NFPA®

1221

Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems

2016

NFPA®

See ALERT

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA STANDARDS

NFPA® codes, standards, recommended practices, and guides ("NFPA Standards"), of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in NFPA Standards.

The NFPA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on NFPA Standards. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Standards available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of NFPA Standards. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

ALERT: THIS STANDARD HAS BEEN MODIFIED BY A TIA OR ERRATA

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that NFPA Standards may be amended from time to time through the issuance of a Tentative Interim Amendment (TIA) or corrected by Errata. An official NFPA Standard at any point in time consists of the current edition of the document together with any TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, go to www.nfpa.org/docinfo to choose from the list of NFPA Standards or use the search feature to select the NFPA Standard number (e.g., NFPA 13). The document information page provides up-to-date document-specific information as well as postings of all existing TIAs and Errata. It also includes the option to register for an "Alert" feature to receive an automatic email notification when new updates and other information are posted regarding the document.

ISBN: 978-145591184-4 (Print)
ISBN: 978-145591221-6 (PDF)

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Standards

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments or corrected by Errata. An official NFPA Standard at any point in time consists of the current edition of the document together with any Tentative Interim Amendments and any Errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of Tentative Interim Amendments or corrected through the issuance of Errata, consult appropriate NFPA publications such as the National Fire Codes® Subscription Service, visit the NFPA website at www.nfpa.org, or contact the NFPA at the address listed below.

Interpretations of NFPA Standards

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing the Development of NFPA Standards shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights referenced in, related to, or asserted in connection with an NFPA Standard. The users of NFPA Standards bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Standards.

NFPA adheres to the policy of the American National Standards Institute (ANSI) regarding the inclusion of patents in American National Standards ("the ANSI Patent Policy"), and hereby gives the following notice pursuant to that policy:

NOTICE: The user's attention is called to the possibility that compliance with an NFPA Standard may require use of an invention covered by patent rights. NFPA takes no position as to the validity of any such patent rights or as to whether such patent rights constitute or include essential patent claims under the ANSI Patent Policy. If, in connection with the ANSI Patent Policy, a patent holder has filed a statement of willingness to grant licenses under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, copies of such filed statements can be obtained, on request, from NFPA. For further information, contact the NFPA at the address listed below.

Law and Regulations

Users of NFPA Standards should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

NFPA Standards are copyrighted. They are made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making these documents available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to these documents.

Use of NFPA Standards for regulatory purposes should be accomplished through adoption by reference. The term "adoption by reference" means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA Standards, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Standards and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA standards during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101; email: stds_admin@nfpa.org.

For more information about NFPA, visit the NFPA website at www.nfpa.org. All NFPA codes and standards can be viewed at no cost at www.nfpa.org/docinfo.

NFPA® 1221

Standard for the

Installation, Maintenance, and Use of Emergency Services Communications Systems

2016 Edition

This edition of NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, was prepared by the Technical Committee on Public Emergency Service Communication. It was issued by the Standards Council on May 26, 2015, with an effective date of June 15, 2015, and supersedes all previous editions.

This document has been amended by one or more Tentative Interim Amendments (TIAs) and/or Errata. See "Codes & Standards" at www.nfpa.org for more information.

This edition of NFPA 1221 was approved as an American National Standard on June 15, 2015.

Origin and Development of NFPA 1221

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems,* dates back to 1898. Originally, it was part of a general standard on signaling systems, but the material on municipal fire alarm systems was separated from the general standard in 1911. This standard has been revised and reissued in editions dated 1904, 1911, 1926, 1934, 1940, 1941, 1946, 1948, 1949, 1950, 1952, 1954, 1955, 1956, 1962, 1963, 1964, 1967, 1973, 1975, 1978, 1980, 1984, 1988, 1991, 1994, 1999, 2002, and 2007.

The 1999 edition of NFPA 1221 was a result of very hard work by committee members, especially the previous chairman, Evan E. Stauffer, Jr. The goal of the committee was to completely rewrite the standard to reflect an emergence of joint communications centers, the increase in technology-based information systems that assist users in both the communications center and the field of operations, and the role communications play in emergency scene operations within the Incident Command System. To reflect the fact that NFPA 1221 is applicable to all emergency responders, not just the fire service, the title was changed from *Standard for the Installation, Maintenance, and Use of Public Fire Service Communication Systems* to *Standard for the Installation, Maintenance, and Use of Emergency Communication Systems.*

The 2002 edition of this document continued to enhance the capabilities of personnel assigned to communications centers as well as the interoperability of systems. Because technology is continually changing, committee members began to assess potential changes to the next edition of this standard. It was recognized that it is incumbent on both users and enforcers of this standard to understand the impact of the standard, both in the area of service delivery and on the safety of those emergency response personnel delivering services.

Competing interests and priorities in a communications center need to be addressed by the authority having jurisdiction to develop standard operating procedures on how calls for service are processed, dispatched, and tracked. The mission of the communications center should be to serve as a conduit between those requesting services and those providing the services. This standard with its current revisions provides the requirements to accomplish that mission.

The 2007 edition of NFPA 1221 was a complete revision incorporating the requirements of the *Manual of Style for NFPA Technical Committee Documents.* As part of the 2007 revision, the committee restructured several chapters and added a new chapter on data network security and several new sections. Subsequently, all chapters were renumbered to accommodate those changes. The entire document was reviewed and editorially updated to clarify requirements and ambiguous language. In addition, the title of the document was again changed, to *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems.*

The 2010 edition of NFPA 1221 added requirements to include an emergency fire plan to safeguard personnel and minimize disruption of vital public safety communications. New communication centers and the buildings in which they are located were now required to be protected from the approach of unauthorized vehicles or to have the building designed to be blast resistant. The committee also addressed the need for reliable in-building tactical emergency communications by developing performance requirements for two-way radio communication enhancement systems.

The 2013 edition of NFPA 1221 added a section on retroactivity that allowed the authority having jurisdiction to require the application of any provision of the document. The committee also addressed an important alarm processing issue in the 2013 edition. NFPA staff had been receiving frequent calls from emergency services about alarm processing times that exceeded the time allotted in the standard. These alarm calls required more time to process because dispatchers and call takers were required to gather additional information before dispatching the appropriate resources. The committee addressed the issue by including six categories of calls that require additional time to process within the standard.

The 2016 edition of NFPA 1221 includes requirements regarding two-way radio communications enhancement systems and pathway survivability from *NFPA 72, National Fire Alarm and Signaling Code,* that the committees of both standards felt are more appropriate to NFPA 1221. Additionally, call processing times have been revisited, resulting in a change to the emergency call processing timeline in the alarm processing section to include verification. The change addresses improvements to the technologies whereby telecommunicators receive emergency calls and the time it takes to verify the location of the emergency prior to processing. A requirement that two telecommunicators be on duty in the communications center at all times is another change made to the 2016 edition. Two additional categories of calls requiring additional time to process at the public safety answering point (PSAP) also have been added.

Technical Committee on Public Emergency Service Communication

Stephen Verbil, *Chair*
Connecticut Department of Emergency Services & Public Protection, CT [E]

Douglas M. Aiken, Lakes Region Mutual Fire Aid, NH [U]
Rep. International Municipal Signal Association

William Ambrefe, City of Beverly, MA [E]

Charles M. Berdan, Smokeater Consulting, CA [SE]

Patrick J. Conroy, Aon Fire Protection Engineering, WA [I]

Thomas Dibernardo, Sunrise Fire Rescue, FL [E]

Jay Dornseif, III, Priority Dispatch Corporation, UT [SE]

Jerry Eisner, RedSky Technologies Inc., IL [IM]

Debbie Fox, Louisville KY EMA Metrosafe, KY [U]

Mark Krizik, Motorola, Inc., IL [M]

Steve Leese, APCO International, FL [U]
Rep. Association of Public-Safety Communications Officials International Inc.

Scott Lheureux, Purvis Systems Inc., RI [M]

Kenneth J. Link, Jr., U.S. Department of Homeland Security, NJ [SE]

Christopher H. Lombard, Seattle Fire Department, WA [U]

Nathan D. McClure, III, AECOM Building Engineering, VA [SE]

Carolina Y. Milan, Vandenberg AFB Emergency Communication Center, CA [U]

Thomas J. Parrish, Telgian Corporation, MI [SE]

Toivo Sari, Cypress Creek Emergency Medical Services, TX [U]

Keith D. Simpkins, County of Chester, PA [U]

Evan E. Stauffer, Jr., Upper Chichester, PA [SE]

Rex Strickland, III, Fairfax County Fire & Rescue Department, VA [L]
Rep. International Association of Fire Fighters

Ty Wooten, National Emergency Number Association, VA [U]
Rep. National Emergency Number Association

Alternates

Frank J. Kiernan, City of Meriden, CT [U]
(Alt. to S. Leese)

Jeffrey G. Knight, City of Newton Fire Department, MA [U]
(Alt. to D. M. Aiken)

Robert W. McMullen, National Emergency Number Association, VA [U]
(Alt. to T. Wooten)

Benjamin Mellon, Seattle Fire Department, WA [U]
(Alt. to C. H. Lombard)

Curt Floyd, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents relating to the operation, installation, and maintenance of public emergency services communications systems.

Contents

NFPA 1221

Standard for the

Installation, Maintenance, and Use of Emergency Services Communications Systems

2016 Edition

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

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

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

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex F. Extracted text may be edited for consistency and style and may include the revision of internal paragraph references and other references as appropriate. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

Information on referenced publications can be found in Chapter 2 and Annex F.

Chapter 1 Administration

1.1 Scope.

1.1.1 This standard shall cover the installation, performance, operation, and maintenance of public emergency services communications systems and facilities.

1.1.2 This standard shall not be used as a design specification manual or an instruction manual.

1.2 Purpose. The purpose of this standard shall be as follows:

(1) To specify operations, facilities, and communications systems that receive alarms from the public
(2) To provide requirements for the retransmission of such alarms to the appropriate emergency response agencies
(3) To provide requirements for dispatching of appropriate emergency response personnel
(4) To establish the required levels of performance and quality of installations of emergency services communications systems

1.2.1 Public fire alarm systems and fire alarm systems on private premises from which signals are received directly or indirectly by the communications center shall be in accordance with *NFPA 72*.

1.2.2 Emergency reporting systems that are not covered by this standard shall be in accordance with *NFPA 72*.

1.3 Application. This standard shall apply to communications systems that include, but are not limited to, dispatching systems, telephone systems, public reporting systems, and one-way and two-way radio systems that provide the following functions:

(1) Communication between the public and emergency response agencies
(2) Communication within the emergency response agency under emergency and nonemergency conditions
(3) Communication among emergency response agencies

1.4 Retroactivity.

1.4.1 Unless otherwise noted, it is not intended that the provisions of this document be applied to facilities, equipment, structures, or installations that were existing or approved for construction or installation prior to the effective date of the document.

1.4.2 In those cases where it is determined that the existing situation involves a distinct hazard to life or property, the authority having jurisdiction shall be permitted to require retroactive application of any provisions of this document.

1.4.3 The portions of this standard that shall be applied retroactively are listed in Table 1.4, Retroactivity.

1.5 Equivalency. Nothing in this standard is intended to prevent the use of systems, methods, or devices of equivalent or superior quality, strength, fire resistance, effectiveness, durability, and safety over those prescribed by this standard.

1.5.1 Technical documentation shall be submitted to the authority having jurisdiction to demonstrate equivalency.

Table 1.4 Retroactivity

Chapter	Retroactive
1	N/A
2	N/A
3	Yes
4	4.1, 4.5.1, 4.5.2, 4.5.5–4.5.7
5	No
6	No
7	Yes
8	Yes
9	No
10	No
11	Yes
12	Yes
13	Yes
14	No

1.5.2 The system, method, or device shall be approved for the intended purpose by the authority having jurisdiction.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document.

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

NFPA 1, *Fire Code,* 2015 edition.

NFPA 10, *Standard for Portable Fire Extinguishers,* 2013 edition.

NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2016 edition.

NFPA 37, *Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines,* 2015 edition.

NFPA 54, *National Fuel Gas Code,* 2015 edition.

NFPA 58, *Liquefied Petroleum Gas Code,* 2014 edition.

NFPA 70®, National Electrical Code®, 2014 edition.

NFPA 72®, National Fire Alarm and Signaling Code, 2016 edition.

NFPA 75, *Standard for the Fire Protection of Information Technology Equipment,* 2013 edition.

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems,* 2015 edition.

NFPA 90B, *Standard for the Installation of Warm Air Heating and Air-Conditioning Systems,* 2015 edition.

NFPA *101®, Life Safety Code®,* 2015 edition.

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2016 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2016 edition.

NFPA 220, *Standard on Types of Building Construction,* 2015 edition.

NFPA 731, *Standard for the Installation of Electronic Premises Security Systems,* 2015 edition.

NFPA 780, *Standard for the Installation of Lightning Protection Systems,* 2014 edition.

NFPA 1061, *Standard for Professional Qualifications for Public Safety Telecommunicator,* 2014 edition.

NFPA 1561, *Standard on Emergency Services Incident Management System,* 2014 edition.

NFPA 1901, *Standard for Automotive Fire Apparatus,* 2016 edition.

NFPA 5000®, Building Construction and Safety Code®, 2015 edition.

2.3 Other Publications.

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

ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials,*2014.

2.3.2 IEEE Publications. IEEE, Three Park Avenue, 17th Floor, New York, NY 10016-5997.

IEEE C2, *National Electrical Safety Code,* 1997.

2.3.3 IESNA Publications. Illuminating Engineering Society of North America, 120 Wall Street, Floor 17, New York, NY 10005.

HB-9-00, *Lighting Handbook*, 9th edition, 2009.

2.3.4 IMSA Publications. International Municipal Signal Association, P.O. Box 539, 165 East Union Street, Newark, NY 14513-0539.

Official IMSA Wire and Cable Specifications Manual, 2012.

2.3.5 TIA/EIA Publications. Telecommunications Industry Association/Electronic Industries Alliance, 2500 Wilson Boulevard, Arlington, VA 22201.

ANSI/TIA-102.BAAA, *FDMA Common Air Interface*, 1998.

TIA-102.BBAB, *Project 25 Phase 2 Two-Slot Time Division Multiple Access Physical Layer Protocol Specification.*

TIA-102.BBAC, *Project 25 Phase 2 Two-Slot TDMA Media Access Control Layer Description.*

TIA-603-D, *Land Mobile FM or PM Communications Equipment Measurement and Performance Standards*, 2010.

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

ANSI/UL 752, *Standard for Bullet-Resistant Equipment,* 2005, Revised 2010.

2.3.7 Other Publications.

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

2.4 References for Extracts in Mandatory Sections.

NFPA 70®, National Electrical Code®, 2014 edition.

NFPA 72®, National Fire Alarm and Signaling Code, 2016 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2016 edition.

NFPA 1000, *Standard for Fire Service Professional Qualifications Accreditation and Certification Systems,* 2011 edition.

NFPA 1021, *Standard for Fire Officer Professional Qualifications,* 2014 edition.

NFPA 1061, *Standard for Professional Qualifications for Public Safety Telecommunicator,* 2014 edition.

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, shall be the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1* Approved. Acceptable to the authority having jurisdiction.

3.2.2* Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements

of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Labeled. Equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

3.2.4* Listed. Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction and concerned with evaluation of products or services, that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states that either the equipment, material, or service meets appropriate designated standards or has been tested and found suitable for a specified purpose.

3.2.5 Shall. Indicates a mandatory requirement.

3.2.6 Should. Indicates a recommendation or that which is advised but not required.

3.2.7 Standard. An NFPA Standard, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and that is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA Manuals of Style. When used in a generic sense, such as in the phrase "standards development process" or "standards development activities," the term "standards" includes all NFPA Standards, including Codes, Standards, Recommended Practices, and Guides.

3.3 General Definitions.

3.3.1* Alarm. A signal or message from a person or device indicating the existence of an emergency or other situation that requires action by an emergency response agency.

3.3.1.1* ***Alarm Data.*** Digital information related to an alarm that contains the physical location of the alarm, callback number of the reporting party/system, and other explanatory information.

3.3.2 Alert Data Message (ADM). An analog or digital signal containing instructions for how a public alerting system alerting appliance (PASAA) is to deliver and, if capable, to acknowledge a public alert.

3.3.3 Alphanumeric Devices. Used as a part of a radio alerting system, paging receivers that provide an audible alert and a text message to the user and that do not have the ability to provide voice messages.

3.3.4 Alternate Communications Center. A designated communications center capable of assuming the functions normally performed at the primary communications center.

3.3.5 Antenna. A device connected to a radio receiver, transmitter, or transceiver that radiates the transmitted signal, receives a signal, or both.

3.3.6* Automatic Location Identification (ALI). A series of data elements that informs the recipient of the location of the alarm.

3.3.7* Automatic Number Identification (ANI). A series of alphanumeric characters that informs the recipient of the source of the alarm.

3.3.8 Band. A range of frequencies between two defined limits.

3.3.9 Base Station. A stationary radio transceiver with an ac or dc power supply or power supply module.

3.3.10 Box Circuit. A circuit that is connected to boxes that transmit an alarm to the communications center.

3.3.11 Cable. A factory assembly of two or more conductors having an overall covering. [**70**, 800.2]

3.3.12 CAD Terminal. An electronic device that combines a keyboard and a display screen to allow exchange of information between a telecommunicator and one or more computers in the system/network.

3.3.13 Call Detail Recording (CDR). A system that provides a record of each call, including automatic number identification (ANI), trunk number, and answering attendant number; and the time of seizure, answer, and disconnect/transfer.

3.3.14* Call Server. A system of electrical, mechanical, and computer components the function of which is to process incoming and outgoing telephone calls.

3.3.15 Certification. An authoritative attestment; specifically, the issuance of a document that states that an individual has demonstrated the knowledge and skills necessary to function in a particular fire service professional field. [**1000**, 2011]

3.3.16 Channel Access Time. The time lapse from activation of a radio transmitter's push-to-talk (PTT) switch to an acknowledgment from the system and commencement of transmission.

3.3.17* Circuit. The conductor or radio channel and associated equipment that are used to perform a specific function in connection with an alarm system.

3.3.18 Coded Receivers. Used as a part of a radio alerting system, paging receivers that respond only to messages directed to the specific unit or to units in an assigned group.

3.3.19 Common Battery. The battery used to power recorders, transmitters, relays, other communications center equipment, and alternate communications center equipment.

3.3.20* Communications Center. A building or portion of a building that is specifically configured for the primary purpose of providing emergency communications services or public safety answering point (PSAP) services to one or more public safety agencies under the authority or authorities having jurisdiction.

3.3.21* Communications Officer. The individual responsible for development of plans to make the most effective use of incident-assigned communications equipment and facilities, installation and testing of all communications equipment, supervision and operation of the incident communications center, distribution and recovery of equipment assigned to incident personnel, and maintenance and on-site repair of communications equipment.

3.3.22 Communications System. A combination of links or networks that serves a general function such as a system made up of command, tactical, logistical, and administrative networks.

3.3.23* Comprehensive Emergency Management Plan (CEMP). A disaster plan that conforms to guidelines established by the authority having jurisdiction and is designed to address natural, technological, and man-made disasters.

3.3.24* Computer-Aided Dispatch (CAD). A combination of hardware and software that provides data entry, makes resource recommendations, and notifies and tracks those resources before, during, and after alarms, preserving records of those alarms and status changes for later analysis.

3.3.25 Control Console. A wall-mounted or desktop panel or cabinet containing controls to operate communications equipment.

3.3.26 Conventional Radio. A radio system in which automatic computer control of channel assignments is not required or used, system-managed queuing of calls is not provided, and channels are selected manually by the users.

3.3.27 Coordinated Universal Time. A coordinated time scale, maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals.

3.3.28 Critical Operations Power Systems (COPS). Power systems for facilities or parts of facilities that require continuous operation for the reasons of public safety, emergency management, national security, or business continuity. [**70:**708.2]

3.3.29 Customer Premise Equipment (CPE). Equipment for the reception and origination of telephone calls located at a PSAP.

3.3.30* Delivered Audio Quality (DAQ). A measure of speech intelligibility of land mobile radios.

3.3.31 Denial-of-Service Attack. An attack on a computer system or network with the objective of causing a loss of service to some or all users, by saturating the system or network with useless traffic, making it impossible for legitimate users of the system to use the facility.

3.3.32 Digital Radio System. A radio system that uses a binary representation of audio from one radio to another.

3.3.33 Direct Exterior Window. A window in a communications center that faces an area that is not part of the secure area assigned solely to the communications center or that is accessible to the public.

3.3.34* Dispatch Circuit. A circuit over which a signal is transmitted from the communications center to an emergency response facility (ERF) or emergency response units (ERUs) to notify ERUs to respond to an emergency.

3.3.35 Dispatcher. See 3.3.102, Telecommunicator.

3.3.36 Dispatching. See 3.3.41, Emergency Alarm Processing/Dispatching.

3.3.37 Display Screen. An electronic device that is capable of displaying text, video, and graphics.

3.3.38 Donor Antenna. Antennas used with two-way radio communications enhancement systems that provide the connection between the wide-area communications system of interest and the in-building system.

3.3.39 Donor Site. The specific wide-area communications site from which the donor antenna acquires services.

3.3.40* Emergency. A condition that is endangering or is believed to be endangering life or property; an event that requires the urgent response of an emergency response agency.

3.3.41* Emergency Alarm Processing/Dispatching. A process by which an alarm answered at the communications center creates a call for service and is transmitted to emergency response facilities (ERFs) or to emergency response units (ERUs) in the field.

3.3.42 Emergency Dispatch Protocol. A standard sequence of questions used by telecommunicators that provides post-dispatch or pre-arrival instructions to callers.

3.3.43* Emergency Response Agency (ERA). Organizations providing law enforcement, emergency medical, fire, rescue, communications, and related support services.

3.3.44* Emergency Response Facility (ERF). A structure or a portion of a structure that houses emergency response agency equipment or personnel for response to alarms.

3.3.45 Emergency Response Unit (ERU). Personnel who respond to fire, medical, law enforcement, and other emergency situations for the preservation of life and safety.

3.3.46 Enhanced 9-1-1. Emergency telephone service that provides selective routing and both automatic number identification (ANI) and automatic location identification (ALI) of the calling party.

3.3.47 Incident Management System. A plan that defines the roles and responsibilities to be assumed by personnel and the operating procedures to be used in the management and direction of emergency operations.

3.3.48 Instant Recall Recorder. A device that records voice conversations and provides a telecommunicator with a means to review such conversations in real time.

3.3.49 Intelligent Transportation System. A means of electronic communications or information processing used singly or in combination to improve the efficiency or safety of a surface transportation system.

3.3.50* IP-Enabled Device. A data-centric device that uses Internet protocol (IP) as a means of communication.

3.3.51 Leaky Feeder Cable. A radiating coaxial cable.

3.3.52 Local Circuit. A circuit that does not depend on the receipt of alarms over box circuits or the retransmission of alarms over dispatch circuits.

3.3.53 Logging Voice Recorder. A device that records voice conversations and automatically logs the time and date of such conversations; normally, a multichannel device that keeps a semipermanent record of operations.

3.3.54 Loss of Power. The reduction of available voltage at the load to below the point at which the equipment can function as designed.

3.3.55 Master Time Source. A system providing time information to connected PSAP equipment that is traceable to Coordinated Universal Time (UTC).

3.3.56 Microwave. Radio waves with frequencies of 1000 MHz and higher.

3.3.57 Mobile Unit. A two-way radio-equipped vehicle or person; also a two-way radio by itself that is associated with a vehicle or person.

3.3.58 Modem (Modulator/Demodulator Unit). A device that converts data that is compatible with data-processing equipment to a form that is compatible with transmission equipment, and vice versa.

3.3.59 Monitor. To listen to or observe message traffic without transmitting a response.

3.3.60 Monitoring for Integrity. Automatic monitoring of circuits and other system components for the existence of defects or faults that interfere with receiving or transmitting an alarm.

3.3.61 Motor-Generator. A machine that consists of a generator driven by an electric motor.

3.3.62* Multiple Line Telephone System (MLTS). A system designed to aggregate more than one incoming voice communication channel for use by more than one telephone.

3.3.63 Non-Coded Receivers. Radio receivers that respond to all messages on their communications channel and that do not have the ability to screen out selective calls.

3.3.64* Notification. The time at which an alarm is received and acknowledged at a communications center.

3.3.65 Numeric Receivers. Used as a part of a radio alerting system, paging receivers that provide an audible alert and a numeric message to the user and that do not have the ability to provide text or voice messages.

3.3.66 Operations Room. The room in the communications center where alarms are received and processed and communications with emergency response personnel are conducted.

3.3.67 P.01 GOS. A probability statement for grade of service that no more than 1 call out of 100 attempts made during the average busy hour will receive a busy signal.

3.3.68 Pager. A compact radio receiver used for providing one-way communication or limited digital/data two-way communication.

