 CFR Part 107, often referred to as “the Small Unmanned Aircraft Rule — Part 107” establishes the less than 55-lb (25 kg) weight limit used in this standard for small unmanned aircraft. Public safety entities will need to apply the applicable weight limit, if any, based on the AHJ. [**2400:**A.1.3.2]

A.6.5.2.2.1.3

This should be a person who has been found to be properly qualified to exercise the privileges of a remote pilot and has the final authority and responsibility for the operation and safety of sUAS operation as determined by the AHJ. See NFPA 2400 for further details.

A.6.5.2.2.1.4

A public safety entity is one that has a mission to protect life, property, or the environment or any combination of these. An example of a public safety operation could be an AHJ conducting an inspection or test of a bridge.

A.6.5.2.2.1.5

See A.6.5.2.2.1.2. Additionally, see Table A.6.1.2 for further information.

A.6.6

The technical committee recognizes the ever-changing technological landscape. The intent of this section is to allow for the consideration of other data collection/transmission devices as appropriate and as they become available and are subject to approval by the AHJ.

A.6.6.1

The technical committee recognizes the ever-changing technological landscape. The intent of this section is to allow for the consideration of other vehicles as appropriate and as they become available and are subject to approval by the AHJ.

A.6.6.2

Examples of data-sensing devices include, but are not limited to, the following:

(1) Pressure transducers

(2) Temperature sensors

(3) Vibration sensors

(4) Motion detectors

(5) Flow sensors

A.7.1

The use of specific data collection formats is an integral consideration when determining applications for remote inspections and tests. Only formats that are approved by the AHJ should be used. The entity performing the remote inspection or test should also be familiar with the data collection/transmission device that has been selected. Finally, the AHJ should provide consideration for nondigital formats, where appropriate.

A.7.1.1

The sender is most likely the entity performing the remote inspection or test but might be others as approved.

A.7.1.2

The receiver is most likely the AHJ but might be others as approved.

A.7.2.1(1)

These signals would generally be from primarily a wireless device. However, a digital collection device could be used.

A.7.2.1.1(1)

Loss of video and/or audio signals can negatively impact the effectiveness of remote inspections and tests. The AHJ will need to determine whether any loss of signal impacts the remote inspection or test.

A.7.2.1.1(2)

Adequate light levels make it possible for the receiver to view the intended area being shown. Great care needs to be taken to provide adequate lighting, which should not be too dim or too bright.

A.7.2.1.1(3)

The quality of video needs to be acceptable to the receiver. While video minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality video that the sender’s data collection/transmission device will support. Unless approved by the AHJ live video should not be edited.

A.7.2.1.1(4)

The quality of audio needs to be acceptable to the receiver. While audio minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality audio that the sender’s data collection/transmission device will support.

A.7.2.2(1)

These signals could be from a wireless device, digital device, or a nondigital device. Generally, a wireless device would provide the video in a digital format. A nondigital device would provide the video via a manual means, such as a tape or some type of magnetic media. Finally, a digital device can provide video by either means.

A.7.2.2.1(1)

Adequate light levels make it possible for the receiver to view the intended area being shown. Great care needs to be taken to provide approved exposure.

A.7.2.2.1(2)

The quality of video needs to be acceptable to the receiver. While video minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality video that the sender’s data collection/transmission device will support.

A.7.2.2.1(3)

The quality of audio needs to be acceptable to the receiver. While audio minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality audio that the sender's data collection/transmission device will support.

A.7.2.2.1(4)

The AHJ will need to be consulted on the type of recorded video to be presented, whether it is original unedited recorded video or edited for quality.

A.7.2.2.2

Manual means of supplying video can include, but not be limited to, physical delivery, mail delivery service, or courier.

A.7.3.1.1

During remote inspections and tests, it might be necessary to have in-person conversations. An example of this is an entity performing the remote inspection or test who is meeting with an AHJ on site. This AHJ, in turn, might be using a phone to relay information to another AHJ at a remote location.

A.7.3.1.1(1)

These signals would generally be from conversation but could also be from radios. This might also include the use of an interpreter.

A.7.3.1.2(2)

This could also include the use of an interpreter.

A.7.3.2

It might be necessary to use live audio during remote inspections and tests. An example of this would be to provide an audio recording of a mechanical fan running to showcase the decibels generated during startup.

The quality of audio needs to be acceptable to the receiver. While audio minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality audio that the sender's data collection/transmission devices will support.

A.7.3.2(1)

These signals could include a variety of data collection/transmission devices, some of which might use video.

A.7.3.2.1(1)

The quality of audio needs to be acceptable to the receiver. While audio minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality audio that the sender's data collection/transmission devices will support.

A.7.3.2.1(2)

The AHJ will need to be consulted on the type of live audio to be presented, whether it is original unedited audio or edited for quality.