3.3.69 Path (Pathways). Any circuit, conductor, optic fiber, radio carrier, or other means connecting two or more locations. [**72,** 2016]

3.3.70 Pathway Survivability. The ability of any conductor, optic fiber, radio carrier,or other means for transmitting system information to remain operational during fire conditions. [**72,** 2016]

3.3.71 Permanent Visual Record (Recording). An immediately readable, not easily alterable print, slash, or punch record of all occurrences of status change.

3.3.72 Portable Radio. A battery-operated, hand-held transceiver.

3.3.73 Power Loss. See 3.3.54, Loss of Power.

3.3.74 Power Source. The power obtained from a utility distribution system, an engine-driven generator, or a battery.

3.3.75* Private Branch Exchange (PBX). A system designed to connect to a local exchange carrier (incumbent or competitive) to allow telephone calls to be distributed to extensions and extensions to use a set of voice communication channels to make outbound calls. A PBX also allows extension-to-extension telephone calls without connecting to the public switched telephone network.

3.3.76 Public Alarm Reporting System. A system of alarm-initiating devices, receiving equipment, and connecting circuits, other than a public telephone network, used to transmit alarms from street locations to the communications center.

3.3.77 Public Alert Signal. A signal or message delivered to a person or device indicating the existence of a situation that affects public safety.

3.3.78 Public Alerting System (PAS). A system that creates, transmits, and displays a public alert message or sounds a signal, or both, that is intended to alert the public to situations that could result in loss of life, endanger their health, or destroy property.

3.3.79 Public Alerting System Alerting Appliance (PASAA). A device that receives a signal from a public alerting system (PAS) and broadcasts an audible and visual alarm that could be in the form of text or speech.

3.3.80 Public Safety Agency/Public Safety Organization. See 3.3.43, Emergency Response Agency (ERA).

3.3.81 Public Safety Answering Point (PSAP). A facility in which 9-1-1 calls are answered.

3.3.82 Public Safety Radio Systems. A radio system provisioned, installed, and maintained for the purpose of providing wireless communication to serve the requirements of emergency response agencies.

3.3.83* Radio Channel. A band of frequencies of a width sufficient to allow its use for radio communications. [**72**, 2016]

3.3.84 Radio Control Station. A mobile or base station radio in a fixed location (often on a desktop or in a dispatcher's console) that operates on a radio frequency configuration so that it can access a land mobile radio-fixed repeater station or fixed trunking station to gain access to the communication system. A radio control station is often used in a 9-1-1 center to provide a backup means to access the public safety communications system.

3.3.85* Radio Frequency. The number of electromagnetic wave frequency cycles transmitted by a radio in 1 second.

3.3.86 Radio Licensing Authority. The government authority in a country that issues licenses for use of radio frequencies by authorized agencies and individuals.

3.3.87 Rectifier. A device without moving parts that changes alternating current to direct current.

3.3.88* Remote Communications Facility. A normally unattended facility, remote from the communications center that is used to house equipment necessary for the functioning of a communications system.

3.3.89 Repeater. A device for receiving and re-transmitting one-way or two-way communication signals.

3.3.90* Response Unit. A vehicle, equipment, or personnel identified by the AHJ for dispatch purposes.

3.3.91 RF Emitting Device. An active device that emits a radio frequency signal as part of a two-way radio communications enhancement system.

3.3.92 Security Vestibule. A compartment provided with two or more doors where the intended purpose is to prevent continuous and unobstructed passage by allowing the release of only one door at a time.

3.3.93 Simplex Radio Channel. A radio channel using a single frequency that, at any one time, allows either transmission or reception, but not both, by a particular radio.

3.3.94* Standard Operating Procedures (SOPs). Written organizational directives that establish or prescribe specific operational or administrative methods that are to be followed routinely for the performance of designated operations or actions.

3.3.95 Stored Emergency Power Supply System (SEPSS). A system consisting of a UPS, a rectifier plant, or a motor generator powered by a stored electrical energy source; a transfer switch designed to monitor preferred and alternate load power source and provide desired switching of the load; and all necessary control equipment to make the system functional. [**111**, 2016]

3.3.96 Subscriber. A mobile radio, portable radio, or radio control station operated by a user in a wireless communications system on a radio frequency configuration so that it can access a land mobile radio fixed repeater station or fixed trunking base station to gain access to the communication system.

3.3.97 Supervising Station. A commerical or proprietary facility that receives alarm and supervisory signals where personnel are in attendance at all times to receive and process alarms and signals and to notify the communications center or other appropriate entity.

3.3.98 Supervisor. An individual responsible for overseeing the performance or activity of other members. [**1021**, 2014]

3.3.99 Tactical Interoperable Communications Plan (TICP). A document used to clearly define the breadth and scope of interoperable assets available in the area and how those assets are shared and how their use is prioritized, and the steps individual agencies should follow to request, activate, use, and deactivate each asset.

3.3.100 Talkgroup. A group of radios addressed as a single entity by the system and functionally equivalent to a conventional repeater channel.

3.3.101 TDD/TTY. A device that is used in conjunction with a telephone to communicate with persons who are deaf, who are hard of hearing, or who have speech impairments, by typing and reading text.

3.3.102 Telecommunicator. An individual whose primary responsibility is to receive, process, or disseminate information of a public safety nature via telecommunication devices. [**1061**, 2014]

3.3.103 Tie Circuit. A circuit that connects a communications center with an alternate communications center or with a public safety answering point (PSAP).

3.3.104 Transceiver. A combined transmitter and receiver radio unit.

3.3.105 Trouble Signal. A signal initiated by a dispatch system or device indicative of a fault in a monitored circuit or component.

3.3.106 Trunked Radio. A radio system that uses computer control to automatically assign channels from an available pool of channels to users and groups of users.

3.3.107* Two-Way Alphanumeric Devices. Used as a part of a radio -alerting system, paging transceivers that provide an audible alert and a text message to the user and that have the ability to acknowledge messages received back to the control point.

3.3.108 Two-Way Radio Communications Enhancement System. A combination of components, RF emitting devices, antennas, cables, power supplies, control circuitry, and programming installed at a specific location to improve wireless communication at that location.

3.3.109* Uninterruptible Power Supply (UPS). A system consisting of a stored energy source, designed to continuously provide a clean, conditioned sinusoidal wave of power under normal conditions and for a finite period of time upon loss of the primary power source. [**111,** 2016]

3.3.110* Voice Communication Channel. A single circuit for communication by spoken word that is distinct from other circuits for communications.

3.3.111 Wired Circuit. A metallic or fiber-optic circuit, leased to or owned by a jurisdiction, that is dedicated to a specific alarm or communication system under the control of that jurisdiction.

Chapter 4 Communications Centers

4.1 General.

4.1.1* Communications centers and alternate communications centers shall comply with Chapter 4.

4.1.2 When provided, remote communications facilities shall comply with Section 4.10.

4.1.3 Communications equipment shall be kept in working order at all times.

4.1.4 Each center shall be provided with a designated primary means of communication that shall be compatible with the designated primary means of communication provided at the Emergency Response Facilities (ERFs).

4.1.4.1 Each center shall be provided with an alternate means of communication that is compatible with the alternate means of communication provided at the ERFs. The alternate means shall be readily available to the telecommunicator in the event of failure of the primary communications system.

4.1.5* Each jurisdiction shall maintain an alternate communications center that meets the criteria in 4.1.5.1 and 4.1.5.2.

4.1.5.1 The alternate communications center shall be capable, when staffed, of performing the emergency functions performed at the primary communications center.

4.1.5.2* The alternate communications center shall be separated geographically from the primary communications center at a distance that ensures the survivability of the alternate center.

4.1.5.3 Each jurisdiction shall develop a formal plan to maintain and operate the alternate communications center.

4.1.5.3.1 The plan shall include the ability to reroute incoming alarm traffic to the alternate center and to process and dispatch alarms at that center.

4.1.5.3.2* The plan shall be included in the Comprehensive Emergency Management Plan (CEMP).

4.1.5.4* When operations are from the alternate communications center, receipt, transfer, processing, and dispatching of alarms in accordance with the requirements of this standard shall not be dependent on the functioning of any equipment at the primary communications center.

4.1.6* The communications center shall be capable of continuous operation long enough to enable the transfer of operations to the alternate communications center in the event of fire or other emergency in the communications center or in the building that houses the communications center.

4.1.7 Systems that are essential to the operation of the communications center shall be designed to accommodate peak workloads as determined by the authority having jurisdiction (AHJ).

4.1.8* Communications centers shall be designed to accommodate the staffing level necessary to operate the center as required by Chapter 7.

4.1.9 The design of the communications center shall be based on number of personnel needed to handle peak workloads as determined by the AHJ.

4.2 Exposure Hazards.

4.2.1 Where the building that houses a communications center is adjacent to another structure, the exposed walls shall be protected in compliance with *NFPA 5000* or in compliance with the building code legally in effect, whichever is more restrictive.

4.2.2* When the building that houses a communications center is located within 150 ft (46 m) of the potential collapse zone of a taller structure, the roof shall be designed to resist damage from collapse of the exposing structure.

4.2.3* The lowest floor elevation of the communications center shall be above the 100-year flood plain established by the Federal Emergency Management Agency.

4.3 Construction.

4.3.1 Communications centers shall be located in buildings of Type I or Type II construction as defined by NFPA 220.

4.3.2 Buildings that house communications centers shall have Class A roof coverings.

4.3.3 Communications centers shall be separated from other portions of buildings occupied for purposes other than emergency communications by fire barriers having a fire resistance rating of 2 hours.

4.3.4 Fire barriers shall comply with NFPA *101* Section 8.2.

4.3.5* Communications centers shall not be located below grade unless the elevation of the lowest floor in the facility is above the 500-year flood plan. Communications centers located below grade shall comply with 11.7.3 of NFPA *101* and be specifically designed for the location.

4.3.6 The exposed surfaces of interior walls and ceilings shall have a flame spread index of 25 or less and a smoke development index of 50 or less when tested in accordance with ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials*.

4.3.7 Interior floor finish shall comply with the requirements of NFPA *101* interior floor finish testing and classification and shall be Class I as established by NFPA *101* or shall have a minimum critical radiant flux of 0.1 W/cm^2.

4.3.8 The operations room shall be equipped with a toilet facility and a lunch area that are directly accessible to the telecommunicators within the secured area as required by Section 4.6.

4.3.8.1* Communications centers shall be provided with backup facilities for sanitation and drinking water to provide for the health and safety of employees during extended periods of failure of public water or sewer systems.

4.3.9 The communications center or that portion of a building to be utilized as a communications center shall be protected against seismic damage in accordance with *NFPA 5000* or the building code legally in effect.

4.4 Climate Control.

4.4.1 Heating, ventilating, and air-conditioning (HVAC) systems shall be provided in accordance with NFPA 90A and NFPA 90B.

4.4.1.1 HVAC systems shall be designed to maintain temperature and relative humidity within limits specified by the manufacturers of the equipment critical to the operation of the communications center as determined by the AHJ.

4.4.1.1.1* Separate temperature and humidity controls shall be provided for each equipment room, for the operations room, for office areas, and for other spaces designated by the AHJ.

4.4.1.2* HVAC systems shall be independent systems that serve only the communications center.

4.4.1.3* HVAC system intakes for fresh air shall be arranged to minimize smoke intake from a fire inside or outside the building and to resist intentional introduction of irritating, noxious, toxic, or poisonous substances into the HVAC system.

4.4.1.4 Emergency controls shall be provided in the operations room to permit closing of outside air intakes.

4.4.1.5* Backup HVAC systems shall be provided for the operations room and other spaces housing electronic equipment determined by the AHJ to be essential to the operation of the communications center.

4.4.1.6 Backup or redundant HVAC units shall be capable of receiving power from all power sources required by Section 4.7.

4.4.1.7* HVAC systems shall be designed so that the communications center is capable of uninterrupted operation with the largest single HVAC unit or component out of service.

4.4.1.8* Primary and backup HVAC systems shall be capable of operating from the normal power source required by 4.7.2 and the alternate power source required by 4.7.3.

4.4.1.9* Primary and backup/redundant HVAC units shall be located to prevent tampering, vehicle impact, or introduction of hazardous/noxious chemicals or odors.

4.4.2 Penetrations into the communications center shall be limited to those necessary for the operation of the center.

4.5 Fire Protection.

4.5.1 The communications center shall be provided with fire extinguishers that meet the requirements of NFPA 10.

4.5.2 The communications center and spaces adjoining the communications center shall be provided with an automatic fire detection, alarm, and notification system in accordance with *NFPA 72*.

4.5.2.1 The alarm system shall be monitored in the operations room.

4.5.2.2 Operation of notification appliances shall not interfere with communications operations.

4.5.3 The building that houses the communications center shall be protected throughout by an approved, supervised automatic sprinkler system that complies with NFPA 13.

4.5.4 Supervision shall be in accordance with 9.7.2 of NFPA *101*.

4.5.5 Electronic computer and data processing equipment shall be protected in accordance with NFPA 75.

4.5.6* Emergency Fire Plan. There shall be a management-approved, written, dated, and annually tested emergency fire plan that is part of the CEMP.

4.5.7* Damage Control Plan. There shall be a management-approved, written, dated, and annually tested damage control plan that is part of the CEMP.

4.5.8* Each jurisdiction shall develop a tactical interoperable communications plan (TICP) utilizing TIA-603-D, *Land Mobile FM or PM Communication Equipment Measurement and Performance Standards*, or a similar reference.

4.5.9 The TICP shall be included in the comprehensive emergency management plan (CEMP).

4.6 Security.

4.6.1 The communications center and other buildings that house essential operating equipment shall be protected against damage from vandalism, terrorism, and civil disturbances.

4.6.2 Entry to the communications center and other buildings and structures that contain equipment essential to the operation of the communications systems shall be restricted to authorized persons.

4.6.2.1 Potential points for unauthorized entry as determined by the AHJ shall be protected by an electronic intrusion detection system.

4.6.2.2 The intrusion detection system shall be annunciated in the operations room and at another location designated by the AHJ.

4.6.3* Entryways to the communications center shall be protected by a security vestibule.

4.6.3.1 Door openings shall be protected by listed, self-closing fire doors that have a fire resistance rating of not less than 1 hour.

4.6.3.2 Door openings shall be protected by listed, self-closing doors that are rated for bullet resistance to Level 4 as defined in ANSI/UL 752, *Standard for Bullet-Resistant Equipment*.

4.6.4 Where a communications center has windows, the requirements of 4.6.4.1 through 4.6.4.5 shall apply.

4.6.4.1 Window sills on all direct exterior windows shall be a minimum of 4 ft (1.2 m) above floor level or 4 ft (1.2 m) above finished grade, whichever is higher.

4.6.4.2 Direct exterior windows shall be rated for bullet resistance to Level 4 as defined in ANSI/UL 752, *Standard for Bullet-Resistant Equipment*.

4.6.4.3 Direct exterior windows that are not bullet resistant shall be permitted, provided that they face a secured area that cannot be accessed or viewed from outside the secured perimeter of the communications center.

4.6.4.4 Direct exterior windows that are required to be bullet resistant shall be configured so that they cannot be opened.

4.6.4.5* Direct exterior windows shall be arranged so that it is not possible to view the interior of the communications center from outside the secured perimeter.

4.6.5* Perimeter walls shall be designed and constructed to provide the same level of ballistic protection as that required for windows.

4.6.6 Means shall be provided to prevent unauthorized vehicles from approaching the building housing the communications center to a distance of no less than 82 ft (25 m).

4.6.7* As an alternative to 4.6.6, unauthorized vehicles shall be permitted to approach closer than 82 ft (25 m) if the building has been designed to be blast resistant, as approved by the AHJ.

4.7 Power.

4.7.1 General. Each communications center shall be provided with a critical operations power system in compliance with *NFPA 70*, Article 708.

4.7.1.1 Designated critical operations areas (DCOAs) shall include the operations room, information technology (IT) rooms, telephone rooms, electrical equipment rooms, mechanical equipment rooms, fire protection equipment rooms, sanitary facilities, and other spaces and equipment designated by the AHJ as requiring critical operations power.

4.7.1.2 At least two independent and reliable power sources shall be provided, one primary and one emergency, and each shall be of adequate capacity for operation of the communications center.

4.7.1.3 Power sources shall be monitored for integrity, with annunciation provided in the operations room.

4.7.1.4 In addition to the two power sources required by 4.7.1.2, a means for connecting a portable or vehicle-mounted generator shall be provided.

4.7.1.5* The means shall include an outdoor weatherproof power connector and a manual disconnecting means for the power connector. The disconnecting means shall connect to the center's power system on the load side of the automatic transfer switch required by 4.7.3.2.

4.7.1.6* Wiring methods for feeders, branch circuits, and any control wiring utilized in the delivery of power for the operation of the communications center shall be designed in accordance with *NFPA 70*, Article 708, Critical Operations Power Systems (COPS).

4.7.2 Primary Power Source. One of the following shall supply primary power:

(1) A feed from a commercial utility distribution system
(2) An approved engine-driven generator installation or equivalent under the control of communications center staff, designed for continuous operation, and with a person specifically trained in its operation on duty at all times
(3) An approved engine-driven generator installation or equivalent under the control of communications center staff, arranged for cogeneration with commercial light and power, and with a person specifically trained in its operation on duty at all times

4.7.3 Emergency Power Source.

4.7.3.1 The emergency power source shall consist of one or more engine-driven generators installed in accordance with *NFPA 70*, Article 701.

4.7.3.2 Upon failure of primary power, transfer to the standby emergency source shall be automatic.

4.7.4* Engine-Driven Generators.

4.7.4.1 Engine generators shall conform with the provisions of Section 4.7 and with NFPA 37.

4.7.4.2 Engine-driven generators shall conform with the provisions of NFPA 110, Type 10, Level 1, Class 75.

4.7.4.2.1 The authority having jurisdiction shall be permitted to require a higher class if necessary to comply with the CEMP.

4.7.4.3* Engine-driven generators shall be sized to supply power for the operation of all functions of the communications center and for any additional loads determined by the AHJ.

4.7.4.4 When installed indoors, engine-driven generators shall be located in a ventilated and secured area that is separated from the communications center by fire barriers having a fire resistance rating of 2 hours.

4.7.4.5 Fire barriers shall comply with NFPA *101*, Section 8.3.

4.7.4.6 When installed outdoors, engine-driven generators shall be located in a secure enclosure concealed from public view and accessible only to authorized personnel.

4.7.4.6.1 The enclosure shall be capable of resisting the entrance of precipitation at the maximum wind velocities referenced in *NFPA 5000* or in accordance with the building code legally in effect, whichever is more restrictive.

4.7.4.6.2 The enclosure shall be capable of resisting penetration by small arms fire. Doors, and windows if provided, shall be rated for bullet resistance to Level 4 as defined in ANSI/UL 752.

4.7.4.6.3 The enclosure shall be equipped with an intrusion detection system complying with NFPA 731 that shall be monitored in the operations room and at another location designated by the AHJ.

4.7.4.7 The area that houses an engine-driven generator shall not be used for storage other than spare parts or equipment related to the generator system.

4.7.4.8 Liquid fuel shall be stored in accordance with NFPA 37.

4.7.4.9 Liquid fuel for engine-driven generators shall not use a gravity-fed system.

4.7.4.10 Natural gas installations shall comply with NFPA 54.

4.7.4.11 Liquefied petroleum gas (LPG) installations shall comply with NFPA 58.

4.7.4.12* Fuel to operate an engine-driven generator for 72 hours at full load shall be available on site.

4.7.4.12.1* Diesel fuel shall be maintained and tested at regularly scheduled intervals as determined by the AHJ.

4.7.4.12.2 Fuel tank levels shall be monitored electronically in the operations room. A low-fuel supervisory alert shall be annunciated when the fuel level in a tank drops to two-thirds rated capacity. The AHJ shall be permitted to designate additional levels for tank level annunciation.

4.7.4.12.3 A dedicated fuel tank shall be provided for each engine.

4.7.4.13 Equipment essential to the operation of the generator shall be supplied with standby power from the generator.

4.7.4.14 Generators shall not use the public water supply for engine cooling.

4.7.4.15 The engine conditions requiring remote audible annunciation for Level 1 systems in NFPA 110, Table 5.6.5.2, shall be individually visually annunciated in the operations room.

4.7.4.15.1 In addition to the visual annunciation, an audible signal common to all annunciated signals shall be provided.

4.7.4.15.2 A silencing switch for the audible signal in the operations room shall be permitted on the condition that when all supervisory signals have cleared, the silencing circuit will automatically reset or the audible alert will re-sound as a reminder to restore the switch to normal.

4.7.5 Power Circuits. Power circuits, together with their associated motors, generators, rectifiers, transformers, fuses, and controlling devices, shall be installed in accordance with *NFPA 70* and the requirements of this subsection.

4.7.5.1 Primary power shall be obtained from the line side of the main service disconnect switch of the connection to a commercial utility distribution system or to the main conductors from an isolated power plant that is located on the premises.

4.7.5.2 Power shall be permitted to be obtained from the load side of the main service disconnect switch only when the building is used exclusively for housing of emergency communications facilities.

4.7.5.3 Power circuit conductors shall not be installed in conduit that is used for other circuits.

4.7.5.4 The power circuit disconnecting means shall be installed so that it is accessible only to authorized personnel.

4.7.6 Surge Arresters.

4.7.6.1* Surge arresters shall be provided in accordance with *NFPA 70*, Article 280.

4.7.6.2 Transient voltage surge suppression (TVSS) shall be provided in accordance with *NFPA 70*, Article 285, for protection of telecommunications equipment, two-way radio systems, computers, and other electronic equipment determined by the AHJ to be essential to the operation of the communications center.

4.7.7* Single-Point Facility Grounding System. Telecommunications equipment, two-way radio systems, computers, and other electronic equipment determined by the AHJ to be essential to the operation of the communications center shall be bonded to the single-point facility ground system in accordance with *NFPA 70*, Article 647.

4.7.8 Uninterruptible Power Supply (UPS) and Battery Systems.

4.7.8.1* In addition to the required engine-driven generators, an uninterruptible power supply system shall be provided. It shall comply with the requirements of 4.7.8 and *NFPA 70*.

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

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

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

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

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

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

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

4.8 Lighting.

4.8.1 General.

4.8.1.1 Artificial lighting shall be provided to enable personnel to perform their assigned duties.

4.8.1.2 Lighting intensity shall be in accordance with IESNA HB-9-00, *Lighting Handbook*.

4.8.1.3 Lighting circuits, together with their associated motors, generators, rectifiers, transformers, fuses, and controlling devices, shall be installed in accordance with *NFPA 70*.

4.8.2 Emergency Lighting.

4.8.2.1 The communications center shall be equipped with emergency lighting that illuminates automatically within 15 seconds of failure of normal lighting power.

4.8.2.1.1 Illumination levels shall be sufficient to allow all essential operations.

4.8.2.2 In addition to the requirement of 4.8.2.1, the operations room shall be equipped with redundant emergency lighting provided by individual unit equipment in accordance with *NFPA 70*, Article 700.

4.8.2.3 Individual unit equipment emergency lighting shall be provided at locations of communications equipment situated outside the operations room and at the locations of engine-driven generators.

4.9* Lightning. Buildings that house communications centers shall have lightning protection that complies with NFPA 780.

4.10 Remote Communications Facilities.

4.10.1 General.

4.10.1.1 Remote communications facilities, where provided, shall comply with 4.10.

4.10.1.2 Equipment essential to the operation of a remote communications facility shall be kept in working order at all times.

4.10.1.3 Equipment that is essential to the operation of a remote communications facility shall be designed to accommodate peak loads as determined by the AHJ.

4.10.2 Exposure Hazards.

4.10.2.1 Where the building that houses a remote communications facility is adjacent to another structure, the exposed walls shall be protected in compliance with *NFPA 5000* or in accordance with the building code legally in effect, whichever is more restrictive.

4.10.2.2* Where the building that houses a remote communications facility is located within 150 ft (46 m) of the potential collapse zone of a taller structure, the roof shall be designed to resist damage from collapse of the exposing structure.

4.10.2.3 In climates where communications towers are subject to accumulation of ice, roofs of communications equipment enclosures located within the falling ice danger zone shall be designed to resist damage from falling ice.

4.10.2.4* Remote communications facilities shall be located above the 100-year floodplain established by the Federal Emergency Management Agency.

4.10.3 Construction.

4.10.3.1 Where located inside buildings, remote communications facilities shall be located in buildings of Type I, Type II, or Type III construction as defined by NFPA 220.

4.10.3.2 Buildings that house remote communications facilities shall have Class A roof coverings.

4.10.3.3 Remote communications facilities shall be separated from other portions of buildings occupied for purposes other than emergency communications by fire barriers having a fire resistance rating of 2 hours.

4.10.3.4 Fire barriers shall comply with NFPA *101*, Section 8.2.

4.10.3.5* Remote communications facilities shall not be located below grade unless the elevation of the lowest floor in the facility is above the 500-year floodplain. Facilities located below grade shall comply with NFPA *101*, Section 11.7, "Underground and Limited Access Structures," and shall be specifically designed for the location.

4.10.3.6* The exposed surfaces of walls and ceilings inside a remote communications facility shall have a flame spread index of 25 or less and a smoke development index of 50 or less when tested in accordance with ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials*.

4.10.3.7* Interior floor finish inside a remote communications facility shall be of noncombustible material or shall comply with the requirements of NFPA *101* interior floor finish testing and classification and shall be Class I as established by NFPA *101* or shall have a minimum critical radiant flux of 0.1 W/cm^2.

4.10.3.8 The AHJ shall determine whether anti-static flooring is required for protection of sensitive electronic equipment.

4.10.3.9 Remote communications facilities shall be protected against seismic damage in accordance with *NFPA 5000* or in accordance with the building code legally in force, whichever is more restrictive.

4.10.4 Climate Control.

4.10.4.1 Heating, ventilating, and air-conditioning (HVAC) systems shall be provided in accordance with NFPA 90A or NFPA 90B.

4.10.4.1.1 HVAC systems shall be designed to maintain temperature and relative humidity within limits specified by the manufacturers of the equipment critical to the operation of the remote communications facility as determined by the AHJ.

4.10.4.1.2 HVAC systems shall be independent systems that serve only the remote communications facility.

4.10.4.1.3 HVAC system intakes for fresh air shall be arranged to minimize smoke intake from a fire inside or outside the building and to resist intentional introduction of irritating, noxious, toxic, or poisonous substances into the HVAC system.

4.10.4.1.4 Backup HVAC systems shall be provided for spaces and enclosures housing electronic equipment determined by the AHJ to be essential to the operation of the remote communications facility.

4.10.4.1.5 HVAC systems shall be designed so that the remote communications facility is capable of uninterrupted operation with the largest single HVAC unit or component out of service.

4.10.4.1.6 Upon failure of the primary HVAC system, the backup system shall come on-line automatically.

4.10.5 Fire Protection.

4.10.5.1 Remote communications facilities shall be provided with clean-agent fire extinguishers that meet the requirements of NFPA 10.

4.10.5.2 A remote communications facility and building spaces adjoining that facility shall be provided with an automatic fire detection and alarm system in accordance with *NFPA 72*.

4.10.5.2.1 The alarm systems shall be monitored in the communications center's operations room in accordance with *NFPA 72*.

4.10.5.3 Where the remote communications facility equipment is housed in a building, the building shall be protected throughout by an approved, supervised automatic sprinkler system that complies with NFPA 13.

4.10.5.4* Remote communications facilities not housed in buildings shall not be required to have automatic sprinkler protection.

4.10.5.5 Penetrations into remote communications facilities shall be limited to those necessary for the operation of the facilities.

4.10.5.6* Facilities that can be exposed to uncontrolled wildfires shall comply with NFPA 1, Chapter 17, Wildland Urban Interface.

4.10.6 Security.

4.10.6.1 Remote communications facilities shall be protected against damage from vandalism, terrorism, and civil disturbances.

4.10.6.2 Entry into remote communications facilities shall be restricted to authorized persons.

4.10.6.3 Doors furnishing access shall be protected by listed, self-closing fire doors that have a fire resistance rating of not less than 1 hour or by doors that are rated for bullet resistance to Level 4 as defined in ANSI/UL 752. The AHJ shall determine which type of door is most appropriate for each location.

4.10.6.4* A remote communications facility shall not have windows in exterior walls.

4.10.6.5* Exterior walls shall provide resistance to direct small arms fire equivalent to Level 4 as defined in ANSI/UL 752.

4.10.6.6* Means shall be provided to prevent unauthorized vehicles from approaching the structure housing the remote communications facility to a distance of no less than 82 ft (25 m).

4.10.6.7* As an alternative to 4.6.6, unauthorized vehicles shall be permitted to approach closer than 82 ft (25 m) if the building has been designed to be blast resistant, as approved by the AHJ.

4.10.6.8* An electronic intrusion detection system shall be provided. The system shall be monitored for alarm and trouble signals in the communications center or by a listed central station, as determined by the AHJ. The system shall comply with NFPA 731.

4.10.7 Power.

4.10.7.1 General. Each remote communications facility shall be provided with a critical operations power system that complies with *NFPA 70*, Article 708.

4.10.7.1.1 Primary and emergency power sources shall be provided, each of which shall be of adequate capacity for operation of the facility.

4.10.7.1.2 Power sources shall be monitored for integrity, with annunciation provided in the operations room.

4.10.7.2 Primary Power Source. One of the following shall supply normal power:

(1) A feed from a commercial utility distribution system
(2) An approved engine-driven generator installation or equivalent under the control of the AHJ, designed for continuous operation and with a person specifically trained in its operation on duty at all times
(3) An approved engine-driven generator installation or equivalent under the control of the AHJ, arranged for cogeneration with commercial light and power, and with a person specifically trained in its operation on duty at all times

4.10.7.3 Emergency Power Source.

4.10.7.3.1 The emergency power source shall consist of one or more engine-driven generators installed in accordance with *NFPA 70*, Article 708.

4.10.7.3.2 Upon failure of the normal source, transfer to the alternate source shall be automatic.

4.10.7.4 Stored Emergency Power Supply System (SEPSS). In addition to the alternate source, a stored emergency power supply system (SEPSS) shall be provided. It shall comply with the requirements of 4.7.4.

4.10.7.5* Engine-Driven Generators. Engine-driven generators shall comply with the requirements of NFPA 110 and the requirements of 4.7.4.

4.10.7.6* Power Circuits. Power circuits, together with their associated motors, generators, rectifiers, transformers, fuses, and controlling devices, shall be installed in accordance with *NFPA 70* and the requirements of 4.7.5.

4.10.7.7 Surge Arresters.

4.10.7.7.1 Surge arresters shall be provided in accordance with *NFPA 70*, Article 280.

4.10.7.7.2* Transient voltage surge suppression (TVSS) shall be provided in accordance with *NFPA 70*, Article 285, for protection of telecommunications equipment, two-way radio systems, computers, and other electronic equipment determined by the AHJ to be essential to the operation of the remote communications facility.

4.10.7.8* Single-Point Facility Grounding System. Telecommunications equipment, two-way radio systems, computers, and other electronic equipment determined by the AHJ to be essential to the operation of the remote communications facility shall be bonded to the single-point facility grounding system in accordance with *NFPA 70*, Article 647.

4.10.8 Lighting.

4.10.8.1 General.

4.10.8.1.1 Artificial lighting shall be provided to enable authorized personnel to safely perform tasks necessary for equipment maintenance.

4.10.8.1.2* Lighting intensity shall be in accordance with IESNA HB-9-00, *Lighting Handbook*.

4.10.8.1.3 External lighting shall be provided as directed by the AHJ in accordance with the security plan for each facility.

4.10.8.1.4 Lighting circuits, together with their associated motors, generators, rectifiers, transformers, fuses, and controlling devices, shall be installed in accordance with *NFPA 70*.

4.10.8.2 Emergency Lighting.

4.10.8.2.1 The remote communications facility shall be equipped with emergency lighting that illuminates automatically upon failure of normal lighting power.

4.10.8.2.1.1 Illumination levels shall be sufficient to allow troubleshooting and emergency maintenance during a power outage.

4.10.8.2.2 Individual unit equipment emergency lighting shall be provided at the locations of engine-driven generators.

4.10.9* Lightning Protection. Remote communications facilities shall have lightning protection that complies with NFPA 780.

4.10.9.1 Remote communications facilities not housed in buildings shall have lightning protection that complies with NFPA 780 and *NFPA 70*, Article 810.

Chapter 5 Communication and Signal Wiring

5.1 Circuit Construction and Arrangement.

5.1.1* Installation shall be in accordance with *NFPA 70*.

5.1.2 As an alternative to 5.1.1, installation of outdoor circuitry shall be in accordance with IEEE C2, *National Electrical Safety Code*, where approved by the AHJ.

5.1.3 Circuits shall be routed so as to avoid damage due to mechanical injury, fire, falling walls, floods, corrosive vapors, and other risks that are identified in the CEMP.

5.1.3.1 Alternate communications centers shall comply with the requirements of Chapter 4.

5.1.4 All circuits shall be routed to allow circuits to be traced.

5.1.5 Record drawings shall be provided as required by Chapter 12.

5.1.6 Circuits shall not pass over, pass under, pass through, or be attached to buildings or property that is not owned by, or under the control of, the AHJ or the entity that is responsible for maintaining the system.

5.1.7 Alarm instruments installed in buildings not under control of the AHJ shall be on separate dedicated circuits.

5.1.8 The combination of public emergency services communication and signaling (C&S) circuits in the same cable with other circuits shall comply with 5.1.8.1 and 5.1.8.2.

5.1.8.1 Other municipally controlled C&S circuits shall be permitted.

5.1.8.2 Circuits of private signaling organizations shall be permitted only by permission of the AHJ.

5.2 Circuit Conductors.

5.2.1 Wires, conductors and fiber-optic strands shall be terminated in order to prevent breaking due to vibration or stress.

5.2.2 Circuit conductors and fiber-optic cables on terminal racks shall be identified and isolated from conductors of other systems wherever possible and shall be protected from mechanical injury.

5.2.3 Fiber-optic cables containing metallic protection or strength members shall be grounded and protected in accordance with *NFPA 70*.

5.2.4 Wiring for control equipment shall be not smaller than 24 AWG.

5.2.5 Unsupported wires and wires that are subject to vibration shall be not smaller than 18 AWG.

5.2.6 The insulation and outer jacket of cables and wiring shall be flame retardant and moisture resistant.

5.2.7 Exterior metallic, fiber-optic cables and wires shall conform to International Municipal Signal Association (IMSA) specifications or an approved equivalent, except where circuit conductors or fiber-optic strands are provided by a public utility on a lease basis.

5.3 Underground Cables.

5.3.1 Underground metallic and fiber-optic communication and signal cables in ducts or of the direct burial type shall be permitted to be brought above ground only at locations approved by the AHJ.

5.3.1.1 Protection from physical damage or heat incidental to fires in adjacent buildings shall be provided.

5.3.2 Underground cables installed in ducts, vaults, and manholes shall comply with 5.3.2.1 through 5.3.2.2.

5.3.2.1 Metallic and fiber-optic communication and signal cables shall be permitted to be located only in duct systems, manholes, and vaults that contain low-voltage C&S system conductors, secondary power cables not exceeding 600 volts nominal, or both.

5.3.2.2 Where located in duct systems or manholes that contain conductors of other circuits operating in excess of 250 volts to ground, metallic and fiber-optic communication and signal cables shall be located as far as possible from such power cables and shall be separated from them by a noncombustible barrier or other means approved by the AHJ to protect the communication and signal cables from physical damage.

5.3.3 All cables that are installed in manholes, vaults, handholes, and other enclosures shall be racked and marked for identification.

5.3.4 All raceways or ducts entering buildings from underground duct systems shall be effectively sealed with an identified sealing compound or other means acceptable to the AHJ to prevent moisture or gases from the underground duct system from entering the building.

5.3.5 Cable splices, taps, and terminal connections shall be located only where accessible for maintenance and inspection and where the AHJ has determined that no potential for damage to the cable due to falling structures or building operations exists.

5.3.6 Cable joints shall be made to provide and maintain conductivity, optical continuity for fiber-optic cable insulation, and protection that is at least equal to that afforded by the cables that are joined.

5.3.7 Cable ends shall be sealed against moisture.

5.3.8 Direct-burial cable, without enclosure in ducts, shall be laid in grass plots, under sidewalks, or in other places where the ground is not likely to be opened for other underground construction.

5.3.8.1 Where splices are made, such splices shall be accessible for inspection and tests.

5.3.8.2 Such cables shall be buried at least 24 in. (609 mm) deep.

5.3.8.2.1 Where crossing streets or other areas likely to be opened for other underground construction, cables shall be installed through solid wall duct or conduit.

5.3.8.2.2 Detectable warning tape shall be buried 12 in. (304 mm) deep above all direct buried cables.

5.4 Aerial Cable and Wire Construction.

5.4.1 Aerial C&S circuit cables and wires shall be run under all power wires but shall not be required to run under other communication wires.

5.4.2 Protection shall be provided where cables and wires pass through trees, under bridges, and over railroads, and at other locations where damage or deterioration is possible.

5.4.3 Wires and cables shall not be attached to a crossarm that carries electric light and power wires.

5.4.4 Support of aerial cables shall comply with 5.4.4.1 and 5.4.4.2.

5.4.4.1 Aerial cable shall be supported by messenger wire that is designed for the application or shall conform to one of the following:

(1) IMSA specifications as a self-supporting cable assembly or an approved equivalent
(2) Fiber-optic cable with integral supporting means or all-dielectric self-supporting (ADSS) type

5.4.4.2 Span lengths shall not exceed the wire or cable manufacturer's recommendations.

5.4.4.3 Single wire shall meet IMSA specifications and shall not be smaller than No. 10 Roebling gauge if of galvanized iron or steel; 10 AWG if of hard-drawn copper; 12 AWG if of approved copper-covered steel; or 6 AWG if of aluminum. Span lengths shall not exceed the manufacturer's recommendations.

5.4.5 Aerial wires and cables connected to buildings shall contact only intended supports.

5.4.6 Aerial circuits shall enter through an approved weatherhead or sleeves slanting upward and inward.

5.4.7 Drip loops shall be formed on wires and cables prior to entering buildings.

5.4.8 Aerial cables extending down poles shall comply with 5.4.8.1 through 5.4.8.4.

5.4.8.1 Aerial cables extending down poles shall be protected against mechanical damage.

5.4.8.2 Any metallic covering of the aerial cables extending down pole(s) shall form a continuous conducting path to earth ground.

5.4.8.3 The installation shall prevent water from entering the conduit.

5.4.8.4 Aerial cables extending down poles shall have 600-volt insulation that is approved for wet locations, as defined in *NFPA 70*.

5.5 Wiring Inside Buildings.

5.5.1 At the communications center, all conductors, cables, and fiber-optic cables shall extend to the operations room in conduits, ducts, shafts, raceways, or overhead racks and troughs that are listed or identified as suitable to provide protection against physical damage.

5.5.1.1 Where fire survivability is required, a listed electrical circuit protective system or a fire-rated cable that is listed to maintain circuit integrity shall be used.

5.5.2* Where installed in buildings, conductors and fiber-optic cables shall be installed in accordance with *NFPA 70* in any one of the following wiring methods:

(1) Electrical metallic tubing
(2) Intermediate metal conduit
(3) Rigid metal conduit
(4) Surface metal raceways
(5) Reinforced thermosetting resin conduit (RTRC)

5.5.2.1 Rigid polyvinyl chloride conduit shall be permitted where approved by the AHJ.

5.5.3 Wire, conductors, and metallic and fiber-optic cables shall have approved insulation in accordance with *NFPA 70*.

5.5.4 The insulation, cable sheath or jacket for wire, conductors, and fiber-optic cables shall have an approved insulation in accordance with *NFPA 70*, Articles 770 and 800.

5.5.5 Conductors and fiber-optic cables shall be installed as far as possible without splices or joints.

5.5.5.1 Splices or joints shall be permitted only in listed junction terminal boxes, enclosures, or other approved termination devices.

5.5.5.2 Wire and fiber-optic terminals, terminal boxes, splices, and joints shall conform to *NFPA 70*.

5.5.5.3 Communications and signal circuits shall be identified by the use of a distinctive color on covers or doors.

5.5.5.4 The words "emergency communication-signal circuit" shall be clearly marked on all terminal and junction locations to prevent unintentional interference.

5.5.6 Conductors that are installed in a vertical riser that connects two or more floors shall meet the requirements of riser-rated cable and installation in accordance with *NFPA 70*.

5.5.7 Metallic and fiber-optic cable terminals and cross-connecting facilities shall be located either in or adjacent to the operations room.

5.5.8 At the communications center, metallic and fiber-optic cable terminals and cross-connecting facilities shall be located either in or adjacent to the operations room.

5.5.9 Where signal conductors, non-dielectric fiber-optic cables, and electric light and power wires are run in the same shaft, they shall be separated by at least 2 in. (51 mm), or each system shall be encased in a noncombustible enclosure.

5.5.10 All wired dispatch circuit devices and instruments whose failure can adversely affect the operation of the system shall be mounted in accordance with the following:

(1) On noncombustible bases, pedestals, switchboards, panels, or cabinets
(2) With mounting designed and constructed so that all components are readily accessible

5.6 Circuit Protection.

5.6.1 Circuit protection required at the communications center shall be provided in all buildings that house communications center equipment.

5.6.1.1 All surge arresters shall be connected to the single-point facility ground in accordance with *NFPA 70*.

5.6.2 The protective devices shall be located in proximity to or shall be combined with the cable terminals.

5.6.3 All protective devices designed and approved for the purpose shall be installed at a location accessible only to qualified persons, marked with the name of the manufacturer and the model designation, and shall be accessible for maintenance and inspection.

5.6.4* Wired communications circuits shall have fast-acting surge suppression installed at the point of entrance to the communications center.

5.6.5 Surge arresters shall be designed and listed for the specific application.

5.6.6 Each conductor that enters a communications center from a partially or entirely aerial line shall be protected by a surge arrester.

5.6.7 At the junction points of open aerial conductors and cable, each conductor shall be protected by a surge arrester in accordance with 5.6.7.1 and 5.6.7.2.

5.6.7.1 The surge arrester shall be weatherproof or protected from the weather.

5.6.7.2 A connection shall be provided between the surge arrester ground and any metallic sheath and messenger wire.

5.6.8 Aerial open wire and non-messenger-supported, two-conductor cable circuits shall be protected by surge arresters at intervals of approximately 2000 ft (610 m).

5.6.9 Wired portions of a radio dispatch circuit shall be protected in a manner that is consistent with the provisions of Sections 5.1 through 5.8.

5.6.10 Buildings that house communications equipment shall have lightning protection that complies with NFPA 780.

5.7 Fuses.

5.7.1 All fuses, fuseholders, and adapters shall be clearly marked with their ampere rating.

5.7.2 All fuses that are rated over 2 amperes shall be of the enclosed type.

5.7.3 Fuses shall be located only at the power source.

5.8 Grounding.

5.8.1* Sensitive electronic equipment determined by the AHJ to be essential to the operation of telecommunications and dispatching systems shall be connected to the single-point facility ground in accordance with *NFPA 70*, Article 647.

5.8.2 Listed isolated ground receptacles in accordance with *NFPA 70* shall be provided for all cord-and-plug-connected essential and sensitive electronic equipment.

5.8.3 Where required by the AHJ, unused wire or cable pairs shall be grounded.

5.8.4 Ground connection for surge suppressors shall be made to the single-point facility ground system in accordance with *NFPA 70*.

5.9 Access. All equipment shall be accessible for the purpose of maintenance.

5.10* Pathway Survivability. All pathways shall comply with *NFPA 70*. [**72:**12.4]

5.10.1 Pathway Survivability Level 0. Level 0 pathways shall not be required to have any provisions for pathway survivability. [**72:**12.4.1]

5.10.2 Pathway Survivability Level 1. Pathway survivability Level 1 shall consist of pathways in buildings that are fully protected by an automatic sprinkler system in accordance with NFPA 13 with any interconnecting conductors, cables, or other physical pathways installed in metal raceways. [**72:**12.4.2]

5.10.3* Pathway Survivability Level 2. Pathway survivability Level 2 shall consist of one or more of the following:

(1) 2-hour fire-rated circuit integrity (CI) or fire-resistive cable
(2) 2-hour fire-rated cable system [electrical circuit protective system(s)]
(3) 2-hour fire-rated enclosure or protected area
(4)* Performance alternatives approved by the authority having jurisdiction

[**72:**12.4.3]

5.10.4 Pathway Survivability Level 3. Pathway survivability Level 3 shall consist of pathways in buildings that are fully protected by an automatic sprinkler system in accordance with NFPA 13 and one or more of the following:

(1) 2-hour fire-rated circuit integrity (CI) or fire-resistive cable
(2) 2-hour fire-rated cable system [electrical circuit protective system(s)]
(3) 2-hour fire-rated enclosure or protected area
(4)* Performance alternatives approved by the authority having jurisdiction

[**72:**12.4.4]

Chapter 6 Emergency Response Facilities

6.1 General. A primary and a secondary means of dispatch notification shall be provided at the ERF and comply with 6.1.1 and 6.1.2.

6.1.1 The primary means of dispatch notification at the ERF shall be compatible with the primary means of dispatch notification that is provided at the communications center.

6.1.2 The secondary means of dispatch notification at the ERF shall be compatible with the secondary means of dispatch notification that is provided at the communications center.

6.1.3 Dispatch notification equipment shall be kept in working order at all times.

6.1.4 A publicly accessible means for reporting alarms to the communications center shall be provided on the exterior of the ERF.

6.2 Commercial Telephone.

6.2.1* A commercial telephone shall be provided at each emergency response facility.

6.2.2* When no other means of voice communication between the communications center and an ERF is provided, the telephone at the ERF shall be arranged so that it cannot be used by the public.

6.3 Fire Protection. Fire protection shall be provided as required by *NFPA 5000* or in accordance with the building code legally in force, whichever is more restrictive.

6.3.1 Sprinkler systems shall comply with NFPA 13.

6.3.2 Fire alarm systems shall comply with *NFPA 72*.

6.4 Power. Two independent and reliable power sources shall be provided, each of which shall be of adequate capacity for operation of the communications equipment.

6.5 Lighting.

6.5.1 Lighting shall be provided to enable personnel to operate communications equipment that is used for the receipt of alarms.

6.5.2 Emergency lighting shall be provided in accordance with NFPA *101*, Section 7.9.

6.6* Communications Conductors. Communications conductors in an ERF shall be installed in accordance with *NFPA 70*.

6.6.1 Circuit protection shall be in accordance with Section 5.6.

6.6.2 Lightning protection shall be in accordance with Section 4.9.

Chapter 7 Operations

7.1 Management.

7.1.1 All system operations shall be under the control of a manager, director, or supervisor of the jurisdiction served by the system.

7.1.1.1 Emergency services dispatching entities shall have trained and qualified technical assistance available for trouble analysis and repair by in-house personnel or by authorized outside contract maintenance services.

7.1.1.1.1 All maintenance records shall be maintained in accordance with the requirements of the AHJ.

7.1.1.2 Where maintenance is provided by an organization or person other than an employee of the jurisdiction, complete written records of all installation, maintenance, test, and extension of the system shall be forwarded to the responsible employee of the jurisdiction.

7.1.1.3 Maintenance performed by an organization or person other than an employee of the jurisdiction shall be by written contract that contains a guarantee of performance as approved by the AHJ.

7.1.2* All equipment shall be accessible to the AHJ for the purpose of maintenance.

7.1.3 Personnel in supervisory roles shall receive supervisory training as defined by the AHJ.

7.1.4 The AHJ shall be responsible for initial and ongoing training in supervisory skills for personnel in supervisory roles.

7.2 Telecommunicator Qualifications and Training.

7.2.1 Telecommunicators shall meet the qualification requirements of NFPA 1061 as appropriate for their position.

7.2.2* Telecommunicators shall be certified in the knowledge, skills, and abilities related to their job-related function.

7.2.2.1 The certification program shall have a skill maintenance component for recertification as defined by the certifying organization.

7.2.3 Telecommunicators shall be trained in general emergency service operations and shall have access to information regarding the following:

(1) Locations of streets
(2) Locations of important structures, including schools, hospitals, and other buildings with a high life hazard
(3) Locations of congested or hazardous areas

7.2.4 Telecommunicators shall have operational knowledge of the functions of communications equipment,systems, and networks in the communications center.

7.2.5 Telecommunicators shall know the rules and regulations that relate to equipment use, including those of the Federal Communications Commission that pertain to emergency service radio use.

7.2.6 The AHJ shall be responsible for providing training to maintain the skill levels of telecommunicators to the level appropriate to their position as identified in NFPA 1061 and Section 7.2.

7.2.7 Telecommunicators shall be trained in TDD/TTY procedures, with training provided at a minimum of every 6 months.

7.2.8 Telecommunicators shall receive training on the CEMP, including the TICP, at least annually.

7.3 Staffing.

7.3.1 There shall be a minimum of two telecommunicators on duty and present in the communications center at all times.

7.3.1.1* The AHJ shall ensure that there are sufficient telecommunicators available to effect the prompt receipt and processing of alarms needed to meet the requirements of Section 7.4.

7.3.1.2* Where communications systems, computer systems, staff, or facilities are used for both emergency and nonemergency functions, the nonemergency use shall not degrade or delay emergency use of those resources.

7.3.1.3 A communications center shall handle emergency calls for service and dispatching in preference to nonemergency activities.

7.3.2* When requested by the incident commander, a telecommunicator shall be dedicated to the incident and relieved of other duties within the communications center.