A.7.3.3(1)

These signals could be from a wireless device, digital device, or a nondigital device. Generally, a wireless device would provide the video in a digital format. A nondigital device would provide the video via a manual means, such as a tape or some type of magnetic media. Finally, a digital device can provide video by either means.

A.7.3.3.1(1)

The quality of audio needs to be acceptable to the receiver. While audio minimum formats change based on signal strength, location, and technological advancement, it is important to provide the highest quality audio that the sender's data collection/transmission device will support.

A.7.3.3.1(2)

The AHJ will need to be consulted on the type of audio to be presented, whether it is original unedited audio or edited for quality.

A.7.3.3.3

Manual means of supplying video can include, but not be limited to, physical delivery, mail delivery service, or courier.

A.7.4.2(1)

The quality of digital photography needs to be acceptable to the receiver. While digital photography minimum formats change based on format, resolution, camera types, and technological advancement, it is important to provide the highest quality photograph that the sender's data collection/transmission device will support. The AHJ will need to be consulted on the type of photography to be presented, whether it is original unedited photography, or edited for quality.

A.7.4.2(2)

The format could include a multitude of computer-based file formats, with .jpg being the most common.

A.7.4.2(3)

The storage size of the file being sent is important, as the receiver might not be able to receive large files by methods such as email. The transmission of photographs should be reviewed ahead of time to determine the most effective method.

A.7.4.4(1)

The quality of nondigital photography needs to be acceptable to the receiver. As nondigital photography could encompass film photography, it is important that minimum requirements be set to ensure the photograph will be correctly used. In some cases, nondigital photographs could be converted to digital photographs via scanning for use in digital storage. As such, it is important to provide the highest quality photograph that the sender's data collection/transmission device will support. The AHJ will need to be consulted on the type of photography to be presented, whether it is original unedited photography or edited for quality.

A.7.4.4(2)

The format would primarily be on printed paper or other suitable materials as approved.

A.7.4.4(3)

The physical size of the nondigital photograph being sent is important. Traditionally sized photographs might not be large enough to accurately show the area being reviewed in the remote inspection or test. The transmission of photographs should be reviewed ahead of time to determine the most effective method.

A.7.5.1

The technical committee recognizes that, in some cases, a written format could be suitable for remote inspections and tests. The use of a written format should only be with the approval of the AHJ.

A.7.6.2

NFPA standards, such as NFPA 20 and NFPA 25, contain annex guidance on automated testing and remote monitoring data formats. This material should be considered when reviewing data formats.

A.7.7

The technical committee recognizes the ever-changing technological landscape. The intent of this section is to allow for the consideration of other data collection formats as appropriate and with the approval of the AHJ.

A.8.1.1

Accumulated data could include, but not be limited to, documents, photos, streaming video, and other media collected during the remote inspection or test.

Cybersecurity recommendations are contained in Annex J of *NFPA 72*. For additional reference, see the NFPA Fire Protection Research Foundation report, *Cybersecurity for Fire Protection Systems*

A.8.2 —

Where required by governing laws, codes, standards, or other parts of this standard, cybersecurity should be provided for equipment, software, firmware, tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

Cybersecurity is not required for every system or application; it is only required when authorities or regulations mandate that cybersecurity be incorporated into the system(s). Generally, there are greater cybersecurity concerns where systems are connected to external networks.

Cybersecurity for Remote Inspection and Test Activities

This annex provides additional guidance on implementing the cybersecurity provisions within Section 8.2, addressing cybersecurity considerations across remote inspection and test activities for network-connected systems.

A.8.2.1 Examples of cybersecurity frameworks and standards that may be acceptable to the AHJ including but are not limited to, the NIST Cybersecurity Framework , ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements, UL 2900: Software Cybersecurity for Network-Connectable Products, and the ANSI/ISA/IEC 62443 Series of Standards.

A.8.2.2 Cybersecurity Risk Assessment

The cybersecurity risk assessment should include an evaluation of potential cyber threats related to data pathways, system interfaces, and connected equipment. Assessing products, equipment, or systems to established standards such as:

(1) UL 2900, Software Cybersecurity for Network-Connectable Products,

(2) ANSI/ISA/IEC 62443, Security for Industrial Automation and Control Systems Series,

(3) ISO/IEC 27001, Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems – Requirements

All utilize Cybersecurity Risk Assessments as part of the evaluation process.

A.8.2.3 Security Controls for Network-Connected Systems

Cybersecurity Controls are sometimes delineated by security levels. While not all the referenced frameworks in 8.2.3 have explicit tiered security levels, they all provide a structured approach to assessing and managing cybersecurity risk.

When designing a tiered security approach, it's important to consider factors like the sensitivity of the data, the criticality of the system, and the potential impact of a security breach. By carefully selecting and implementing appropriate security controls, organizations can effectively protect their network-connected equipment and systems. The specific standards that an organization should follow depend on its industry, size, and risk tolerance.