7.3.3 The AHJ shall establish standard operating procedures to identify the circumstances under which a telecommunicator will be assigned to the incident and how that will be accomplished.

7.3.4* Supervision shall be provided when more than two telecommunicators are on duty.

7.3.4.1 Supervision shall be provided by personnel located within the communications center who are familiar with the operations and procedures of the communications center.

7.3.4.2 The supervisor shall be allowed to provide short-term relief coverage for a telecommunicator, provided that the telecommunicator does not leave the communications center and is available for immediate recall as defined in the policies and procedures of the AHJ.

7.4 Operating Procedures.

7.4.1* Ninety-five percent of alarms received on emergency lines shall be answered within 15 seconds, and 99 percent of alarms shall be answered within 40 seconds. *(For documentation requirements, see 12.5.2.)*

7.4.1.1 Compliance with 7.4.1 shall be evaluated monthly using data from the previous month.

7.4.2* With the exception of the call types identified in 7.4.2.2, 90 percent of emergency alarm processing shall be completed within 64 seconds, and 95 percent of alarm processing shall be completed within 106 seconds. *(For documentation requirements, see 12.5.2.)*

7.4.2.1 Compliance with 7.4.2 shall be evaluated monthly using data from the previous month.

7.4.2.2 Emergency alarm processing for the following call types shall be completed within 90 seconds 90 percent of the time and within 120 seconds 99 percent of the time:

(1) Calls requiring emergency medical dispatch questioning and pre-arrival medical instructions
(2) Calls requiring language translation
(3) Calls requiring the use of a TTY/TDD device or audio/video relay services
(4) Calls of criminal activity that require information vital to emergency responder safety prior to dispatching units
(5) Hazardous material incidents
(6) Technical rescue
(7) Calls that require determining the location of the alarm due to insufficient information
(8) Calls received by text message

7.4.3* For law enforcement purposes, the AHJ shall determine time frames allowed for completion of dispatch.

7.4.4* Where alarms are transferred from the primary public safety answering point (PSAP) to a secondary answering point, the transfer procedure shall not exceed 30 seconds for 95 percent of all alarms processed. *(For documentation requirements, see 12.5.2.)*

7.4.4.1 The PSAP shall transfer alarms as follows:

(1) The alarm shall be transferred directly to the telecommunicator.
(2) The answering transferring agency shall remain on the line until it is certain that the transfer is effected.
(3) The transfer procedure shall be used on emergency 9-1-1 calls.

7.4.5 All alarms, including requests for additional resources, shall be transmitted to the identified emergency response units over the required dispatch systems.

7.4.6 An indication of the status of all emergency response units shall be available at all times to telecommunicators who have dispatching responsibility.

7.4.7* Records of the dispatch of emergency response units to alarms shall be maintained in accordance with the records retention policy of the AHJ and shall identify the following:

(1) Unit designation for each emergency response unit (ERU) dispatched
(2) Time of dispatch acknowledgment by each ERU responding
(3) Enroute time of each ERU
(4) Time of arrival of each ERU at the scene
(5) Time of patient contact, if applicable
(6) Time each ERU is returned to service

7.4.8* Where voice transmission is used as a dispatch method, the announcement for the emergency response shall be preceded by an audible warning or alerting signal that differentiates the emergency from routine radio traffic.

7.4.9 The first emergency response unit that arrives at the location of the alarm shall provide a brief preliminary report on observed conditions to the communications center.

7.4.10* A communications officer shall be assigned at major incidents.

7.4.11* All emergency response agencies that interact shall use common terminology and integrated incident communications.

7.4.11.1 Integrated incident communications shall include a plan that provides for on-demand interoperability of communication methods among emergency response agencies.

7.4.11.2* The plan shall identify the communications links and protocols to be used among emergency response agencies at incidents, including the following:

(1) Type 5 incidents (local, discipline specific) as defined in NFPA 1561
(2) Type 4 incidents (local, jurisdiction specific) as defined in NFPA 1561
(3)* Type 3 incidents (regional or state, multi-agency and multi-discipline specific) as defined in NFPA 1561

7.4.11.3 The plan shall be written, distributed to all agencies identified in the plan, and reviewed at least annually by each agency identified.

7.4.12 The communication equipment involved in each alarm shall be restored promptly after each alarm.

7.4.13 When the device monitoring the system for integrity indicates that trouble has occurred, the telecommunicator shall act as follows:

(1) Take appropriate steps to troubleshoot and repair the fault according to the policies and procedures of the AHJ.
(2) Isolate the fault and notify the official responsible for maintenance as soon as practical.

7.4.14 Standard operating procedures shall include but not be limited to the following:

(1) All standardized procedures that the telecommunicator is expected to perform without direct supervision
(2) Implementation plan that meets the requirements of 4.1.5.3
(3) Procedures related to the CEMP
(4) Emergency response personnel emergencies
(5) Activation of an emergency distress function
(6) Assignment of incident radio communications plan matrix
(7) Time limit for acknowledgment by units that have been dispatched
(8) Methods for call trace
(9) Methods for caller location determination

7.4.15* Every communications center shall have a comprehensive regional emergency communications plan as part of the CEMP.

7.4.15.1* The emergency communications plan shall provide for real-time communications between organizations responding to the same emergency incident.

7.4.15.2* This plan shall be exercised at least once a year.

7.4.16 A distinctive alert tone signal shall precede the transmission of emergency message traffic.

7.4.16.1 A separate and unique alert tone shall be operated for emergency evacuation orders.

7.4.17 In the event that an ERU(s) has not acknowledged its dispatch/response within the time limits established, the telecommunicator shall perform one or more of the following:

(1) Attempt to contact the ERU(s) by radio
(2) Redispatch the ERU(s) using the primary dispatch system
(3) Dispatch the ERU(s) using the secondary dispatch system
(4) Initiate two-way communication with the ERU's supervisor
(5) If the SOP time for dispatch has elapsed, initiate dispatch of backup ERU

7.4.18* The AHJ shall develop and implement standard operating procedures for responding to and processing TDD/TTY calls.

7.4.19 Calls received as an open-line or "silent call" shall be queried as a TDD/TTY call if no acknowledgment is received by voice.

7.5 Time.

7.5.1 All systems shall have the ability to interface with a master time source and to synchronize the time clocks of all appliances, devices, computers, and servers.

7.5.2 All systems shall have the ability to automatically update the time clocks of all appliances, devices, computers, and servers without the intervention of the AHJ.

7.5.3 All systems shall have the ability to automatically update the time clocks of all appliances, devices, computers, and servers to adjust from standard time to daylight savings time and from daylight savings time to standard time without the intervention of the AHJ.

7.5.4 All timekeeping devices not capable of being synchronized with the master time source shall be maintained within60 seconds of the master time source.

7.6 Recording.

7.6.1 Communications centers shall have a logging voice recorder with one channel for each of the following:

(1) Each transmitted or received radio channel or talkgroup
(2) Each voice dispatch alarm circuit
(3)* Each telecommunicator telephone

7.6.2 All logging recording equipment shall have the ability to associate the date, time, and channel designation with each transmission.

7.6.2.1 All logging recording equipment connected to a Next Generation 9-1-1 ESInet shall have the ability to record logging events data.

7.6.3 Each telecommunicator position shall have the ability to instantly recall telephone and radio recordings from that position.

7.6.3.1 All recordings, including transmissions and data, shall be maintained in accordance with the records retention policies of the AHJ.

7.6.4 Alarms that are transmitted over the required dispatch circuit(s) shall be automatically recorded, including the dates and times of transmission.

7.6.4.1 The recording device shall be networked with the master time source.

7.7* Quality Assurance/Improvement. Communications centers shall establish a quality assurance/improvement program to ensure the consistency and effectiveness of alarm processing.

Chapter 8 Telephones

8.1* Telephone Receiving Equipment. The provisions of Chapter 8 shall apply to facilities and equipment that are needed to receive alarms.

8.2 Directory Listing.

8.2.1 Where 9-1-1 service is not provided, all of the following requirements shall be met:

(1) A specific telephone number shall be assigned for calls requesting emergency services.
(2) The telephone number shall be publicized as such.
(3) A separate number shall be assigned for business (nonemergency) use.

8.2.1.1 A separate telephone line with a number that is not listed shall be maintained for communication with other emergency service agencies and receipt of central station alarms.

8.2.1.2* A separate number shall be assigned for business (nonemergency) use.

8.2.2 Where 9-1-1 service is provided, the telephone directory listings shall indicate that 9-1-1 is the number to call for all emergencies.

8.2.3 Telephone directory listings shall be as specified in 8.2.3.1 through 8.2.3.5.

8.2.3.1 The text and symbols shown in Figure 8.2.3.1(a) through Figure 8.2.3.1(c) shall appear on the inside front cover or the page facing the inside front cover of the white pages directory.

8.2.3.2 The emergency services listing shall appear in the directory under the name of the jurisdiction, including government listings, and under the headings for police, fire, and ambulance where provided.

FIGURE 8.2.3.1(a) Telephone Directory Listing for Fire Department.

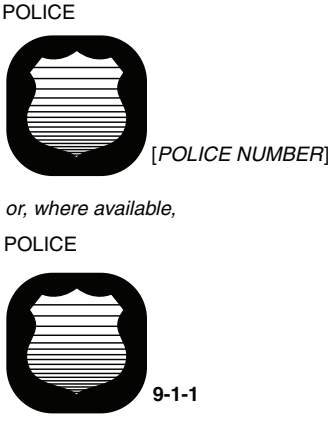

FIGURE 8.2.3.1(b) Telephone Directory Listing for Police Department.

EMERGENCY MEDICAL SERVICES

[*EMERGENCY MEDICAL SERVICES NUMBER*]

or, where available,

EMERGENCY MEDICAL SERVICES

9-1-1

FIGURE 8.2.3.1(c) Telephone Directory Listing for Emergency Medical Services.

8.2.3.3 The following listings and telephone numbers shall appear as follows in the white pages directory:

(1) Fire department
   (a) To report an emergency [fire number] or, where available, 9-1-1
   (b) Nonemergency purposes [business number]
(2) Police department
   (a) To report an emergency [police number] or, where available, 9-1-1
   (b) Nonemergency purposes [business number]
(3) Emergency medical services
   (a) To report an emergency [emergency medical number] or, where available, 9-1-1
   (b) Nonemergency purposes [business number]

8.2.3.4 If the directory covers an area that is protected by more than one emergency service, each agency or district shall appear in the listing as specified in 8.2.3.1.

8.2.3.5 If the emergency service protects an area that is covered by more than one directory, each directory shall list the agency or district as specified in 8.2.3.1 through 8.2.3.3.

8.2.3.6* Where an ERF that is not continuously staffed by trained telecommunicators is listed in the telephone directory, callers shall be provided with a recorded message that refers them to the appropriate emergency number when calls to the listed number are not answered.

8.3 Equipment and Operations. At the communications centers, telephone lines shall be provided as follows:

(1)* At least two telephone lines shall be assigned exclusively for receipt of emergency calls.
(2) Additional emergency lines shall be provided as required for the volume of calls handled to provide P.01 GOS.
(3) Additional telephone lines shall be provided for the normal business (nonemergency) number(s) as needed.
(4) At least one outgoing-only line shall be provided.
(5) A separate telephone line shall be provided as required in 8.2.1.1.

8.3.1 The AHJ shall ensure that the published emergency lines are answered prior to nonemergency lines.

8.3.1.1 When all emergency lines are in use, emergency calls shall hunt to other predetermined lines that are approved by the AHJ.

8.3.1.2 Calls to the business number shall not hunt to the designated emergency lines.

8.3.2 When a PSAP receives an emergency call for a location that is not in its jurisdiction or a call for an agency not under the control of the PSAP, the PSAP shall transfer the call directly to the responsible communications center, when possible.

8.3.2.1 The PSAP shall remain on the line until it is certain that the transfer has been made.

8.3.2.2 The transfer procedure shall not rely on the PSAP personnel relaying the information to the responsible communications center.

8.3.3 All incoming calls on designated emergency lines shall be recorded in accordance with this standard.

8.3.4* If an incoming call on any designated emergency line is not answered within 60 seconds, an alarm indication shall be automatically transmitted to a location approved by the AHJ.

8.3.5* Where the AHJ permits the communications center to receive automated voice alarms, the following requirements shall apply:

(1) A separate, unlisted telephone line(s) shall be provided to receive such alarms.
(2) Such voice alarms shall not be permitted to connect to the telephone lines required by 8.2.1 and Section 8.3.

8.3.6 Where the communications center is permitted to receive automated data alarms through dial-up telephone service, the following requirements shall apply:

(1) A separate, unlisted telephone line(s) shall be provided to receive such alarms.
(2) Such data alarms shall not be permitted to connect to the telephone lines required by 8.2.1 and Section 8.3.

8.3.7 Published emergency numbers shall meet the requirements of Section 8.5.

8.3.8 All telecommunicator positions that are available for receiving emergency calls shall be equipped with TDD/TTY equipment.

8.4 Universal Emergency Number 9-1-1 Service.

8.4.1 General. Universal emergency number 9-1-1 service shall meet the minimum requirements as specified in Section 8.4.

8.4.2 Reliability.

8.4.2.1 The universal emergency number service equipment shall be designed so that no single point of failure can prevent calls from being answered.

8.4.2.2 Under failure conditions, the full-feature complement shall not be required to be maintained but the calling party shall be able to communicate with the telecommunicator.

8.4.3 Circuits.

8.4.3.1* At least two 9-1-1 call delivery paths with diverse routes arranged so that no single incident interrupts both routes shall be provided to each communications center.

8.4.3.2* Where multiple communications centers that serve a jurisdiction are not located in a common facility, at least two circuits with diverse routes, arranged so that no singular incident interrupts both routes, shall be provided between communications centers.

8.4.4 Where enhanced 9-1-1 services are provided, the communications center shall be capable of receiving automatic number information and automatic location information (including Wireless Phase II data) from sources identified in Section 8.1.

8.5 Published Emergency Number Alternative Routing.

8.5.1* Communications centers shall maintain a plan as part of the CEMP for rerouting incoming calls on emergency lines when the center is unable to accept such calls.

8.5.2 Where the AHJ requires that overflow calls to emergency lines be routed to alternative telephone lines within the PSAP, the alternative telephone lines shall be monitored for integrity and recorded as required by this standard.

8.5.3 Where a PSAP operates on a part-time basis, an automatic alternative routing plan shall be put in place that ensures the rapid transfer of calls to the designated backup PSAP, even if the transfer switch, where provided, is not turned on.

8.5.4 Any call that has not been answered after 20 seconds shall be automatically routed as required by one of the following:

(1) A designated alternate PSAP
(2)* A holding queue
  (a) When in queue, the callers shall receive a recorded message informing them that they have reached the PSAP, including a TDD/TTY recorded message.
  (b) The system shall periodically remind callers to the PSAP who are in queue that they are connected during their wait.
  (c) There shall be an audible and visual indication within the operations room that unanswered calls are waiting in the queue.

8.6 Multiple Line Telephone Systems (MLTS).

8.6.1* Every MLTS shall be designed to allow any extension to dial 9-1-1 without the need to dial any digit to obtain a dial tone.

8.6.2* The MLTS shall outpulse or signal the public switched telephone network with a dialable telephone number that, when dialed, will reach the original 9-1-1 caller.

8.6.3* The owner or entity responsible for the operation of the MLTS shall cause the location of the 9-1-1 caller to be made available to the public safety answering point telecommunicator in those jurisdictions where the enhanced 9-1-1 features ANI and ALI are available and in use.

8.6.3.1* The ALI associated with the ANI of the MLTS extension shall be sufficient to direct a response to the 9-1-1 caller in an efficient manner and include, at a minimum, the civic address, building number, and floor, except as provided in 8.6.3.2.

8.6.3.2* Paragraph 8.6.3.1 shall not apply to any MLTS serving a facility of less than 7000 ft^2.

Chapter 9 Dispatching Systems

9.1 Fundamental Requirements of Alarm Dispatching Systems.

9.1.1* General.

9.1.1.1 An alarm dispatching system shall be designed, installed, operated, and maintained to provide for the receipt and retransmission of alarms.

9.1.1.2 The transmission of any trouble signal shall not interfere with the transmission and receipt of alarms.

9.1.1.3 The required number of dispatching circuits shall be in accordance with 9.1.1.3.1 through 9.1.1.3.3.

9.1.1.3.1 Jurisdictions that receive 730 alarms or more per year shall provide two separate and dedicated dispatch circuits as follows:

(1) Separate primary and secondary dispatch circuits shall be provided for transmitting alarms.
(2) The failure of any component of the primary circuit shall not affect the operation of the secondary circuit and vice versa.

9.1.1.3.2* Jurisdictions that receive fewer than 730 alarms per year shall provide a minimum of one dedicated dispatch circuit for transmitting alarms.

9.1.1.3.3* A circuit that terminates at a telephone handset only shall not be considered as fulfilling the requirements for a dispatch circuit. *(See 9.2.2.2.)*

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

(1) Wired circuit, monitored for integrity in accordance with 9.1.2 through 9.1.2.4.3
(2)* Nontrunked voice radio channel with duplicate system elements, with the following features:
  (a) Monitored for integrity as required by 9.1.2.6
  (b) In the event of a failure of the primary system, a means to switch to the secondary system that is immediately available to the telecommunicator
(3) Microwave carrier channel, monitored for integrity in accordance with 9.1.2 through 9.1.2.5.2, with the following features:
  (a) Redundant transceivers at both ends of each microwave path
  (b) Automatic switchover to the second transceiver if the first transceiver fails during operation
(4) Polling or self-interrogating digital data radio channel with the following features:
  (a)* Redundant transceivers at each installed location
  (b) Monitoring for integrity in accordance with 9.1.2 through 9.1.2.5.2
  (c) Automatic switchover to the second transceiver if the first transceiver fails during operation
(5) Dedicated telephone circuit that is monitored for integrity in accordance with 9.1.2 through 9.1.2.4.3, excluding the following:
  (a) Telephone connection through a public-switched telephone network
  (b) Nondedicated phone lines
(6) Trunked radio system in compliance with 9.1.1.4(2) or 9.1.1.4(4)

9.1.1.5 The secondary dispatch circuit shall not be required to be monitored for integrity.

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

(1) A wired circuit
(2)* A designated radio channel
(3) If radio is used for both the primary and secondary dispatch circuits, the following shall apply:
    (a) The primary dispatch circuit shall comply with 9.1.1.4.
    (b)* The secondary dispatch circuit shall consist of a separate radio system operating on a separate channel with a separate receiver for the secondary circuit at each ERF.
(4) An approved dedicated telephone circuit
    (a) Where a telephone dispatch circuit is used as a primary dispatch circuit, a telephone circuit shall not be used as the required secondary dispatch circuit.
    (b) A telephone connection through a public-switched telephone network via a regular dial-up modem and nondedicated telephone line shall not be considered to be an approved dispatch circuit.
(5)* The dispatch signal circuit path for the secondary dispatch circuit specified in 9.1.1.5.1(4)(a) shall be separate and independent of the dispatch signal circuit path of the primary dispatch circuit from the dispatch console to separate control/relay switching equipment connection ports at the ERF.

9.1.1.6* Where voice transmission is used as a dispatch method, the announcement for the emergency response shall be preceded by an audible warning or alerting signal that differentiates the emergency from routine voice traffic.

9.1.1.7 Alarms shall be retransmitted to ERFs or to ERUs in the field from the location at which alarms are received.

9.1.1.7.1 Alarms transmitted from the communications center shall be automatically received at ERFs and ERUs.

9.1.1.7.2 Dispatch methods shall provide for the operation of houselights or other auxiliary functions at the ERF as required by the AHJ.

9.1.1.8 Alarms that are transmitted over the required dispatch circuit(s) shall have the dates and times of transmission automatically recorded at the communications center.

9.1.1.9 Audible devices shall be installed throughout the ERF to ensure that all emergency response personnel are alerted to alarms.

9.1.1.10 Equipment shall be provided to allow personnel to alert all other personnel in the ERF.

9.1.1.11 A means of acknowledging receipt of an alarm from the emergency response personnel to the telecommunicator shall be provided.

9.1.2* Monitoring for Integrity. Primary dispatch circuits and devices upon which transmission and receipt of alarms depend shall be monitored constantly to provide prompt warning of trouble that impacts operation.

9.1.2.1* A polling or self-interrogating radio system shall be monitored hourly for integrity to ensure system reliability.

9.1.2.2 The primary and secondary power sources supplied to all required circuits and devices of the system shall be monitored for integrity.

9.1.2.3 Trouble signals shall actuate an audible device and a visual signal located at a constantly attended location.

9.1.2.4 The audible alert trouble signals from the fault and failure monitoring mechanism shall be distinct from the audible alert emergency alarm signals.

9.1.2.4.1 The audible trouble signal shall be permitted to be common to several monitored circuits and devices.

9.1.2.4.2 A switch for silencing the audible trouble signal shall be permitted if the visual signal continues to operate until the silencing switch is restored to the designated normal position.

9.1.2.4.3 The audible trouble signal shall respond to faults that occur on all other circuits prior to the restoration of the silencing switch to the "normal" position.

9.1.2.5 Where dispatch systems use computer diagnostic software, monitoring of the primary dispatch circuit components shall be routed to a dedicated terminal(s) that meets the following requirements:

(1) It shall be labeled and identified as "dispatch circuit integrity status."
(2) It shall be located within the communications center.
(3) It shall not be used for routine dispatch activities.

9.1.2.5.1 The computer diagnostic software shall be capable of displaying and testing each circuit that can be electronically monitored from the dispatch console to the station control unit or junction relay switching equipment in the ERF.

9.1.2.5.2 Any fault or failure condition within the dispatch circuit path shall be displayed on the dedicated terminal screen in a prominent (highlighted) fashion that satisfies the visual trouble signal requirement, and with an audible trouble signal, referenced in 9.1.2.4 through 9.1.2.5.2, that actuates and sounds in accordance with the type of dispatch circuit that is being monitored.

9.1.2.6* The radio communications system shall be monitored in the following ways:

(1) Monitoring for integrity shall detect faults and failures in the radio communications system.
(2) Detected faults and failures in the radio communications system shall cause audible and visual indications to be provided to the telecommunicator and radio system manager at the time of signal activation.

9.1.2.6.1 Monitoring for integrity of portable radios and radio equipment installed in an ERF and in emergency response vehicles shall not be required.

9.2 Wired Dispatching Systems.

9.2.1 Wired Circuits — General.

9.2.1.1* A separate tie circuit shall be provided from the communications center to each alternate communications center or a PSAP.

9.2.1.2 Equipment shall be designed and installed so that it is capable of performing its intended function over the range of 85 percent to 110 percent of its rated voltage.

9.2.1.3 The normal operation of the system shall not require the use of a ground return to provide any essential function.

9.2.1.3.1 Circuits that extend outside the communications center shall test free of grounds.

9.2.1.3.2 The ground connection shall be permitted to be used to provide function under abnormal line conditions where such use would not prevent the reception or transmission of a signal under normal conditions if the circuit were accidentally grounded.

9.2.1.4 A public alarm reporting system circuit that enters an ERF and that is connected to automatic recording and sounding equipment shall be permitted to be one of the two required dispatch circuits.

9.2.1.5 In jurisdictions where fewer than 730 alarms per year are received or where all stations have recording and sounding devices that respond to each public reporting circuit, the second dispatch circuit shall not be required; only the circuit that is monitored for integrity shall be required.

9.2.1.6 The following requirements shall apply to systems in which an alarm from a fire alarm box is automatically transmitted to fire stations and, if used, is transmitted to supplementary alerting devices (Type B system):

(1) Equipment shall be installed to automatically transmit alarms that are received from any public reporting circuit to all emergency response facilities and, where employed, to outside sounding devices.
(2) Control equipment shall allow any or all circuits to be individually connected to or disconnected from the repeating mechanism.
(3) Coded transmitting devices that use metal conductors shall be provided with a means to transfer the signal from one dispatch circuit to another.

9.2.1.7 A wired dispatch circuit that is part of a public alarm reporting system shall meet the requirements of *NFPA 72*.

9.2.1.8 A wired circuit shall not be connected to alarm instruments in more than five emergency response facilities.

9.2.1.9 Coded signals shall be transmitted as follows:

(1) At a minimum rate of two strokes per second
(2) Over separate circuits at a rate that is suitable for such devices where outside alerting devices are employed

9.2.1.10 Where wired voice dispatch circuits are used, each circuit shall be dedicated to each emergency response facility.

9.2.1.11 For coded and telegraphic systems, a permanent record that indicates the exact location from which the alarm is being received and an audible signal shall be required to indicate the receipt of an alarm.

9.2.1.12 Where telegraphic retransmission is used, the telecommunicator shall be permitted to enter dates and times manually where approved by the AHJ.

9.2.2 Telephone Circuits.

9.2.2.1 A telephone circuit that is used as one of the dispatch circuits shall meet the requirement in 9.1.1.4.

9.2.2.2 Where the primary or secondary dispatch circuit is a telephone dispatch circuit, it shall have voice amplification with the following capabilities:

(1) It shall be equipped with a loudspeaker(s).
(2) The use of a handset shall automatically disconnect the loudspeaker(s) from the circuit(s).

9.3 Radio Dispatching Systems.

9.3.1 General.

9.3.1.1* All radio communications shall comply with the rules and regulations governing wireless communications in the country of operation.

9.3.1.2 The communications center shall be equipped for radio communications with ERUs using subscriber radios.

9.3.1.2.1 Radio communication systems shall be designed to provide no less than 95 percent coverage of the jurisdictional area as defined by the AHJ, 95 percent of the time, with a 95 percent confidence factor.

9.3.1.2.2* Radio and outdoor coverage shall be sufficient to provide a delivered audio quality (DAQ) of 3.0 for analog or digital systems.

9.3.1.3* A communications radio channel, separate from the radio dispatch channel, shall be provided for on-scene tactical communications.

9.3.1.4* At a minimum, the tactical communications channel identified in 9.3.1.3 shall be capable of operating in analog simplex mode.

9.3.1.5* Trunked system talk groups shall be permitted to be used to provide on-scene tactical communications if desired by the AHJ, and the provisions of9.3.1.3 and 9.3.1.4 shall still apply.

9.3.1.6* Communications system design shall be such that a portable radio is capable of operating within the dispatch area without the use of mobile radio frequency (RF) amplifiers.

9.3.1.7 If the radio includes scanning capability, it shall have an automatic priority feature that causes the radio receiver to revert automatically to its primary channel when the channel is being used.

9.3.1.8 A visual indication shall be provided indicating that the radio equipment is turned on.

9.3.1.9 With the exception of mobile and portable radios, radio antenna systems shall include surge arresters.

9.3.1.10 Radio communications equipment shall be capable of transmitting a distinctive alert tone for emergency traffic as required in NFPA 1561.

9.3.2 Signaling and Control Systems.

9.3.2.1 Signaling and control systems that are used to alert a specific ERF(s) shall initiate distinctive announcement tones for various voice alarms.

9.3.2.2 Signaling and control systems shall use both polling and automatic transmission communications methods and shall support redundant designs as required in 9.1.1.4.

9.3.2.3 If used for signal and control systems, Internet protocol (IP) wide-area networks shall comply with the following:

(1) They shall comply with the communication methods of 9.3.2.2.
(2) If the primary network connector fails during operations, switchover to the second network connection shall be automatic, with audible and visual indicators to the telecommunicator.
(3)* The network path used shall be under the control of the AHJ.

9.3.3 Conventional Two-Way Voice Systems.

9.3.3.1* Analog System Requirements. Systems shall be equipped with a coded squelch system to minimize interference.

9.3.3.2 Digital Conventional System Requirements. Digital conventional systems shall comply with ANSI/TIA-102.BAAA, *FDMA Common Air Interface*.

9.3.3.3 Call Indicator. A call indicator shall be provided for each conventional channel controller from the control center console.

9.3.4 Trunked Two-Way Voice Systems.

9.3.4.1* Signaling Channel Concept.

9.3.4.1.1 The trunked system shall operate using a dedicated signaling control channel protocol concept embodied in either a distinct RF channel used for control signaling only or embedded control signals in the voice channels such that a dedicated RF channel for control signaling is not necessary but the same result is effected.

9.3.4.1.2 System control messages and calls and mobile requests for service shall be transmitted to and from the system on the signaling channel.

9.3.4.1.3 Each unit shall send its unique discrete address identification to the system each time the unit transmits, regardless of whether the system is operating in the message trunking mode or transmission trunking mode.

9.3.4.1.4 Mobile and portable units shall be capable of operating on at least five radio channels.

9.3.4.1.5* Mobile and portable units shall be capable of scanning trunked talkgroups and conventional channels with a user-selectable priority.

9.3.4.1.6 A system controller shall automatically assign all channels so that all system users (field units and console dispatchers) shall have access to all voice channels via a system priority protocol.

9.3.4.1.7 Channel access time in single-site systems, assuming a channel is available, shall be less than ½ second.

9.3.4.1.8* Priority Levels.

9.3.4.1.8.1 A minimum of eight levels of operational talkgroup priority shall be incorporated into the system.

9.3.4.1.8.2 Dispatch consoles shall be capable of elevating the operational priority of a talkgroup by one increment to facilitate channel assignments in critical situations.

9.3.4.1.9* Emergency Priority.

9.3.4.1.9.1 All field units in the system shall be capable of gaining access to the system within ½ second of activation of an instantaneous emergency switch.

9.3.4.1.9.2 When a field unit activates the emergency function of the radio unit, the field unit ID shall be displayed at the dispatch terminal, console, or both, and an audible alert shall be activated.

9.3.4.1.9.3 A voice channel shall be immediately assigned to handle the emergency communications regardless of system loading.

9.3.4.1.10* Failure of Trunking System.

9.3.4.1.10.1 If the trunking system control fails, the system, at a minimum, shall revert to conventional operation while in failover mode.

9.3.4.1.10.2 ERUs that share trunked radio systems with other emergency or nonemergency services shall operate on a channel that is not shared with nonemergency users.

9.3.4.1.10.3 Standard operating guidelines shall be written to explain to field units, first responders, and radio dispatchers on the trunked radio system how to detect that the system is in failover mode and what revised operational procedures they are to adopt when the trunked system is in failover mode.

9.3.4.1.11* Queuing of Request for Voice Channel.

9.3.4.1.11.1 If all available talking channels are assigned, the second- and lower precedence–level requests for a talking channel shall be placed in a queue according to the priority levels involved.

9.3.4.1.11.2 The queue shall cause the system to assign talking channels as they become available on a priority-level basis.

9.3.4.1.11.3 If multiple talkgroups with the same priority are in the queue, they shall be assigned a channel on a first-in-first-out (FIFO) basis.

9.3.4.1.11.4 The queuing protocol shall process and assign channels to requesting units that have been involved in recent conversations before processing and assigning channels to units not involved in any recent conversations, assuming both talkgroups have equal priorities.

9.3.4.1.12 When any unit is placed into a system-busy queue, the unit requesting the channel shall be notified automatically by the system when it assigns a channel to the unit.

9.3.4.1.13 All units operating within the same talkgroup shall receive both sides of every conversation addressed to or from the talkgroup.

9.3.4.1.14 Where required for mobile or portable units, the system shall provide a means for selectively alerting one unit from another unit or from a dispatch location.

9.3.4.1.15 Continuous Talkgroup Affiliation Notification.

9.3.4.1.15.1 The system shall broadcast a continuous update of the talkgroup channel assignments to field units.

9.3.4.1.15.2 Units that become activated during a conversation, or units that leave the system coverage and return, shall use the continuous update to immediately affiliate with their assigned talkgroup.

9.3.4.1.16* Whenever a field unit leaves the coverage of the signaling channel and attempts to access the system using the push-to-talk (PTT) button, an audible alert shall be sounded.

9.3.4.1.17* Individual Unit Disable.

9.3.4.1.17.1 Hardware and software that allow disablement of any mobile or portable unit(s) currently operating on the system shall be provided.

9.3.4.1.17.2 Disablement of such a unit(s) shall be possible even if the system manager terminal or the console is inoperative.

9.3.4.1.18* The system shall allow a telecommunicator to initiate a change in the operating talkgroup of any field unit from a system manager terminal.

9.3.4.1.19* Where telephone interconnect has been provided as a part of the system, the system shall be configured so that no telephone call prevents or delays any dispatch communications required by the AHJ.

9.3.4.1.20 Monitoring for Integrity.

9.3.4.1.20.1 A subsystem dedicated to monitoring the trunked system infrastructure backbone shall be provided.

9.3.4.1.20.2 Fault and status information, including information on the condition of base station repeaters and controllers, shall be accessible from a system manager terminal.

9.3.4.1.20.3 A means shall be provided that is capable of recording system problems as they occur.

9.3.4.1.21 Console Call Indicator.

9.3.4.1.21.1 A call indicator shall be provided for each talkgroup controlled from the control center console.

9.3.4.1.21.2 When a channel is selected, the call indicator shall flash when audio is available.

9.3.4.1.22 When required by the AHJ, the console shall operate in the full duplex mode so that a telecommunicator can simultaneously transmit to a trunked talkgroup and receive their response without releasing the PTT button.

9.3.4.1.23 Console Trunked Busy Indication.

9.3.4.1.23.1 If the telecommunicator attempts to make a call and all trunked channels are busy, a visual alert shall be initiated at the console.

9.3.4.1.23.2 When the channel becomes available, the console shall automatically alert the telecommunicator with an audible tone and "hold" the channel for the telecommunicator for 2 seconds to 4 seconds to allow the telecommunicator time to activate a PTT for the appropriate talkgroup.

9.3.4.1.24* Console Dispatch Preemption.

9.3.4.1.24.1 The system shall be configured so that no "busy" indication is received by a telecommunicator attempting to access a talkgroup required for dispatch of an alarm.

9.3.4.1.24.2 If necessary, the requirement of 9.3.4.1.24.1 shall be met by preemption of the lowest-priority communication on the system at the time of attempted access to the talkgroup.

9.3.4.1.25 The telecommunicator shall have the following capabilities:

(1) The telecommunicator shall be able to designate a higher tactical priority for certain talkgroups at their workstation.
(2) Designation of higher tactical priority shall be achieved by means of a switch on that talkgroup appearance.

9.3.4.2* Digital Trunked System Requirements. Digital trunked systems shall comply with ANSI/TIA-102.BAAA, *FDMA Common Air Interface*, or TIA-102.BBAB, *Project 25 Phase 2 Two-Slot Time Division Multiple Access Physical Layer Protocol Specification*; and with TIA-102.BBAC *Project 25 Phase 2 Two-Slot TDMA Media Access Control Layer Description* and shall meet the requirements in 9.3.4.1.

9.3.5* Two-Way Mobile Equipment.

9.3.5.1 All emergency response units shall be equipped with a two-way mobile radio that is capable of communicating with the communications center.

9.3.5.2 Mobile radios shall be equipped with a visual transmit indicator.

9.3.5.3 All mobile radios shall be equipped with a carrier control timer that disables the transmitter and signals the operator with a distinctive tone after a time predetermined by the AHJ.

9.3.5.4 Mobile radios and associated equipment shall be manufactured for the environment in which they are to be used.

9.3.5.5 Mobile radios shall be capable of multiple-channel operation to enable on-scene simplex radio communications that are independent of dispatch channels.

9.3.5.6 Spare mobile radio units shall be provided for emergency response units as follows:

(1) Minimum of one spare unit for each model not directly interchangeable
(2) Minimum of one spare unit for each 20 units, or fraction thereof, in service

9.3.6* Two-Way Portable Equipment.

9.3.6.1 All ERUs shall be equipped with a portable radio that is capable of two-way communication with the communications center.

9.3.6.2 Portable radios shall be manufactured for the environment in which they are to be used and shall be of a size and construction that allow their operation with the use of one hand.

9.3.6.3 Portable radios that are equipped with key pads that control radio functions shall have a means for the user to disable the keypad to prevent inadvertent use.

9.3.6.4 All portable radios shall be equipped with a carrier control timer that disables the transmitter and signals the operator with a distinctive tone after a time predetermined by the AHJ.

9.3.6.5 Portable radios shall be capable of multiple-channel operation to enable on-scene simplex radio communications that are independent of dispatch channels.

9.3.6.6 Portable radios shall be designed to allow channels to be changed while emergency response personnel are wearing gloves.

9.3.6.7 Single-unit battery chargers for portable radios shall be capable of fully charging the radio battery while the radio is in the receiving mode.

9.3.6.8 Battery chargers for portable radios shall automatically revert to maintenance charge when the battery is fully charged.

9.3.6.9 Battery chargers shall be capable of charging batteries in a manner that is independent of and external to the portable radio.

9.3.6.10 Spare batteries shall be maintained in quantities that allow continuous operation as determined by the AHJ.

9.3.6.11 A minimum of one spare portable radio shall be provided for each 10 units, or fraction thereof, in service.

9.3.6.12* Portable radios used by first responders who might encounter hazardous locations because of the presence of explosive gas or explosive dust atmospheres shall be rated as intrinsically safe for operation in such atmospheres by a nationally recognized testing laboratory, if determined necessary by the AHJ.

9.3.7* Mobile Command Vehicles. Vehicles that are used in command or communications functions shall meet the requirements of NFPA 1901.

9.3.8 Microwave Systems.

9.3.8.1 General Requirements. Microwave radio systems shall meet the following minimum requirements:

(1) The microwave radio shall be suitable for two-frequency, full-duplex operation.
(2)* The microwave radio shall be suitable for operating in network configurations offering ring or star protection.
(3) The microwave radio shall include a transmitter, a receiver, a modem, a power supply, an automatic switching device, a multiplexer, service channels/orderwire, and all associated interconnections.
(4) The microwave radio shall allow full access to all modules for normal system maintenance.
(5) All replaceable/plug-in modules shall be accessible.

9.3.8.2 Recovery and Protection.

9.3.8.2.1 Receivers shall provide both manual and fade initiated automatic errorless switching.

9.3.8.2.2 Recovery of a system from RF signal loss shall take place within 250 milliseconds after a valid signal is restored.

9.3.8.2.3 The system shall be designed so that protection circuits and units not in service or operation can be tested and repaired without affecting on-line system operation.

9.3.8.2.4 Partial or complete failure of protection control or switching equipment shall not render the microwave link inoperable.

9.3.8.3 Electromagnetic Interference.

9.3.8.3.1 The microwave equipment shall be operationally compatible with public safety communications equipment co-located in the same equipment location.

9.3.8.3.2* The microwave equipment shall be capable of meeting full specifications when operating in the vicinity of commercial AM and FM radio and TV transmitters.

9.3.8.4 Environmental Considerations. Microwave systems equipment shall function properly in the environmental conditions and at altitudes in which it is installed.

9.3.8.5 Microwave System Network Management.

9.3.8.5.1* General. The microwave system shall have sufficient alarm, control, and metering capabilities to detect defective or failing components.

9.3.8.5.2 Fault and Failure History Log.

9.3.8.5.2.1 The microwave radio shall maintain an electronic file that records the date and time of all fault and failure conditions and switching actions.

9.3.8.5.2.2 The file shall be downloadable for on-site review and electronic communications to others.

9.3.8.5.3 Fault and Failure Indications. Fault and failure conditions shall be displayed at the site and at a remotely monitored location.

9.3.8.5.4 External Alarms. Each microwave radio assembly shall accommodate external site/housekeeping alarm inputs.

9.4 Radio Alerting Systems.

9.4.1 General.

9.4.1.1 Radio alerting systems shall include one or more of the following:

(1) Voice receivers
(2) Coded receivers
(3) Noncoded receivers
(4) Numeric receivers
(5) Alphanumeric devices
(6) Two-way alphanumeric devices

9.4.1.2 Where radio home alerting receivers, portable radios, pagers, and similar radio devices are used to receive alarms or are used on-scene, they shall conform to the requirements of this standard.

9.4.1.3 Where portable two-way radio equipment is used to receive fire alarms, such units shall be equipped to receive a coded alert.

9.4.2 Radio Paging Systems and Pagers.

9.4.2.1* The paging system shall be under the direct control of the AHJ where used as a method of emergency dispatch.

9.4.2.2 No part of the paging system shall utilize the public Internet for any portion of its operation when used as a method of emergency dispatch.

9.4.2.3 Page-encoding equipment shall be located in the communications center where used as a method of emergency dispatch.

9.4.2.4 The paging system shall comply with the general requirements for radio systems as outlined in this document.

9.4.2.5 Pagers shall audibly indicate a low-battery condition.

9.4.2.6 Alphanumeric pagers shall support the maximum text message that can be sent from the communications center.

9.4.2.7* Coded receivers shall audibly indicate the presence of an unacknowledged message.

9.4.2.8 Alphanumeric devices and two-way alphanumeric devices shall audibly indicate the presence of an unread message.

9.4.2.9 Two-way alphanumeric devices shall automatically transmit an acknowledgment when the device has received and stored a message.

9.4.2.10 Two-way alphanumeric devices shall automatically transmit an acknowledgment when the responding user has read the message.

9.4.2.11* Two-way alphanumeric devices shall be capable of providing and transmitting multiple-choice replies, manually selected by the user.

9.4.2.12* Status of the two-way alphanumeric devices, including messages sent and acknowledged, shall be monitored in the operations room.

9.4.3* Alerting Receivers. Where radio alerting receivers are used to receive emergency dispatch messages, they shall be provided with two sources of power.

9.5 Outside Audible Alerting Devices.

9.5.1 Outside audible alerting devices used to indicate an emergency shall be located to alert all emergency response personnel expected to respond.

9.5.2 Coded alerting devices shall operate at speeds of at least one actuation per second, with three or four rounds of coded signals required where outside alerting devices are operated for summoning emergency personnel.

9.5.3 Compressed air alerting devices shall have a distinctive tone. If coded, the duration of the blast shall be neither less than ½ second nor longer than 1½ seconds, with silent intervals of 1 to 1½ times the blast duration.

9.5.3.1 Storage tanks shall meet the following criteria:

(1) Storage tanks shall comply with ASME specifications for unfired pressure vessels.
(2) Storage tanks shall be equipped with safety relief valves.
(3) Storage tank size shall be such that, at 85 percent of working pressure, eight times the largest number of blasts assigned to any signal but not fewer than 50 blasts shall be capable of being sounded.

9.5.4 Compressors shall have the capacity to fill storage tanks to working pressure within 30 minutes.

9.5.4.1 Piping of ferrous materials shall be provided with scale traps that are accessible for cleaning.

9.5.4.2 All piping shall be arranged to allow inspection and repair.

9.5.5 IP Devices. Where adopted by the AHJ, IP-enabled devices (e.g., smartphones, tablets, laptops) shall comply with the rules and regulations governing wireless communications in the country of operation.

9.5.5.1 The communications center shall be equipped for IP-enabled two-way communications with the ERUs using IP-enabled devices as determined by the AHJ.

9.5.5.2 IP-enabled devices shall be capable of fully charging the battery while in use.

9.6 Two-Way RadioCommunications Enhancement Systems.

9.6.1 All system components shall be designed, installed, tested, inspected, and maintained in accordance with the manufacturers' published instructions and the requirements of Section 9.6.

9.6.2 Pathway survivability levels shall be as described in Section 5.10. [**72:**24.3.13.1]

9.6.2.1 Two-way radio communications enhancement systems shall comply with 9.6.2.1.1 through 9.6.2.1.4. [**72:**24.3.13.8]

9.6.2.1.1* Where a two-way radio communications enhancement system is used in lieu of a two-way in-building wired emergency communications system, it shall have a pathway survivability of Level 1, Level 2, or Level 3. [**72:**24.3.13.8.1]

*Exception: Where leaky feeder cable is utilized as the antenna, it shall not be required to be installed in metal raceway. [**72:***24.3.13.8.1]*

9.6.2.1.1.1 The feeder and riser coaxial cables shall be rated as plenum cables that match the building's fire rating and pathway survivability.

9.6.2.1.1.2 The feeder coaxial cables shall be connected to the riser coaxial cable using hybrid coupler devices of a value determined by the overall design. [**72:**24.3.13.8.1.2]

9.6.2.1.2 Where a two-way radio communications enhancement system is used in lieu of a two-way in-building wired emergency communications system, the design of the system shall be approved by the AHJ. [**72:**24.3.13.8.2]

9.6.2.1.3* Riser coaxial cables shall be rated as riser cables and routed through a 2-hour–rated enclosure. [**72:**24.3.13.8.3]

9.6.2.1.4 The connection between the riser and feeder coaxial cables shall be made within an enclosure matching the building's fire rating and pathway survivability, and passage of the feeder cable in and out of the enclosure shall be fire-stopped to the building's fire rating and pathway survivability.

9.6.3* Systems shall have lightning protection that complies with NFPA 780.

9.6.4 Systems that are used to comply with the requirements of Section 9.6 shall be tested in accordance with 11.3.9 and 11.3.9.1.

9.6.5 Non-Interference and Non-Public Safety System Degradation.

9.6.5.1 No amplification system capable of operating on frequencies or causing interference on frequencies assigned to the jurisdiction by the licensing authority of the country of jurisdiction shall be installed without prior coordination and approval of the AHJ.

9.6.5.2 The building manager/owner shall suspend and correct equipment installations that degrade the performance

of the public safety radio system or public safety radio enhancement system.

9.6.5.3 Systems that share infrastructure with non-public safety services shall ensure that the coverage and performance of the public safety communications channels are not degraded below the level of performance identified in 9.6.7 and 9.6.8, regardless of the amount of traffic carried by the non-public safety services.

9.6.6 Approval and Permit.

9.6.6.1 Plans shall be submitted for approval prior to installation.

9.6.6.2 At the conclusion of successful acceptance testing, a renewable permit shall be issued for the public safety radio enhancement system where required by the AHJ.

9.6.7* Radio Coverage.

9.6.7.1 Radio coverage shall be provided throughout the building as a percentage of floor area as specified in section below through section on amplification components.

9.6.7.2 The system shall adhere to the maximum acceptable propagation delay standard provided by the AHJ.

9.6.7.3 Radio coverage shall be determined by the AHJ.

9.6.7.4 Critical Areas. Critical areas, including fire command centers, fire pump rooms, exit stairs, exit passageways, elevator lobbies, standpipe cabinets, sprinkler sectional valve locations, and other areas deemed critical by the AHJ, shall be provided with 99 percent floor area radio coverage.

9.6.7.5 General Building Areas. General building areas shall be provided with 90 percent floor area radio coverage.

9.6.7.6 Amplification Components. Buildings and structures that cannot support the required level of radio coverage shall be equipped with a system that includes RF emitting devices that are certified bythe radio licensing authority to achieve the required adequate radio coverage.

9.6.8* Signal Strength.

9.6.8.1* Inbound. A minimum inbound signal strength sufficient to provide usable voice communications, as specified by the AHJ, shall be provided throughout the coverage area. The inbound signal level shall be sufficient to provide a minimum of DAQ 3.0 for either analog or digital signals.

9.6.8.2 Outbound. A minimum outbound strength sufficient to provide usable voice communications, as specified by the AHJ, shall be provided throughout the coverage area. The outbound signal level shall be sufficient to provide a minimum of DAQ 3.0 for either analog or digital signals.

9.6.9 Isolation. If a donor antenna exists, isolation shall be maintained between the donor antenna and all inside antennasto a minimum of 20 dB under all operating conditions.

9.6.10 System Radio Frequencies. The public safety radio enhancement system shall be capable of transmitting all radio frequencies, as required by the AHJ assigned to the jurisdiction, and be capable of using any modulation technology in current use by the public safety agencies in the jurisdiction.

9.6.10.1 List of Assigned Frequencies. The AHJ shall maintain a list of all inbound/outbound frequency pairs for distribution to system designers.

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

9.6.11 System Components.

9.6.11.1* Component Approval. RF emitting devices and cabling used in the installation of the public safety two-way radio communications enhancement systems shall be approved by the AHJ, and all RF emitting devices shall have the certification of the radio licensing authority and be suitable for public safety use prior to installation.

9.6.11.2 Component Enclosures. All repeater, transmitter, receiver, signal booster components, external filters, and battery system components shall be contained in a NEMA4- or NEMA4X-type enclosure(s).

9.6.11.3 RF Emitting Devices. RF emitting devices shall meet the following requirements in addition to any other requirements determined by the AHJ:

(1) RF emitting devices shall have the certification of the radio licensing authority prior to installation.
(2) All RF emitting devices shall be compatible with both analog and digital communications, as required to be used by the radio licensing authority and the AHJ, simultaneously at the time of installation.

9.6.12 Power Supplies. At least two independent and reliable power supplies shall be provided for all RF emitting devices and any other components of the system: one primary and one secondary.

9.6.12.1 Primary Power Source. The primary power source shall be supplied from a dedicated branch circuit and comply with *NFPA 72*.

9.6.12.2 Secondary Power Source. The secondary power source shall consist of one of the following:

(1) A storage battery dedicated to the system with 12 hours of 100 percent system operation capacity
(2) An alternative power source of 12 hours at 100 percent system operation capacity as approved by the AHJ

9.6.12.3 Monitoring Integrity of Power Supplies. Monitoring the integrity of power supplies shall be in accordance with 9.1.2.2.

9.6.13 System Monitoring.

9.6.13.1 Fire Alarm System. The system shall include automatic supervisory signals for malfunctions of the two-way radio communications enhancement systems that are annunciated by the fire alarm system in accordance with *NFPA 72*, and shall comply with the following:

(1) Monitoring for integrity of the system shall comply with *NFPA 72*, Chapter 10.
(2) System supervisory signals shall include the following:
    (a) Donor antenna malfunction
    (b) Active RF emitting device failure

(c) Low-battery capacity indication when 70 percent of the 12-hour operating capacity has been depleted
(d) System component failure

(3) Power supply supervisory signals shall include the following for each RF emitting device and system component:
(a) Loss of normal ac power
(b) Failure of battery charger

(4) The communications link between the fire alarm system and the two-way radio communications enhancement system must be monitored for integrity.