A.8.2.4 Authorized Access

Access control requirements in Section 8.2.5 include maintaining credentials for authorized personnel, implementing least privilege access, and ensuring proper access logging for network-connected systems. Organizations may refer to NIST Special Publication 800-63-4 for best practices in credential management and user access verification to support compliance.

A.8.2.7 Cybersecurity Incident Response

The cybersecurity incident response requirements in Section 8.2.8 provide a structured approach to addressing cybersecurity incidents. Recommended practices, including system isolation and stakeholder communication, align with the guidelines in the NIST Cybersecurity Framework and ANSI/ISA/IEC 62443 for managing cybersecurity threats effectively .

A.8.3.2 __

Content for submission could include multiple forms of data obtained in Chapter 7 but could also be in the form of a report.

A.8.3.3

It is not the intent of this section to prohibit or require the recording of a live remote inspection or test.

A.8.4.2

The submission of content should be transmitted in as secure a method as practicable or as required by the AHJ.

A.8.4.4

The AHJ must oversee the capture of all live content. One example of live transmission could include streaming video. Use of video conferencing or live streaming applications should be approved by the AHJ.

A.8.4.5

The technical committee understands that each jurisdiction has different processes and internal requirements. A procedure to reasonably verify the transmission of content should be developed and shared with relevant stakeholders. An acknowledgement of receipt should not be interpreted as approval by the AHJ.

A.8.5.1

Some content material might not be stored, storable, or retrievable for future use. One example of this is live streaming. There could also be security concerns or contractual agreements that need to be considered.

A.8.5.2

The storage and delivery of content might not be subject to any explicit requirements. Promulgated federal, state, or local laws or capabilities sometimes limit the amount of control that AHJs have to modify specific policies or procedures.

A.8.6

Absent any specific laws or requirements, a recommendation for retention of remote inspection or test records is 3 years.

Statement of Problem and Substantiation for Public Input

This Public Input is being submitted on behalf of NFPA 915 Task Group 5, Joseph Cervantes, George Mostardini, Scot Stockstill, Maria Marks, Yousef Alsaadi. The provisions in Annex A.8.2 address the increasing reliance on network-connected systems and equipment for remote inspections, automated testing, and monitoring. These systems introduce unique cybersecurity risks, including unauthorized access, data breaches, and system malfunctions that could compromise safety, reliability, and compliance.

The annex aligns NFPA 915 with globally recognized cybersecurity standards and frameworks, such as the NIST Cybersecurity Framework, ISO/IEC 27001, and ANSI/ISA/IEC 62443, ensuring organizations adopt proven methodologies for risk assessment, security controls, and incident response. Incorporating cybersecurity requirements strengthens the resilience of network-connected systems by identifying and mitigating vulnerabilities across data pathways, interfaces, and connected devices.

By emphasizing structured risk assessments, tailored security controls, access management, and incident response, these provisions provide a comprehensive approach to safeguarding remote inspection and testing activities. This ensures operational continuity, protects critical data, and maintains trust in the technology used, fostering global consistency and industry alignment with best practices.

Related Public Inputs for This Document

Related Input	Relationship

Public Input No. 31-NFPA 915-2025 [Section No. 3.3]
Public Input No. 32-NFPA 915-2025 [Section No. 3.3]
Public Input No. 33-NFPA 915-2025 [Section No. 8.2]
Public Input No. 34-NFPA 915-2025 [Section No. 3.3]
Public Input No. 35-NFPA 915-2025 [Section No. 3.3]
Public Input No. 36-NFPA 915-2025 [Chapter 4]

Submitter Information Verification

Submitter Full Name: Joseph Cervantes
Organization: Space Age Electronics
Affiliation: NFPA 915 Task Group 5
Street Address:
City:
State:
Zip:
Submittal Date: Tue Jan 07 12:28:33 EST 2025
Committee: REI-AAA

Committee Statement

Resolution: These items have been resolved based on actions taken via PI-33.

Public Input No. 9-NFPA 915-2024 [Section No. A.1.1.1]

A.1.1.1

Methods for conducting remote inspections and tests can range from handheld devices to other means, including, but not limited to, unmanned aircraft systems (drones), to achieve the stated objectives of the authority having jurisdiction. Requirements for implementation of the procedures, methods, and documentation required by this standard are to be developed by the authority having jurisdiction to best respond to their specific needs. Inspections and tests of buildings, structures, systems, and premises, including underground spaces and aerial areas, can include electrical, HVAC, and fire protection, among other disciplines.

Tests can be either observed remotely (the same as an inspection) while they are happening or recorded for review by the authority having jurisdiction.