9.6.13.2 Dedicated Panel.

(1) A dedicated monitoring panel shall be provided within the fire command center to annunciate the status of all RF emitting devices and system component locations. The monitoring panel shall provide visual and labeled indications of the following for each system component and RF emitting device:
(a) Normal ac power
(b) Loss of normal ac power
(c) Battery charger failure
(d) Low battery capacity (to 70 percent depletion)
(e) Donor antenna malfunction
(f) Active RF emitting device malfunction
(g) System component malfunction

(2) The communications link between the dedicated monitoring panel and the two-way radio communications enhancement system must be monitored for integrity.

9.6.14 Technical Criteria. The AHJ shall maintain a document of technical information specific to its requirements that shall contain, as a minimum, the following:

(1) Frequencies required
(2) Location and effective radiated power (ERP) of radio sites used by the public safety radio enhancement system
(3) Maximum propagation delay (in microseconds)
(4) List of specifically approved system components
(5) Other supporting technical information necessary to direct system design

Chapter 10 Computer-Aided Dispatching (CAD) Systems

10.1 General.

10.1.1* Computer-aided dispatching (CAD) systems, when required by the AHJ, shall conform to the items outlined in this chapter.

10.1.2* Where a CAD system is used for emergency dispatch service operations, and an enhanced 9-1-1 emergency number telephone system is in use, the CAD system shall contain all hardware and software components necessary for interface with the 9-1-1 system.

10.1.2.1* The CAD interface shall accept a transfer of 9-1-1 emergency call data from the customer premise equipment (CPE) to the CAD system.

10.1.2.2 The CAD system shall be capable of populating a call-for-service data entry form with the 9-1-1 data provided by the CPE.

10.2* Secondary Dispatch Method. Where a CAD system is used for emergency services dispatch operations, a secondary dispatch method shall be provided and shall be available for use in the event of a failure of the CAD system.

10.3 Security.

10.3.1 CAD systems shall utilize different levels of security to restrict unauthorized access to sensitive and critical information, programs, and operating system functions.

10.3.2 The AHJ shall have the ability to control user and supervisor access to the various security levels.

10.3.3 Physical access to the CAD system hardware shall be limited to authorized personnel as determined by the AHJ.

10.3.4 Operation of the CAD system software shall be limited to authorized personnel by log-on/password control, workstation limitations, or other means and audited as required by the AHJ.

10.3.5* CAD systems shall provide network isolation necessary to preserve bandwidth for the efficient operation of the system and processing of alarms.

10.3.5.1 The CAD system shall provide measures to prevent denial-of-service attacks and any other undesired access to the CAD portion of the network.

10.3.5.2 CAD systems shall employ antivirus software where necessary to protect the system from infection.

10.4 Alarm Data Exchange.

10.4.1 The CAD system shall have the capability to allow alarm data exchange between the CAD system and other CAD systems.

10.4.1.1* Alarm data exchange between two PSAPs shall comply with the elements contained in 10.4.1.2 through 10.4.1.7.

10.4.1.2 Alarm data elements for alarm processing shall contain the following items from the sending CAD system:

(1) Street address or intersection of event
(2) Latitude/longitude of event
(3) Reporting party name
(4) Reporting party address
(5) Reporting party callback number
(6) Event type
(7) Any remarks entered to that point

10.4.1.3 The new alarm information shall display as a pending event in the receiving CAD system.

10.4.1.4 The receiving CAD system shall automatically send a confirmation message to the sending CAD system that it received the call.

10.4.1.5 It shall be up to the AHJ to decide whether or not to use or display this information.

10.4.1.6 The sending CAD shall continue to send updates related to the event as needed until the event is terminated by either agency.

10.4.1.7 The sending dispatchers shall be able to send and receive administrative (not tied to an incident) messages to the receiving dispatchers.

10.4.1.8 The sending CAD shall send status changes on all units that the sending CAD has jointly identified to the receiving CAD without dispatcher intervention.

10.4.1.9 The requirements in 10.4.1.3 to 10.4.1.8 shall also apply conversely to the receiving CAD.

10.4.1.10 Each CAD system shall be set up with conversion tables that can translate event types from one system to the other.

10.4.2 The CAD system shall have the capability to allow alarm data exchange between the CAD system and supervising stations.

10.4.3 The CAD system shall have the capability to allow alarm data exchange between the CAD system and 9-1-1 databases.

10.4.4* The CAD system shall have the capability to allow data exchange between the CAD system and other systems as required and approved by the AHJ.

10.4.5 CAD systems that are connected to third-party systems to receive alarms directly shall have agreements in place with the third-party providers to monitor the system for integrity.

10.5 CAD Capabilities.

10.5.1 The installation of a CAD system in emergency service dispatching shall not negate the requirements for a secondary dispatch circuit.

10.5.2 Computer hardware provided as a part of the CAD system shall be of a quality and reliability sufficient to meet the requirements of the AHJ.

10.5.3 All components that are required for the operation of the CAD system ("critical loads") shall be supplied with electrical power through an approved SEPSS *(see 4.10.7.4)*.

10.5.3.1 The SEPSS shall be capable of supporting the critical loads for no less than 60 minutes.

10.5.3.2* The SEPSS shall receive its power from circuit(s) that are automatically connected to the emergency generator, as specified in 4.7.3, in the event of a power failure or insufficiency.

10.5.4 All characters shall be visible in a lighted room without being affected by the glare of ambient lighting.

10.5.5 Printers.

10.5.5.1 The system shall support as many printers as the AHJ deems necessary for its operation.

10.5.5.2 Logging or utility functions shall be assignable to any printer under system control.

10.5.5.3 A spare printer shall be available.

10.5.6* Software that is a part of the CAD system shall provide data entry; provide resource recommendations, notification, and tracking; store records relating to all alarms and all other calls for service and status changes; and track those resources before, during, and after alarms, preserving records of those alarms and status changes for later analysis.

10.5.6.1* The AHJ shall put in place safeguards to preserve the operation, sustainability, and maintainability of all elements of the CAD system in the event of the demise or default of the CAD supplier.

10.5.6.2 The system applications shall function under the overall control of a standard operating system that includes support functions and features as required by the AHJ.

10.5.7 Where the CAD system is a primary or secondary dispatch circuit for ERFs and ERUs, it shall provide an audible notification of alarms and shall be permitted to provide a visual notification of alarms and other calls for service.

10.5.7.1 If voice announcement is used, it shall be preceded by an audible warning or alerting signal that differentiates the alarm or emergency from any other voice messages carried by the system.

10.5.7.2* If text messages are used, they shall be accompanied by audible warning or alerting signal(s) that notify ERF or ERU personnel that an alarm or emergency message has been transmitted.

10.5.7.3 Printers located in an ERF as a part of the dispatch system shall be capable of printing a completed emergency message in less than 30 seconds.

10.6 Performance.

10.6.1* The system shall accommodate the call volume, call types, and other sizing parameters required by the AHJ.

10.6.2 The system shall recommend units for assignment to calls.

10.6.2.1 The system shall ensure that the optimum response units are selected.

10.6.2.2 The CAD system shall allow the telecommunicator to override the CAD recommendation for unit assignment.

10.6.2.2.1 The CAD system shall automatically log that the recommendation was overridden manually by the telecommunicator.

10.6.2.3 The CAD system shall have the ability to prioritize all system processes so that emergency operations take precedence.

10.6.3 The system shall detect faults and failures.

10.6.3.1 The system shall automatically perform all required reconfiguration as a result of the faults or failures.

10.6.3.2 The system shall queue a notification message to the supervisor and any designated telecommunicator positions.

10.6.4* Under all conditions, the system response time shall not exceed 2 seconds, measured from the time a telecommunicator completes a keyboard entry to the time of full display of the system response at any position where a response is required.

10.6.5 The system shall be available and fully functional 99.95 percent of the time, excluding planned maintenance.

10.6.6* The system shall include automatic power-fail recovery capability.

10.7* Backup. The system shall include a data backup system, utilizing either removable media or independent disk storage arrays dedicated to the backup task.

10.8 Redundancy.

10.8.1 The failure of any single component shall not disable the entire system.

10.8.1.1 The CAD system shall provide automatic switchover in case of failure of the required system component(s).

10.8.1.2 Manual intervention by telecommunicators or others shall not be required.

10.8.1.3 Notwithstanding the requirements of 10.8.1.1, the system shall provide the capability to manually initiate switchover.

10.8.1.4 Systems that utilize redundant server and workstation configurationsshall continue from the point where the primary server stopped without requiring a restart of the CAD system or re-entry of the calls in the system at the time of the switchover.

10.8.1.5 Systems that utilize distributed processing, with workstations in the operations room also providing the call processing functions, shall be considered to meet 10.8.1.4, as long as all such workstations are continually sharing data and all data necessary to pick up at the point where the failed workstation stopped are available to all other designated dispatch workstations.

10.8.1.6* CAD systems that are connected to third-party systems to receive alarms directly into the CAD shall have an alternate method of receiving these alarms.

10.8.2 Monitoring for Integrity.

10.8.2.1 The system shall continuously monitor the CAD interfaces for equipment failures, device exceptions, and time-outs.

10.8.2.2 The system shall, upon detection of faults or failures, send an appropriate message to the supervisor and designated telecommunicator positions, accompanied by visual and audible indications.

10.8.3* The system shall log system messages and transactions.

10.8.4 Logs of system messages shall not be modified or erased during the period required by the records retention policy set by the AHJ as defined in Section 12.7.

10.8.5* A spare display screen, pointing device, and keyboard shall be available in the communications center for immediate change-out for every three workstations, or fraction thereof, up to a maximum of three spare display screens, pointing devices, and keyboards.

10.9 Storage Network.

10.9.1 The system shall provide on-line storage that meets all of the functional and performance requirements of this standard for programs and data.

10.9.2 Capacity shall be provided for the storage of a minimum of 100 days of history log data.

10.10 Information Transmittal.

10.10.1 Wired data communications systems that connect ERFs and administrative sites with the system shall communicate at a minimum rate of 56,000 bits per second.

10.10.2 Wireless data communications systems that connect ERFs and administrative sites with the system shall communicate at a minimum rate of 56,000 bits per second.

10.10.3 Mobile units shall communicate with the CAD system at a minimum rate of 9600 bits per second.

10.10.4 The transmission of computer information to mobile units or fixed locations that are associated with emergency operations shall be in accordance with the applicable government rules and regulations for the type of service being used.

10.11 Mobile Data Computers (MDCs).

10.11.1 MDCs and associated equipment shall be manufactured for the environment in which they are to be used.

10.11.2 System Availability.

10.11.2.1 Data communications between CAD and MDCs shall provide the following indications:

(1) Indicate to the telecommunicator that the MDC system is operational
(2) Indicate to the telecommunicator the failure of any message to an MDC
(3) Indicate to the ERU the failure of any message to CAD

10.11.2.2* If communication between MDCs and CAD has failed, messages in transit shall not be lost.

10.11.3 Emergency messages to MDCs shall take priority over other messages.

10.11.3.1 The MDC shall immediately display an indication of an emergency message.

10.11.3.2 The emergency message shall be accompanied by an audible indication from the MDC of sufficient volume to overcome ambient noise.

10.11.3.3 Vehicles equipped with printers shall have the capability to print emergency messages.

10.11.3.4 Displayed emergency messages shall not be automatically replaced by other messages.

10.11.3.5 The MDC shall display emergency information with a minimum use of multipage display.

10.11.4 Nonemergency Messaging.

10.11.4.1 A manual acknowledgment feature shall be provided to indicate that a message sent from the operations room has been viewed.

10.11.4.2 An MDC shall display vehicle status as currently registered within the CAD system.

10.11.5 Equipment and Operation.

10.11.5.1 The MDC shall not require external power to maintain programmed functions.

10.11.5.2 Required connections between the MDC and other essential system components shall be fastened so as to not come loose under normal operating conditions.

10.11.5.3 The MDC shall allow a single action by the operator to initiate an emergency response status change.

10.11.5.4* The MDCs shall provide the following functionality:

(1) The ability to power on and off
(2) A visual indication that the unit is energized
(3) The ability to adjust display intensity
(4) An emergency alert button that transmits a distress signal to the operations room

10.11.5.5 The MDCs shall have a last-in-first-out (LIFO) feature that allows the user to recall the last 10 messages received.

10.11.5.6 Each MDC shall be capable of receiving single, group, or all-call messages.

10.11.5.7 Keyboard.

10.11.5.7.1 The bottoms of detachable keyboards shall have nonskid surfaces.

10.11.5.7.2 The illumination of the keyboard shall be adjustable by the user.

10.11.5.7.3 The keyboard design shall prevent malfunction caused by foreign materials.

10.11.5.7.4 Keyboard malfunctions shall not adversely affect the MDC, the MDC system, the MDC interface, or the CAD system.

10.11.5.8 Display Screens.

10.11.5.8.1 All information shall be visible in direct sunlight conditions.

10.11.5.8.2 The display screen shall be stable and free of unintentional motion.

10.11.5.8.3 Characters shall have a uniform appearance on all parts of the screen.

10.11.5.9 Mobile printers shall provide the following functionality:

(1) The ability to power on and off
(2) A visual indication that the unit is energized

10.12 Integrated Mapping Interface.

10.12.1 The CAD system shall have the ability to interface with a map display system.

10.12.2 The map display system interface shall have the ability to accept spatial positioning data for calls for service and units from CAD.

10.12.3 The map display system interface shall have the ability to position an indicator on the map based on the provided spatial information.

Chapter 11 Testing

11.1 General.

11.1.1 Tests and inspections shall be made at the intervals specified in this standard.

11.1.2 All equipment shall be restored to operating condition after each test or alarm for which the equipment functioned.

11.1.3 Where tests indicate that trouble has occurred anywhere on the system, one of the following shall be required:

(1) The telecommunicator shall take steps to repair the fault.
(2) If repair is not possible, action shall be taken to isolate the fault and to notify the official responsible for maintenance.

11.1.4 Procedures that are required by other parties and that exceed the requirements of this standard shall be permitted.

11.1.5 The requirements of this chapter shall apply to both new and existing systems.

11.2 Acceptance Testing.

11.2.1 New equipment shall be provided with operation manuals that cover all operations and testing procedures.

11.2.2 All functions of new equipment shall be tested in accordance with this chapter and the manufacturers' specifications before being placed in service.

11.2.3 All cables shall be tested in accordance with this chapter where installed with all taps and splices made.

11.2.3.1 Before connection to terminals, cables shall be tested for insulation resistance.

11.2.3.2 Resistance tests shall demonstrate an insulation resistance of at least 200 megohms per mile between any one conductor and all other conductors, the sheath, and the ground.

11.2.4 The frequency, modulation, power output, and receiver sensitivity and selectivity shall be tested and recorded when any radio is installed or repaired.

11.3 Operational Testing.

11.3.1 Wired Dispatch Circuits. Manual test of wired dispatch circuits shall be as follows:

(1) A test shall be performed and recorded at least once every 24 hours.
(2) Circuits for transmission of graphic signals shall be tested by a message transmission.

11.3.2 Power Supply for Wired Dispatch Circuits. Manual tests of the power supply for wired dispatch circuits shall be made and recorded at least once during every 24 hours and shall include the following:

(1) The current strength of each circuit shall be tested, and changes in the current of any circuit that amount to 10 percent of normal current shall be investigated immediately.
(2) The voltage across terminals of each circuit inside terminals of protective devices shall be tested, and changes in the voltage of any circuit that amount to 10 percent of normal voltage shall be investigated immediately.
(3) The voltage between ground and circuits shall be tested as follows:
    (a) Where the test indicates a reading in excess of 50 percent of that shown in the test specified in 11.3.2, the trouble shall be located immediately and cleared.
    (b) Readings in excess of 25 percent shall be given early attention.
    (c) Systems in which each circuit is supplied by an independent current source shall require tests between ground and each side of each circuit that are performed with a voltmeter of not more than 100 ohms resistance per volt.
(4) A ground current reading shall be permitted in lieu of the test specified in 11.3.2, and all grounds that indicate a current reading in excess of 5 percent of the normal line current shall be given immediate attention.

(5) The voltage across common battery terminals on the switchboard side of fuses or circuit breakers shall be tested.
(6) The voltage between common battery terminals and ground shall be tested and abnormal ground readings investigated immediately.
(7) If more than one common battery is used, each common battery shall be tested.

11.3.3 Alerting Means. Outside audible alerting devices, radio, telephone, or other means for alerting emergency response personnel shall be tested as required by the AHJ.

11.3.4 Radio and Voice Amplification Circuits. All primary and secondary radio and voice amplification circuits shall be subjected to a voice test twice daily.

11.3.5 Public Safety Answering Point (PSAP) Telephone Testing. All emergency phone circuits of a PSAP shall be tested daily in accordance with the requirements of the AHJ.

11.3.6 Emergency Lighting. Emergency lighting shall be tested in accordance with NFPA *101*.

11.3.7 Stored Emergency Power Supply System/Uninterruptible Power Supply (SEPSS/UPS). An SEPSS/UPS shall be tested in accordance with NFPA 111.

11.3.8 TDD/TTY. The TDD/TTY system shall be tested daily.

11.3.9* Where two-way radio communications enhancement systems are installed, a system test shall be conducted, documented, and signed by a person approved by the AHJ upon system acceptance and once every 12 months.

11.3.9.1 All testing and maintenance shall be performed in accordance with the requirements of *NFPA 72*.

11.4 Power.

11.4.1 Emergency and standby power systems shall be tested in accordance with NFPA 110.

11.4.2 Weekly discharge tests of the emergency battery power systems shall be performed for 30 minutes to ensure that the batteries are capable of supplying the system with power.

11.4.3 To maximize battery life, the battery voltage for lead acid cells shall be maintained within the limits specified in Table 11.4.3.

11.4.4 To maximize battery life, the following battery-charging voltages shall be used:

(1) Float voltage: 1.42 V/cell ± 0.01 V
(2) High-rate voltage: 1.58 V/cell + 0.07 V – 0.00 V

Table 11.4.3 Battery Maintenance Voltage

Float Voltage	High-Gravity Battery (Lead Calcium)	Low-Gravity Battery (Lead Antimony)
Maximum	2.25 V/cell	2.17 V/cell
Minimum	2.20 V/cell	2.13 V/cell
High-rate voltage	2.33 V/cell	—

Note: High- and low-gravity voltages are +0.07 V and –0.03 V, respectively.

Chapter 12 Records

12.1 General. Complete records to ensure operational capability of all dispatching system functions shall be maintained.

12.2 Installation.

12.2.1 Wired Circuits. Records of wired dispatch circuits shall include the following:

(1) Outline plans that show all terminals in sequence
(2) Diagrams of office wiring
(3) Materials used, including trade name, manufacturer, and year of purchase or installation

12.2.2 Radio Channel. Records of radio dispatch channels and any associated wired circuits shall include the following:

(1) Outline plans that show transmitters and receivers
(2) Diagrams of interconnecting office wiring
(3) Materials used, including trade name, manufacturer, and year of purchase or installation

12.2.3 Changes and Additions. Changes or additions shall be recorded in accordance with 12.2.1 and 12.2.2.

12.3 Acceptance Test Records/As-Built Drawings. After completion of acceptance tests that have been approved by the AHJ, the following shall be provided:

(1) A set of reproducible, as-built installation drawings
(2) Operation and maintenance manuals
(3) Written sequence of operation
(4) Results of all operational tests and values at the time of installation

12.3.1 For software-based systems, access to site-specific software shall be provided to the AHJ.

12.3.2 The AHJ shall be responsible for maintaining the records for the life of the system.

12.3.3 Paper or electronic media shall be permitted.

12.4 Training Records. Training records shall be maintained for each employee as required by the AHJ.

12.5 Operational Records.

12.5.1 Call and dispatch performance statistics shall be compiled and maintained in accordance with Section 7.4.

12.5.2 Statistical analysis for call and dispatch performance measurement shall be done monthly and compiled over a 1-year period.

12.5.2.1 A management information system (MIS) program shall track incoming calls and dispatched alarms and provide real-time information and strategic management reports.

12.5.3 Records of the following, including the corresponding dates and times, shall be kept by the jurisdiction:

(1) Test, alarm, and dispatch signals
(2) Circuit interruptions and observations or reports of equipment failures
(3) Abnormal or defective circuit conditions indicated by test or inspection

12.6 Maintenance Records.

12.6.1 Records of maintenance, both routine and emergency, shall be kept for all alarm-receiving equipment and alarm-dispatching equipment.

12.6.2 All maintenance records shall include the date, time, nature of maintenance, and repairer's name and affiliation.

12.7 Retention of Records.

12.7.1 Records required by Sections 12.2, 12.3, 12.5, and 12.6 shall be maintained for the life of the affected equipment.

12.7.2 Records that are required by Sections 7.4, 7.6, 11.3, and 12.5 shall be maintained for 2 years or as required by law or by the AHJ.

12.7.3 Where call detail recording (CDR) is provided, records shall be maintained for 2 years or as required by law or by the AHJ.

Chapter 13 Data Security

13.1* Data Security Plan. Communications centers shall develop, implement, and utilize a comprehensive defense in depth process and plan to ensure total data security. The defense in depth approach shall encompass people, technology, and operations and shall provide a framework for safeguarding the vital mission of public safety communications centers, including the CAD systems and IP-based NG9-1-1 systems, and the public safety wireless networks used by first responders, including any IP-enabled wireless devices, whether used on public safety or public wireless carrier networks.

13.1.1 The plan shall include the items required by 13.1.2 through 13.1.12.

13.1.2 The plan shall include a policy statement from the AHJ detailing the requirements and goals of the plan.

13.1.3* The plan shall require the assignment of responsibilities for the performance of security functions.

13.1.4* The plan shall specify training and education requirements for employees and shall include a continuing education plan component.

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

13.1.6* The communications center shall implement network security provisions to prevent unauthorized persons from gaining access to the public safety IP network, the public safety phone network, the land mobile radio network, and any other networks that operate within or under the control of the communications center that are required for the receipt or processing of alarms and to prevent unauthorized use of public safety handheld IP-enabled devices used on either a public safety network or a public wireless carrier network.

13.1.7* The communications center shall implement computer security provisions to prevent attacks on the center's computers and servers.

13.1.8* The communications center shall implement software patch management provisions to ensure that all software is periodically updated with the latest improvements to facilitate better security.

13.1.9* The AHJ shall implement data disaster recovery procedures to ensure rapid recovery of databases, servers, and similar equipment used in the communications center, in the public safety wireless network, and for local storage of important information.

13.1.10* The communications center shall implement logging and auditing provisions to allow for the investigation of security or operational problems.

13.1.11* The AHJ shall implement a vulnerability management process to assess periodically the ability of the public safety communications systems, including communications centers, wireless networks, and wired IT networks.

13.1.12* The communications center shall implement environmental and physical security provisions to ensure that it can monitor various physical aspects of the public safety communications system at all locations, such as physical entry, fire or smoke, power supply performance, base radio performance, and other parameters as judged necessary by the AHJ.

13.2* Testing Security. The plan shall include methods and procedures, including schedules, for testing of the system for security breaches or failures, with the frequency of testing to be determined by the AHJ.

13.3 Testing Records. Testing records of the plan shall be maintained in accordance with Section 12.7.

Chapter 14 Public Alerting Systems

14.1 General. Public alerting systems (PASs) shall meet the requirements specified in this chapter.

14.1.1 All PASs and related components shall comply with national, state, provincial, and local rules and regulations governing PASs and related system components.

14.1.2 The AHJ shall develop and maintain standard operating procedures for when and how the systems are to be used.

14.1.3 A PAS that utilizes a communications network(s) developed and used for the purposes of alerting the public shall be engineered to work within the capacity of the network(s).

14.1.4* A PAS utilizing a public alerting system alerting appliance (PASAA) that is part of a communications network used to deliver messages of a nonemergency nature shall be engineered to give priority to the PAS.

14.1.5 An upgrade installed to a PAS shall be backward compatible with existing systems.

14.2 Security.

14.2.1 The AHJ shall develop and enforce security procedures that are consistent with any national, state, provincial, tribal, or local rules and regulations to prevent unauthorized use of the PAS.

14.2.2 The AHJ shall enforce security procedures to prevent the misuse of sensitive information.

14.3* Permitted Uses. Systems shall be used for alerting the public to natural and man-made events, including tornadoes, hurricanes, floods, fire, and chemical releases, that can be

expected to result in loss of life, endanger public health, or destroy property.