Automated inspections and tests are permitted by many of ~~the installation~~ the standards for fire protection systems, including NFPA 13, NFPA 14, NFPA 20, NFPA 25, and *NFPA 72*. If approved for use by the authority having jurisdiction, periodic inspections and tests such as those required for water-based fire protection systems, fire alarm systems, and other mechanical and electrical systems can be performed automatically and the results recorded for review.

Distance monitoring involves installing electronic devices, meters, or equipment to observe conditions in mechanical and electrical systems that can be constantly reported to a dashboard or similar display or requested on an as needed basis.

Statement of Problem and Substantiation for Public Input

: Two of the NFPA references aren't installation standards. NFPA 72 is a code, and NFPA 25 is an inspection, testing, and maintenance standard. Removing the term "installation" more accurately denotes the intent of the sentence.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 11:48:55 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-2-NFPA 915-2025
Statement: The committee agreed with the submitter. This change to the annex material pertaining to automated inspections and tests reflects that the standards referenced address more than installation requirements.

Public Input No. 15-NFPA 915-2024 [Section No. A.3.3.14]

A.3.3.14 Inspection.

An inspection is a means to determine compliance. Examples of this include conformity to a specification or design or a process to ensure expected performance. This can take many forms. The inspection should ~~match the~~ verify compliance with the approved design and installation documents, or witness a test to prove compliance with acceptance criteria. In all of these cases confirmation is required, which can either be in person by the AHJ or through the use of technologies that can provide the same result or better than an in-person inspection.

Statement of Problem and Substantiation for Public Input

The term “match” is poor legislative text. Adding these terms clarifies the intent of the standard and is better legislative text.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 14:33:15 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-8-NFPA 915-2025
Statement: The committee agreed with the submitter. Removing the term "match" and replacing with the proposed text clarifies the intent of this section, and provides the language in improved legislative text.

Public Input No. 16-NFPA 915-2024 [Section No. A.3.3.19]

A.3.3.19 Remote Inspection.

The following are examples of remote inspections:

(1) Evaluation of objects, materials, equipment, installations, or construction from a distance or off-site location

(2) Aerial inspections

(3) Off-site witnessing of fire system testing

Statement of Problem and Substantiation for Public Input

NFPA 915 applies to all types of inspections, including the inspection of equipment and installations. Adding these terms clarifies the intent of the standard.

Submitter Information Verification

Submitter Full Name: Terry Victor
Organization: Risk Suppression Partners LLC
Affiliation: On behalf of the NFPA 915 Task Group #3
Street Address:
City:
State:
Zip:
Submittal Date: Mon Dec 02 14:37:05 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-9-NFPA 915-2025
Statement: The committee agreed with the submitter, as these additions in the annex provide clarity on items that can be included within the definition for remote inspection within NFPA 915.

Public Input No. 6-NFPA 915-2024 [Section No. A.7.6.2]

A.7.6.2

NFPA standards, such as NFPA 20 and NFPA 25, contain annex guidance on connectivity and data collection for automated testing and remote monitoring ~~data formats~~ . This material should be considered when reviewing data formats.

Statement of Problem and Substantiation for Public Input

This re-wording will make it easier to locate those annex sections in NFPA 20 and 25 since the titles of the respective annex sections in those documents share similar nomenclature.

Submitter Information Verification

Submitter Full Name: Joe Scibetta
Organization: BuildingReports
Street Address:
City:
State:
Zip:
Submittal Date: Fri Nov 22 10:28:09 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: FR-13-NFPA 915-2025
Statement: The committee agreed with the submitter to provide this change. As noted in the submitter's PI, this change correlates to annex sections in NFPA 20 and 25 since the titles of the respective annex sections in those documents share similar nomenclature.

Public Input No. 7-NFPA 915-2024 [Section No. A.8.2]

A.8.2

Where required by governing laws, codes, standards, or other parts of this standard, cybersecurity should be provided for equipment, software, firmware, tools, installation methods, physical security of and access to equipment, data pathways, testing, and maintenance.

Cybersecurity is not required for every system or application; it is only required when authorities or regulations mandate that cybersecurity be incorporated into the system(s). Generally, there are greater cybersecurity concerns where systems are connected to external networks.

Cybersecurity ~~recommendations~~ requirements are contained in ~~Annex J~~ Chapter 11 of *NFPA 72*. For additional reference, see the NFPA Fire Protection Research Foundation report, *Cybersecurity for Fire Protection Systems*.

Statement of Problem and Substantiation for Public Input

As of the 2025 edition of NFPA 72, the recommendations in Annex J are now requirements in Chapter 11.

Submitter Information Verification

Submitter Full Name: Joe Scibetta
Organization: BuildingReports
Street Address:
City:
State:
Zip:
Submittal Date: Fri Nov 22 10:36:03 EST 2024
Committee: REI-AAA

Committee Statement

Resolution: These items have been resolved based on actions taken via PI-33.