14.4 Permitted Systems. The following types of systems shall be permitted:

(1) Automated telecommunications dial-out systems delivering recorded voice messages
(2) Automated telecommunications dial-out systems with signals transmitted to a PASAA
(3)* Radio broadcast systems and tone alert systems using a PASAA
(4) Wireless systems with a PASAA
(5) Paging systems with a PASAA
(6) Siren systems with loudspeakers
(7) Integrated public alert and warning system (IPAWS)

14.5* Public Alerting System Alerting Appliances (PASAAs). PASAAs shall be capable of the following:

(1) Receiving an alert data message (ADM) from a PAS
(2) Providing an audible alert in response to an ADM that meets the audible characteristics of an alarm as defined in *NFPA 72*
(3) Providing a visual alert signal in response to an ADM that meets the following requirement:
    (a) The signal shall be a flashing light that is red, clear, amber, or blue in color.
(4) Providing a local trouble signal in response to a low-battery condition that meets the following conditions:
    (a) The trouble signal shall not use lights of the same color used for other purposes.
    (b) The trouble signal shall have a battery source of power that can serve as either the primary or secondary power supply.
(5) Providing a local visual and/or audible trouble alert that is distinctly different from that used with an ADM, if the PASAA is capable of detecting loss of service or functions

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.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 documents in a broad manner, since 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.3.3.1 Alarm. All incoming calls on designated emergency telephone lines should be considered emergency alarms until answered by a telecommunicator. If a telecommunicator determines that the reason for the call is not an emergency as defined in 3.3.40, the call will not count against the performance requirements of 7.4.2. A trouble or supervisory signal is not an indication of an alarm. *(See also 3.3.105, Trouble Signal.)*

A.3.3.1.1 Alarm Data. Other explanatory information can include, but is not limited to, sensor types, alarm types, and access information.

A.3.3.6 Automatic Location Identification (ALI). Automatic location identification is typically associated with an enhanced 9-1-1 telephone call. ALI can include the civic street address, building, floor, and room numbers and/or the latitude and longitude.

A.3.3.7 Automatic Number Identification (ANI). Automatic number identification is typically used in two disparate systems in emergency communications. First, ANI is a critical component of enhanced 9-1-1, where it identifies the device making the call to 9-1-1. Second, in two-way radio communications, ANI can be associated with the radio device that is active on the voice communication channel.

A.3.3.14 Call Server. *Call server* is a generic term for a centralized, computer application–based telephone system. Call servers are the next generation of private branch exchange (PBX) systems. There are many advantages to using a call server over a legacy PBX, including the ability to add features via modification to the application code and the ability to add extensions using either physical telephones or computer-based clients.

A.3.3.17 Circuit. Specific types of circuits include dispatch, local, and tie circuits.

A.3.3.20 Communications Center. Examples of functions of a communications center are as follows:

(1) Communications between the public and the communications center
(2) Communications between the communications centers, the emergency response agency (ERA), and emergency response facilities (ERFs)
(3) Communications within the ERA and between different ERAs

A.3.3.21 Communications Officer. The position is a function that falls under the logistics section of the incident command system (ICS).

A.3.3.23 Comprehensive Emergency Management Plan (CEMP). In some jurisdictions a CEMP could also be known as a disaster management plan.

A.3.3.24 Computer-Aided Dispatch (CAD). CAD systems have become the preferred method of providing dispatching services. These requirements are intended to ensure that these critical resources are secure, reliable, and redundant.

A.3.3.30 Delivered Audio Quality.

(1) DAQ 1 Unusable: Speech present but not understandable
(2) DAQ 2 Speech understandable with considerable effort: Requires frequent repetition due to noise/distortion
(3) DAQ 3 Speech understandable with slight effort: Requires occasional repetition due to noise/distortion
(4) DAQ 3.4 Speech understandable without repetition: Some noise/distortion present
(5) DAQ 4 Speech easily understood: Occasional noise/distortion present

A.3.3.34 Dispatch Circuit. A dispatch circuit was formerly called an alarm circuit.

A.3.3.40 Emergency. The AHJ of the responding agency can determine which types of alarms qualify as an emergency.

A.3.3.41 Emergency Alarm Processing/Dispatching. This term includes caller interrogation and resource selection [determination of which emergency response unit (ERU) will respond] up to the start of the ERF notification process.

A.3.3.43 Emergency Response Agency (ERA). An ERA includes any public, governmental, private, industrial, or military organization that engages in the operations specified in the definition.

A.3.3.44 Emergency Response Facility (ERF). Examples of ERFs include a fire station, a police station, an ambulance station, a rescue station, a ranger station, and similar facilities.

A.3.3.50 IP-Enabled Device. An IP-enabled device is not a land mobile radio narrowband device; examples include smart phones, tablets, and laptop computers.

A.3.3.62 Multiple Line Telephone System (MLTS). The term *multiple line telephone system* refers to any solution, independent of the technology used, that allows an entity to use a group of voice communication channels from an exchange carrier to connect a multiplicity of end users for inbound, outbound, and intersystem telephone calls. An MLTS includes both PBX- and call server–based solutions, including network-based and premises-based systems (e.g., Centrex, VoIP, as well as PBX, hybrid, and key telephone systems, as classified by the FCC under Part 68 requirements).

A.3.3.64 Notification. Notification can be made by either electronic or mechanical means.

A.3.3.75 Private Branch Exchange (PBX). The PBX system was first developed to allow a private entity to connect the telephone company to many users, breaking the one phone–to–one phone line ratio. Originally, this process was a manual one, in which a switchboard operator would answer an incoming call and, using a physical patch cord, connect the incoming caller to the desired extension. When users wanted to make either an outbound or intersystem call, they first had to notify the switchboard operator and verbally explain their request. As technology progressed, switchboard operators were replaced first by mechanical devices that could interpret a rotary dial and later by dual tone multifrequency (DTMF) "Touch Tone®".

A.3.3.83 Radio Channel. The width of the channel depends on the type of transmissions and the tolerance for the frequency of emission. Channels normally are allocated for radio transmission in a specified type for service by a specified transmitter. [**72,** 2013]

A.3.3.85 Radio Frequency. The present practicable limits of radio frequency (RF) are roughly 10 kH to 100,000 MHz. Within this frequency range, electromagnetic waves can be detected and amplified as an electric current at the wave frequency. *Radio frequency* usually refers to the *RF* of the assigned channel.

A.3.3.88 Remote Communications Facility. Remote communications facilities might be housed in buildings under the control of the AHJ, in buildings not under the control of the AHJ, on high land forms such as mountaintops, and at other locations as necessary to ensure operation of a communications system over a geographic area designated by the AHJ. Remote transmitters, receivers, repeaters, and their associated antennas are frequently found at such facilities. When not housed in a building, equipment is usually located in prefabricated enclosures to provide weather protection.

A.3.3.90 Response Unit. Some examples of response units include patrol car, ambulance, rescue vehicle, pumper, ladder truck, elevating platform, service vehicle, marine unit, supervisor's vehicle, tow truck, motor assistance vehicle, construction equipment, mass transit vehicles, and personnel assigned a unique identification number or name used for dispatches.

A.3.3.94 Standard Operating Procedures (SOPs). In some jurisdictions, SOPs are also known as standard operating guidelines (SOGs).

A.3.3.107 Two-Way Alphanumeric Devices. Two-way alphanumeric devices do not have the capability of providing voice messages.

A.3.3.109 Uninterruptible Power Supply (UPS). A UPS is a solid-state system relying solely on battery power as an emergency source. A static UPS consists of a rectifier (a device for converting ac to dc), an inverter (a device for converting dc to ac, and an energy storage medium, for example, batteries. The inverter in the static UPS also includes components for power conditioning.

A.3.3.110 Voice Communication Channel. The voice communications channel can be physically switched, as with wired circuits, wirelessly switched, as with radio channels; or virtually switched, as with circuits created for voice over Internet protocol (VoIP) network-based circuits.

A.4.1.1 Uninterrupted operation of emergency communications systems is critical to the safety and security of the community at large. In the event of a major natural or manmade disaster, the continued operation of the communications center will be an essential element in maintaining the continuity of government, thereby lessening loss of life and preventing the breakdown of law and order.

Most NFPA documents are written to furnish minimum requirements for the safety to life and property in any given individual building. However, survival and continued functioning of emergency services communications systems are necessary for the health and safety of the entire community. The

emergency services communications systems infrastructure needs to be able to withstand the effects of hurricanes, earthquakes, terrorism, wildfires, blizzards, tsunamis, and other disasters of similar scale. Because of that need, this document contains requirements that in some cases are more stringent than those for an otherwise similar business occupancy.

A.4.1.5 One means of meeting this requirement could be a mutual-aid agreement with another jurisdiction to use its communications center as the alternate center. This is dependent on whether the other communications center has enough capacity to handle the added call volume and enough work stations to accommodate personnel relocated from the evacuated center. It also is heavily dependent on the ability of another jurisdiction's center to transmit and receive on the dispatch frequencies in use at the primary center. Such an agreement should be made in writing.

A.4.1.5.2 The alternate communications center should not be located in close proximity to the primary center. In determining the minimum geographical separation required between the primary communications center and the alternate communications center, the AHJ should evaluate the potential for a single disaster (terrorist attack, flood, tornado, etc.) to render both the primary and alternate centers inoperable. When preparing evacuation and continuity of operations plans, the AHJ should also consider the length of time it will take center personnel to travel under adverse conditions to an unstaffed alternate center and place it in operation.

A.4.1.5.3.2 The CEMP should be exercised on a regular basis to ensure that the plan is workable and that employees are familiar with the procedures. The local emergency planning committee (LEPC) comprises emergency response agency representatives, local government, schools, emergency management personnel, other governmental agencies, and the private sector. The CEMP is developed by this committee and used as part of the planning process in emergency management. *NFPA 1600* also outlines the requirements for emergency planning. The communications center is a critical component of any emergency plan and serves as a link between the emergency operations center (EOC) and ERAs.

A.4.1.5.4 This requirement is intended to ensure that emergency communications systems will continue to operate, even if the primary communications center is completely destroyed.

A.4.1.6 The decision to evacuate or to not evacuate the communications center in the event of a fire or threat of fire is not simple. It involves moving the telecommunicators to a backup dispatch center or to a cooperating agency in a nearby jurisdiction. The communications center should be assigned dedicated fire suppression resources in the event of a fire in the communications center or a fire in the building housing the communications center. Decisions that involve continued operation or evacuation of the center should be made by the fire suppression officer and the telecommunicator supervisor.

A.4.1.8 During the planning and design phases, it is essential that sufficient space be allotted for both personnel and equipment, to enable telecommunicators and supervisors to work efficiently. It is very important to include the users of the facility(ies) in the planning process from its inception. These users include telecommunicators, supervisors, and representatives of each emergency response agency to be dispatched from the center. Fact-finding visits to centers in other jurisdictions should be undertaken. The number of personnel that must be accommodated within the center will be determined by the AHJ in accordance with the requirements of this standard and other factors. Prior to design, a detailed analysis of the tasks to be performed in the operations room is essential. Since electronic equipment will be replaced periodically throughout the life of the center, "swing space" needs to be provided to enable new equipment to be installed and commissioned before older equipment is decommissioned and removed.

A.4.2.2 Consideration should also be given to hazards associated with falling trees, antennas, or other similar structures.

A.4.2.3 When siting communications centers, AHJs should consider increasing this requirement, to above the 500-year floodplain. Over time, 100-year floodplains have tended to expand, and "freak" storms that exceed the 100-year intensity have become more frequent. Therefore, depending on the flood danger in the area, it would be wise to chose a site significantly above the 100-year floodplain elevation.

A.4.3.5 Design consideration for belowgrade centers should include the following:

(1) Special requirements for means of egress
(2) Depth of the local water table relative to the floor elevation
(3) Humidity control
(4) Sumps and pumps having the capacity to prevent flooding under the heaviest possible rainfall
(5) Smoke removal or control systems
(6) Additional backup power needs
(7) Employee morale
(8) Other pertinent issues

A.4.3.8.1 Such facilities can include an on-site drilled water well with pumping facilities provided with both primary and secondary power, and a septic system or adequately sized effluent holding tank. For small centers with few employees, the AHJ might determine that a chemical toilet and adequate stocks of bottled water are sufficient. When relying on bottled water, consideration should be given to the fact that bottled water has an expiration date; therefore, stocks must be renewed accordingly.

A.4.4.1.1.1 The cooling and heating loads of a communications center typically vary significantly, depending on the functions performed in each individual space. Computers, radio equipment, uninterruptible power supplies, and similar equipment typically found in modern communications centers generate a significant amount of heat that needs to be removed to prevent the equipment from overheating and shutting down. On the other hand, that same amount of cooling provided to the operations room, break room, conference rooms, and general office areas will make employees in those normally occupied rooms uncomfortable.

When humans are uncomfortable due to room temperature, their first reaction is to adjust the thermostat. If the same thermostat also controls the amount of cooling provided to sensitive electronic equipment, equipment will overheat and systems failure may result. Therefore, for the reliable operation of the communication systems (as well as comfort and morale of employees), it is essential that individual space temperature controls be provided.

A.4.4.1.2 For communications centers located in multi-use buildings, it is important to avoid drawing contaminants (including smoke from a fire) from other parts of the building

into the center. For these and other reasons, it is necessary to provide the communications center with independent HVAC systems.

A.4.4.1.3 U.S. Army Technical Manual TM 5-602-01, *Utility Systems Terrorism Countermeasures for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*, furnishes additional guidance, which the AHJ might want to consider when planning a new communications center.

A.4.4.1.5 A backup heating, ventilating, and air-conditioning (HVAC) system is needed for use during routine maintenance of the primary system and in the event of a primary system failure.

When HVAC systems fail and no backup is provided, the first casualty is usually security. Doors or windows that are required to be closed are opened, often without the knowledge or consent of the AHJ.

A.4.4.1.7 Examples of equipment include packaged cooling systems and components such as chillers, compressors, condensers, supply air fans, and return air fans.

A.4.4.1.8 HVAC systems that cool essential electronic equipment are equally essential, as loss of cooling will cause equipment to shut down or fail outright. Therefore, backup power needs to be provided for both primary and backup HVAC systems that cool this equipment.

A.4.4.1.9 Air intakes should be installed and maintained in accordance with NIOSH *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*, DHHS (NIOSH) Pub No. 2002-139.

A.4.5.6 A written emergency fire plan should be prepared and posted that assigns specific responsibilities. This plan should be coordinated with all responding emergency agencies. Personnel should receive continuing instructions in at least the following:

(1) Evacuation of personnel and designated assembly area
(2) The operations of all fire-extinguishing and automatic fire detection systems
(3) The use of portable fire extinguishers

A.4.5.7 A damage control plan should provide guidance for the following:

(1) Preventing or minimizing damage to electronic equipment
(2) Preventing or minimizing damage to other operations and equipment

For example, whenever electronic equipment or any type of record is wet, smoke damaged, or otherwise affected by the results of a fire or other emergency, it is vital that immediate action be taken to clean and dry the electronic equipment. If the water, smoke, or other contaminations are permitted to remain in the equipment longer than absolutely necessary, the damage can be grossly increased.

In addition, a means should be provided for preventing water damage to electronic equipment. The proper method of doing this will vary according to the individual equipment design.

(3) Identifying procedures for a return to normal operations

A.4.5.8 Tactical Interoperable Communication Plan (TICP) templates are available at www.safecomprogram.gov.

A.4.6.3 This requirement previously read "Entryways to the communications center that lead directly from the exterior shall be protected by a security vestibule." However, when the center occupies just a portion of a mixed-use building, and the building as a whole provides a lower level of security than required by this standard, it will be necessary to establish a security boundary within the building around the communications center. Therefore the requirement for security vestibules applies to all entrances into the center regardless of whether they are indoor or outdoor entrances. Note that doors that are provided for emergency egress only and cannot be opened from outside the center should not be considered entrances and therefore need not be provided with security vestibules. Also, when the whole building envelope provides the level of security required by this standard, the AHJ might determine that internal security vestibules are not required.

A.4.6.4.5 For instance, a window facing a break area within the secure area assigned solely for the use of the communications center does not require bullet-resistant glass as long as a block wall surrounds the break area.

A.4.6.5 This applies whether the wall in question is provided with windows or not.

A.4.6.7 Refer to the Department of Defense Unified Facilities Criteria (UFC) 4-010-01, *Minimum Antiterrorism Standards for Buildings*; UFC 4-022-02, *Selection and Application of Vehicle Barriers*; UFC 4-023-03, *Design of Buildings to Resist Progressive Collapse*; UFC 4-023-07, *Design to Resist Direct Fire Weapons Effects*; and UFC 4-024-01, *Security Engineering: Procedures for Designing Airborne Chemical, Biological, and Radiological Protection for Building*, for additional guidance.

A.4.7.1.5 This connection provides a quick and safe way to provide power to the communications center during a worst-case scenario power failure. The socket should be physically located to allow easy access for a trailer-mounted generator that would be pulled to the site. The disconnect switch should be of the make-break-make (center-off) type and lockable. Connecting the wiring from the socket between the automatic transfer switch and the electrical distribution panel for the communications center provides a means to get power to the center in case of failure of the transfer switch. When the COPS is supplied by a single generator, all wiring and equipment should be of sufficient ampacity to handle the entire critical load of the center, as determined by the AHJ in accordance with the requirements of Chapter 4.

A.4.7.1.6 An example of control wiring that would be required to receive COPS treatment would be the remote generator annunciation wiring.

A.4.7.4 Engine-driven generators should be sized to supply power for the operation of all critical operating functions of the remote communications facility and for any additional loads determined by the AHJ.

A.4.7.4.3 For large communications centers, a spare generator should be provided so that the center can operate with the largest single generator out of service. This will allow one generator to be taken off line for maintenance and testing without degrading the reliability of the overall system, as well as prevent degradation of communications center function in the event a generator fails during an extended commercial power

outage. For smaller centers where this is not practicable as determined by the AHJ, an exterior weatherproof connection for connection of a mobile (trailer or truck mounted) generator should be provided.

A.4.7.4.12 This is a minimum requirement. The AHJ should consider common local power failure scenarios and historical data on the length of power outages in the jurisdiction to determine if additional fuel storage is required. The possibility of extended power outages due to hurricanes, tornadoes, blizzards, earthquakes, wildfires, and other natural disasters should be considered. As part of the CEMP, the AHJ should evaluate the effect of natural disasters on the ability to resupply fuel tanks during such disasters to determine if additional fuel for operation for more than 72 hours needs to be stored on site. Recent disasters such as Hurricane Katrina have shown that in some cases it could be necessary for communications facilities to operate for a week or more before primary power is restored. In the aftermath of such disasters, roads may be impassable and fuel delivery trucks may have been damaged beyond immediate repair. Under such conditions, it could take many days to resupply fuel.

A.4.7.4.12.1 Commercial distillate fuel oils used in modern diesel engines are subject to various detrimental effects. The origin of the crude oil, refinement processing techniques, time of year, and geographical consumption location all aid in the determination of fuel blend formulas. Sulfur, naturally occurring gums, waxes, soluble metallic soaps, water, dirt, and temperature all begin to degrade fuel as it is handled and stored. These effects begin at the time of fuel refinement and continue until consumption. Proper fuel storage is critical to engine start-up, efficiency, and longevity. Storage tanks should be kept water free and have provisions for drainage on a scheduled basis. Water can contribute to steel tank corrosion and the potential development of microbiological growth where fuel and water interface. Copper and its alloys, along with zinc or zinc coatings, should be avoided in fuel-handling systems. These elements can react with fuel to form certain gels or organic acids, resulting in clogging of filters or further system corrosion. Stable storage temperatures are conducive to fuel health. Tanks that are aboveground and subject to extreme daily temperature variations cause fuel to degrade more rapidly. This is further exacerbated with large aboveground tanks that are less than full. Airspace allows for condensation that can add to the contaminant levels. Reflective exterior tank coatings reduce but do not eliminate the solar heating effect.

Scheduled fuel maintenance and testing help to reduce or nearly eliminate fuel contamination. Fuel maintenance filtration can remove contaminants and water and return fuel to the condition in which it will provide reliability and efficiency for standby generators when in emergency conditions. Fuel maintenance and testing should begin the day of installation and first fill to establish a benchmark guideline for further comparison. Fuel monitoring and testing services are available nationwide from many companies.

A.4.7.6.1 In addition to normal surge protection from electrical and lightning surges that can disrupt the operations of a communications center, other electromagnetic disruptions can also occur. Communications centers that protect very large urban or regional population centers could become a target of enemy military or terrorist attack and might want to consider taking additional measures to protect against an electromagnetic pulse (EMP) event, which could occur as a result of detonation of a nuclear device in the atmosphere. An EMP will create transient high induced surge currents in wires and cables leading into a communications center and could even induce damaging currents inside electronic equipment that is not suitably shielded, such that the equipment will fail. Additional information can be found in a U.S. Army Technical Manual TM 5-690, *Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*, at http://140.194.76.129/publications/armytm/tm5-690/c-5.pdf, The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, *Executive Report*, or at other sources.

A.4.7.7 Additional guidance can be obtained from U.S. Army Technical Manual TM 5-690, *Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*.

A.4.7.8.1 Storage batteries preferably should be located on the same floor as the operating equipment.

A.4.7.8.3 When sizing a UPS, consideration should be given to the potential for increased electrical loads as the center grows over time.

A.4.9 U.S. Army Technical Manual TM 5-811-3, *Electrical Design: Lightning and Static Electricity Protection*, provides additional guidance.

A.4.10.2.2 Consideration should also be given to hazards associated with falling trees, antennas, and other similar structures.

A.4.10.2.4 When siting remote communications facilities, AHJs should consider increasing this requirement to above the 500-year floodplain. Over time, 100-year floodplains have tended to expand, and "freak" storms that exceed the 100-year intensity have become more frequent. Therefore, depending on the flood danger in the area served by the communications center, it might be wise to choose a site above the 500-year floodplain elevation.

A.4.10.3.5 Design consideration for belowgrade facilities should include the following:

(1) Special requirements for means of egress
(2) Depth of the local water table relative to the floor elevation
(3) Humidity control
(4) Sumps and pumps having the capacity to prevent flooding under the heaviest possible rainfall
(5) Other pertinent issues

A.4.10.3.6 A common example of such material is gypsum wallboard.

A.4.10.3.7 Examples of noncombustible floor materials are concrete, aluminum, and steel.

A.4.10.5.4 An example of such a facility is a free-standing, prefabricated or site-built enclosure that houses communications system equipment to protect it from precipitation, extremes in temperature, and vandalism.

A.4.10.5.6 FM Global Property Loss Prevention Data Sheet 9-19, *Bushfire Exposure*, provides additional engineering guidance.

A.4.10.6.4 Such locations could include interior courtyards, light wells, and the like.

A.4.10.6.5 Department of Defense UFC 4-023-07, *Design to Resist Direct Fire Weapons Effects*, provides useful guidance.

A.4.10.6.6 Department of Defense UFC 4-022-02, *Selection and Application of Vehicle Barriers*, provides additional guidance.

A.4.10.6.7 Department of Defense UFC 4-023-03, *Design of Buildings to Resist Progressive Collapse*, provides additional guidance.

A.4.10.6.8 For the more information on central stations, refer to *NFPA 72*. For guidance on intrusion detection systems (IDS) see Department of Defense UFC 4-021-02NF, *Security Engineering Electronic Security Systems*.

A.4.10.7.5 If the public water supply is used for engine cooling, interruption of the supply will cause overheating of the engine and failure of the generator.

A.4.10.7.6 Examples are motorized intake air louvers, fans supplying cooling or combustion air, fuel transfer pumps, and coolant pumps.

A.4.10.7.7.2 Refer to A.4.10.5.4.

A.4.10.7.8 Additional guidance is contained in U.S. Army Technical Manual TM 5-693, *Uninterruptible Power Supply System Selection, Installation, and Maintenance for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*.

A.4.10.8.1.2 During the design of a lighting system for a normally non-staffed facility, consideration should be given to the fact that it is customary for maintenance personnel to bring portable lights with them.

A.4.10.9 U.S. Army Technical Manual TM 5-811-3, *Electrical Design: Lightning and Static Electricity Protection*, provides additional guidance that the AHJ might want to consider.

A.5.1.1 Refer to *NFPA 70*, Section 90.2, for examples of installations that are and are not covered by *NFPA 70*.

A.5.5.2 Environmental conditions could exist that necessitate the use of rigid nonmetallic conduit.

A.5.6.4 Examples of fast-acting surge suppression criteria for power lines can be found in the Telcordia Technologies publication TR-NWT-001011, *Generic Requirements for Surge Protective Devices (SPDs) on AC Power Circuits*. Examples of fast-acting surge suppression criteria for telephone lines can be found in the Telcordia Technologies publication TR-NWT-001361, *Generic Requirements for Gas Tube Protector Units (GTPUs)*.

A.5.8.1 Sensitive electronic equipment includes computers, telecommunications equipment, and two-way radio systems.

A.5.10 The intent of the pathway survivability designation is to provide options for the protection of the pathway circuits and not to create a hierarchical ranking. [**72:**A.12.4]

A.5.10.3 Methods of survivability protection might alternate within a protected premise. For example, 2-hour resistive cable might extend from a 2-hour fire-rated enclosure. [**72:**A.12.4.3]

A.5.10.3(4) A performance-based alternative is needed because it is possible to construct a non-sprinklered, Type V(000) building that employs relocation or partial evacuation (e.g., a single-story ambulatory health care occupancy) that would not warrant either a 2-hour fire resistance–rated enclosure or a 2-hour cable. Examples of performance alternatives that might be considered in a design for survivability are a strategic application of Class A, Class X, or Class N segments and also wireless communication pathways. [**72:**A.12.4.3(4)]

A.5.10.4(4) A performance-based alternative is needed because it is possible to construct a sprinklered single-story Type V(111) or multistory Type II(111) building that employs relocation or partial evacuation (e.g., a health care occupancy) that would not warrant either a 2-hour fire resistance–rated enclosure or a 2-hour cable (a 1-hour enclosure would suffice). Examples of performance alternatives that might be considered in a design for survivability are a strategic application of Class A, Class X, or Class N segments and also wireless communication pathways. [**72:**A.12.4.4(4)]

A.6.2.1 The ability to have access to a telephone system not maintained and operated by the AHJ allows for continuity of communication with ERFs. An AHJ's internal telephone system, using a system such as private branch exchange (PBX), is not considered a commercial telephone system.

A.6.2.2 Such an arrangement is not meant to apply to the office of the chief and other executive officers or to the communications center, which can be housed in an ERF.

A.6.6 Local area network (LAN) computer and telephone cable are examples of communications conductors.

A.7.1.2 In the case of equipment such as repeaters, transmitters, towers, and generators, access needs to be available at all times.

A.7.2.2 The AHJ can develop a certification program or use the certification programs of others. Examples of other certification programs are Associated Public Safety Communications Officials International, International Municipal Signal Association, and National Academies of Emergency Dispatch and Power Phone.

A.7.3.1.1 In jurisdictions receiving fewer than 730 alarms per year (an average of two alarms per 24-hour period), provision of a dedicated telecommunicator might not be necessary where alternate means approved by the AHJ can effect the prompt receipt and processing of alarms in accordance with Section 7.4. Telecommunicator staffing is an important issue in achieving prompt receipt and processing of alarms. Consider the following two concepts of communications center operations:

(1) *Vertical Center*. A single telecommunicator performs both the call-taking and dispatching functions.
(2) *Horizontal Center*. Different telecommunicators perform the call-taking and dispatching functions.

Telecommunicators working in a vertical center are known to engage in multitasking that can inhibit their ability to perform assigned job functions. Routine evaluation of telecommunicator staffing, number of inbound emergency and nonemergency calls, and other operational statistics are necessary to allow a prompt receipt and processing of alarms.

A.7.3.1.2 The processing of N-1-1 calls or other nonemergency 7- or 10-digit calls should not degrade or delay the processing of any emergency calls.

A.7.3.2 The issue of communication capabilities and/or failures is cited by the National Institute for Occupational Safety and Health (NIOSH) as one of the top five reasons for fire fighter fatalities. The importance of an assigned telecommunicator for specific incidents is a critical factor in incident scene safety. The assignment process should be outlined in specific SOPs within each agency represented in the communications center. This assignment process is further assisted when a command/communications vehicle is being staffed at the incident scene.

A.7.3.4 The supervisor position(s) in the communications center are provided in addition to the telecommunicators positions. Although supervisory personnel are intended to be available for problem solving, the supervisor position is permitted to be a working position.

A.7.4.1 Statistical analysis for performance measurement should be completed over a period of 1 month as shown in Figure A.7.4.1(a) and Figure A.7.4.1(b).

A.7.4.2 See Figure A.7.4.1(a).

A.7.4.3 Alarms should be retransmitted to emergency response personnel as soon as the location and general nature of the emergency have been ascertained by the telecommunicator. However, for some alarms involving criminal activity, the safety of emergency response personnel could require the telecommunicator to ascertain additional information from the caller, such as a description(s) of the suspect(s), a description(s) of the vehicle(s), the direction of travel, and the weapon(s) involved, which could make compliance with the 60-second time limit impractical. Therefore, the AHJ for each law enforcement agency served by the communications center should establish time frames for the dispatch of law enforcement personnel in accordance with the corresponding agency's SOPs.

A.7.4.4 See Figure A.7.4.1(b).

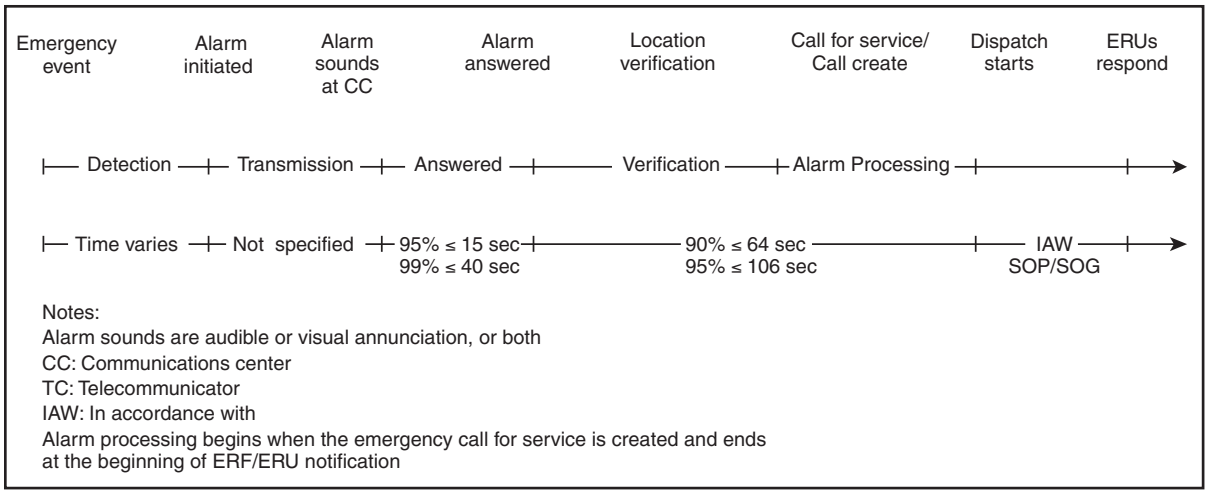

FIGURE A.7.4.1(a) Alarm Time Line Where Primary PSAP Is Communications Center.

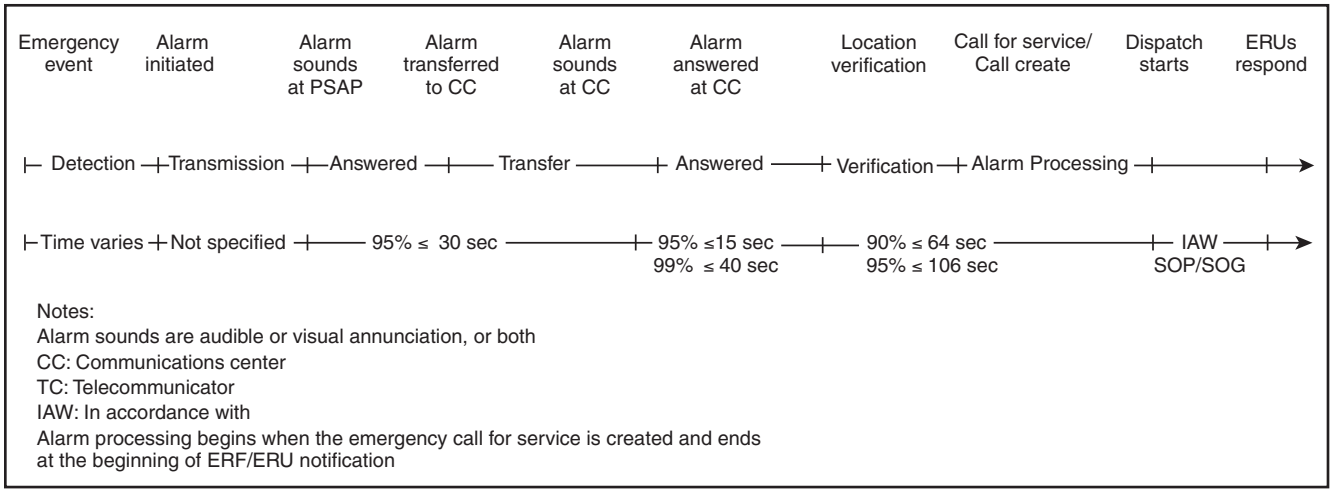

FIGURE A.7.4.1(b) Alarm Time Line Where Primary PSAP Is Other Than Communications Center.

A.7.4.7 The first unit to arrive at an emergency incident is responsible for notifying the communications center by radio of its arrival and for providing a brief description of the conditions observed and the precise location of the incident. The responding officer should report arrival and should establish the initial command post at the emergency. As soon as conditions allow, the incident commander should report supplementary information to the communications center and should make additional progress reports if operations keep the units at the emergency longer than a few minutes. An extended or complex emergency incident can necessitate the use of a communications unit for effective coordination, command, and control.

A.7.4.8 The audible warning or signal is typically a distinctive tone.

A.7.4.10 The assignment of a communications officer/unit leader to incidents that are more complex ensures that adequate communication is achieved using available telephone and radio systems. Such an assignment also ensures that the availability of existing frequencies or networks is maximized and that system overloading is minimized. An assigned communications officer can be particularly important and useful during multi-agency fires and other incidents. It can be necessary to establish specific nets and monitoring systems to guarantee communications in some situations. In complex incidents, communications discipline is critical in avoiding system overload.

A.7.4.11 The common emergency organization, that is, the incident management system (IMS), includes two important communications concepts as follows:

(1) *Common Terminology.* All participating departments and agencies use clear text and established standard terms and phrases. In multi-agency emergencies, it is extremely difficult to guarantee that all agency and department codes represent identical meanings. To avoid potential misunderstandings between telecommunicators, the IMS requires clear text or plain language for all radio messages. Although this is a significant departure from public safety agency tradition, it has been found to be efficient in actual practice.
(2) *Integrated Incident Communications.* Participating departments and agencies plan in advance for the use of integrated radio frequencies to tie together all tactical and support units assigned to an incident. To ensure the best possible use of all participating department and agency radios at major incidents, an Incident Radio Communications Plan matrix is developed. The matrix lists all available radio systems on an incident and aids in assigning them to provide command, tactical, and logistical coverage for a complete operation.

Preparation of the matrix necessitates training and a knowledge of cooperating department and agency frequencies and radio components. Use of the matrix is greatly enhanced by the existence of a frequency-sharing agreement. *(See Annex B.)*

The Federal Communications Commission (FCC) has no prohibition against public agencies sharing frequencies during emergencies, provided that the responsible agency has granted permission to assisting agencies to do so. The agreement specifies the mutual permission of participating agencies to use other agency frequencies when providing assistance. The agreement lists the terms and conditions of use by others and includes all frequencies that can be made available under critical conditions. Such agreements facilitate better multiagency dispatching and incident communications and can be prepared by groups or agencies who work together frequently.

A.7.4.11.2 These communications links can include but are not restricted to a number of methodologies, including radio, data communication, face-to-face, satellite communication, or telephone. Such communication links permit units from multiple agencies to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results. These links permit communications between agencies when needed but not necessarily with every unit involved at an incident at all times.

A.7.4.11.2(3) Extended operations can include long-term disaster recovery, security at major events, or criminal justice surveillance.

A.7.4.15 Effective communication among emergency response personnel during the initial response to any major incident and throughout its extended operations has a significant impact on the rapid mitigation to the affected population.

A plan should lend itself to rapid activation in case of an incident. These incidents include major storms, conflagrations, hazardous materials incidents, wildland fires, mass transit accidents, domestic terrorism, and other incidents that can overwhelm the agencies serving the community and their normal resources.

The plan should include all agencies that normally would be utilized to mitigate any major incident. The plan should also include the communication integration of all agencies into a command structure. Additionally, the plan should include the communications path for transition to the next level of support.

The plan should include SOPs that outline the following:

(1) Activation of such plan
(2) Radio systems to be utilized
(3) Assigned radio frequencies and bandwidth for conventional or trunked systems
(4) Talkgroups
(5) Unit/agency designations
(6) Talk paths to be utilized (e.g., gateway, cross band repeaters, and telecommunicator assisted)

The plan should define applicable continuous tone-coded squelch system (CTCSS) codes, in compliance with TIA-603-D, *Land Mobile FM or PM — Communications Equipment — Measurement and Performance Standards,* for analog channels designated for interoperability.

The plan should define interoperability channels designated for digital operation. These channels should be compliant with TIA/EIA-102.BAAA, *Common Air Interface.*

A.7.4.15.1 The key to the successful operation of the various resources into a region depends heavily upon the ability of all public safety agencies to communicate effectively with each other in real time. At a minimum, interoperability should be supported at the command level. It is not required that every responder have total interoperability with every other responder.

A.7.4.15.2 Exercising this plan identifies areas that need improvement.

A.7.4.18 Procedures for handling telecommunication relay services (TRS) calls should be included in the SOPs.

A.7.6.1(3) Recording by telecommunicator position, rather than by line, allows all telephone lines that are used in the communications center to be taped using a minimum of recorder resources.

A.7.7 The purpose of the quality assurance program is to follow up and review calls with communications center employees, improve procedures, and make the corrections needed to improve service and response. Generally accepted statistical methods should be used when selecting calls for review.

A.8.1 Cellular or Internet personal communications services (PCS) systems include such devices as personal digital devices, advanced voice and data devices, and other cellular-based wireless systems. Text messaging, Internet access, cable modems, and other devices using wireless fidelity (WiFi) all use voice over Internet protocol (VoIP).

A.8.2.1.2 The separate business number listed in the telephone directory and used for nonemergency purposes should terminate at a location where personnel are on duty at least 40 hours per week, Monday through Friday.

A.8.2.3.6 A telephone line terminating at an unstaffed ERF and provided with a recorded message should not be used to meet the intent of the business line (nonemergency) listed in the directory and assigned for business (nonemergency) use as specified in 8.2.3.4.

A.8.3(1) In no case is it ever recommended that the telephone system be designed at less than P.01 GOS. An industry standard traffic study should be conducted that meets the public safety requirements of the AHJ.

A.8.3.4 The monitoring service is to be provided by the 9-1-1 vendor. Monitoring at the communications center itself is not sufficient, since a failure at the communications center can also involve a failure of the monitoring and also does not cover situations where 9-1-1 calls are not completed due to cable failure or intermediate central office failure.

A.8.3.5 Automated voice alarms, by their design, repeat their message many times and, therefore, can monopolize an inbound line for a considerable time. Therefore, they are not permitted to connect with published emergency numbers, and their use is not encouraged. Many state and local statutes prohibit such connections to designated emergency lines or to 9-1-1.

A.8.4.3.1 Call delivery paths can include analog as well as IP call delivery.

A.8.4.3.2 Two circuits run in the same conduit, duct bank, or trench or run on the same pole line do not provide the level of safety intended by the committee.

A.8.5.1 See *NFPA 1600* for additional guidance.

A.8.5.4(2) The AHJ can approve a queuing system for calls on emergency lines. Such systems often require the additional approval of regional, county, or state authorities.

A.8.6.1 The MLTS must be programmed to allow a user to dial 9-1-1 without first having to dial 9 or any other number to reach the public switched telephone network. For example, 9-9-1-1 is not permissible.

A.8.6.2 The dialable number is used by the Public Safety Answering Point to call the 9-1-1 caller back in the event more information is needed or a call is dropped before sufficient information is obtained to initiate a dispatch.

A.8.6.3 There are multiple methods to meet this requirement. Incumbent and competitive local exchange carriers offer private switch ALI, commonly known as PS/ALI services. PS/ALI allows the MLTS owner to manage the location associated with the extension's telephone number. In addition, commercial services are available to both automate and act as an MLTS agent in providing and maintaining ALI for extensions that have both static and dynamic locations.

A.8.6.3.1 This matches the location granularity stated within the proposed model MLTS legislation in NENA 06-750 v3, "NENA Model Legislation E9-1-1 for Multi-Line Telephone Systems."

A.8.6.3.2 This matches the location granularity exception stated within the proposed model MLTS legislation in NENA 06-750 v3, "NENA Model Legislation E9-1-1 for Multi-Line Telephone Systems."

A.9.1.1 Communications centers that dispatch for volunteers or paid-call personnel have the responsibility of summoning such personnel at any hour of the day or night. Personnel can be summoned by the use of the telephone or radio, supplementing sirens or horns that provide an outside alarm. Alarms can be telephoned to the central telephone office where the telephone telecommunicator can start a siren or operate an air horn to indicate that there is an alarm. In areas where a communications center is not attended 24 hours a day, telephone companies can provide a telephone line that connects to special telephones that are located in places of business or residences selected by the jurisdiction. The jurisdiction then arranges to activate the alarms. In emergency response agencies that have an emergency response facility desk attendant, the telephone central telecommunicator can call the ERF, and the attendant can sound the outside alarm to call volunteers. If there is a code-sounding siren or air horn, coded signals can be sent. Usually a transmitting apparatus is used to send out the code.

If radio equipment is used, a receiver with selective calling equipment can be placed in the home of each volunteer or call person. Selective signaling is accomplished on a group-call principle, allowing the volunteer or call forces to be divided into several groups that can be summoned as a whole or as individual groups to handle a particular incident. Pagers are commonly used for this purpose, since they can be carried anywhere. Pagers can include either a tone alarm, a voice receiver, or a digital display.

A.9.1.1.3.2 In jurisdictions receiving fewer than 730 alarms per year (average of two alarms per 24-hour period), a second dedicated dispatch circuit might not be necessary.

A.9.1.1.3.3 When an alarm is transmitted to an ERF, it should be audible throughout the ERF, without the time delay caused by a responder going to a telephone instrument, picking up the handset, and then relaying the information to other affected responders.

A.9.1.1.4(2) System elements can include but are not limited to transmitters, transceivers, repeaters, receivers and receiver comparators (where required), microphones, encoders, control circuitry, antennas, and appropriate ancillary devices to

constitute a complete radio system. Audible monitoring for integrity can be accomplished by a receiver in the operations room operating on the dispatch channel providing side tone audio. Visual monitoring for integrity can be accomplished by receiver module indication(s) of audio on the dispatch channel. It is not the intent of this requirement to require duplicate equipment at each ERF for a voice radio primary dispatch circuit.

A.9.1.1.4(4)(a) It is not the intent of this requirement to require a redundant digital data radio transceiver at each ERF, unless the ERF is a location that retransmits the signal to other ERF receivers, transceivers, or pagers. Transceivers designed for wide area coverage do not necessarily meet requirements for redundant transceivers.

A.9.1.1.5.1(2) Where the primary dispatch circuit is provided through a radio system, regardless of whether the system is a conventional radio, a trunked radio, or a microwave radio, the system cannot also be used to provide the secondary means of dispatch.

A.9.1.1.5.1(3)(b) A separate receiver is not required for each ERU.

A.9.1.1.5.1(5) The separate control/relay switching equipment connection ports in the ERF are permitted to connect common audio alerting devices and auxiliary equipment such as audio amplifiers and loudspeakers, ERF response lights, and printer equipment.

A.9.1.1.6 The audible warning or signal is typically a distinctive tone.

A.9.1.2 Portions of any dispatch system circuit can need a metal wire connection, such as a wired cable from a microphone to the transmitter/receiver equipment of a microwave/radio dispatch circuit. Such wired circuit connections in a portion of a radio or telephone dispatch circuit do not constitute a wired dispatch circuit where all transmitting facilities are local to the communications center. Where such connections are between the communications center and one or more remote transmitting or repeater facility sites, a connection between the communications center and the remote facility site does constitute a wired dispatch circuit, requiring monitoring for integrity fault or failure trouble signal annunciation if signal transmission failure occurs.

A.9.1.2.1 Polling or self-interrogation is one of many methodologies that can monitor a dispatch circuit to determine its integrity. Polling allows for remote and automatic querying of dispatch channel elements to verify their functionality periodically when the elements have not otherwise reported a fault or failure. The self-interrogation feature of polling equipment allows the overall system to determine and verify its own integrity.

A.9.1.2.6 Audible and visual indications of faults or failures annunciated to an off-site vendor support center and pager signals of fault conditions to field technicians are ancillary to fault and failure indications being received at the communications center for the telecommunicator and any other location for the AHJ radio system manager, such as a county or regional microwave and radio system operations facility.

A.9.2.1.1 This refers to a Type B Automatic Telegraph System where several box/alarm circuits come into a remote location and pass through concentrator/identifier-like equipment. The signal is sent on to the communications center via a separate tie circuit. It eliminates having to run all box/alarm circuits back to the communications center. *(Refer to NFPA 72, Section 9.5.)*

A.9.3.1.1 Frequencies, their assignment, and the widths of channels are regulated throughout the world. In the United States, the FCC provides this regulation through allocation, licensing, and rules for all except federal government allocations. In Canada, the comparable regulating agency is Industry Canada. The National Telecommunications Information Administration (NTIA), under the U.S. Department of Commerce, performs functions similar to the FCC, but only for federal agencies. Wire, line, and radio communications are subject to FCC rules and regulations, which govern many areas of radio usage known as *service*. Of primary concern to emergency communications systems users are the public safety radio services, which provide for the use of radio communications systems by nonfederal governmental entities.

A.9.3.1.2.2 It is recommended that the system be designed for DAQ of 3.4.

A.9.3.1.3 The communications center should have the ability to monitor all radio communications, including those communications on tactical radio communications channels, where practical. The AHJ should carefully evaluate the various communication solution alternatives available, providing the incident commanders with the appropriate mix of communications capabilities to address their specific scenarios, ranging from a small rural residence to a mammoth concrete and steel structure in an urban downtown area. The AHJ should provide a simplex radio communications channel for use in locations outside the coverage area of any installed radio infrastructure.

If the simplex frequencies selected for tactical use are the same as the output frequencies of any repeaters used by the system, a method of positive lockout of automatic system use of that frequency should be provided, controlled from the responsible telecommunicator workstation.

A.9.3.1.4 The AHJ should provide at a minimum a simplex radio communications channel for use in locations outside the coverage area of any installed radio infrastructure or for off-network operations such as incident tactical communications (e.g., "fireground"). Various communication solution alternatives are available for on-scene tactical communications. If a solution other than simplex analog communications is determined by the AHJ to best address that agency's needs, requiring a simplex analog channel requirement provides a secondary communications choice if for some reason the preferred alternative becomes unusable. This requirement also allows for incidents such as mutual aid scenarios, when responding agencies might utilize a different methodology in their own day-to-day operations. Additionally, the communications center should have the ability to monitor all radio communications, including those communications on tactical radio communications channels, where practical.

A.9.3.1.5 The intent of 9.3.1.5 is to provide flexibility to the AHJ to use trunking, if desired, on the tactical on-scene channel, but there must be the provision of using simplex direct analog mode for any reason it might be required.

A.9.3.1.6 This does not prohibit the use of field-deployed portable repeater systems.

A.9.3.2.3(3) The public Internet is not acceptable because it is not under the control of the AHJ. The use of a commercially available network is acceptable if the network is dedicated to public safety or government-only use.

A.9.3.3.1 Coded squelch systems could utilize a specific tone or digital code, transmitted continuously, simultaneous with the desired message traffic. Examples of such a tone or code are a continuous tone-coded squelch system (CTCSS) and a continuous digital-coded squelch system (CDCSS). Analog trunked radio systems utilize a digital code for system access, specific to that analog trunked system, which accomplishes the same goal.

A.9.3.4.1 In a digital access radio system, all units turned on and unassigned within the radio system coverage area monitor the signaling channel. Talkgroup assignments, emergency assignments, individual signaling calls, and special signal calls are broadcast to all monitoring units on the signaling channel. Requests for service (e.g., talkgroup calls, emergency calls, selective alerting) from unassigned units are transmitted by the requesting unit, as data bursts, to the system on the signaling channel.

A.9.3.4.1.5 While it is possible to find units that will scan both trunked talkgroups and conventional channels simultaneously, there are operational issues that must be understood in such operations. Anytime a mobile or portable unit scans off its home trunked talkgroup to other conventional channels or other trunking talkgroups, the radio runs the risk of missing some or all of new transmissions on the home talkgroup during the time that the radio is off the home trunked talkgroup. For that reason, if user radios cannot afford to miss transmissions on the home trunked talkgroup, either scanning should not be used, or a separate radio should be provided to allow one radio to scan and the other radio to remain on the home trunked talkgroup.

A.9.3.4.1.8 A system manager terminal allows the system supervisor to assign individual or talkgroup priority levels, or both, to all field units. The signaling language is structured so that access to the system is in accordance with the level of priority involved.

A.9.3.4.1.9 The emergency level of priority is intended for use only when immediate communications are necessary to preserve safety or protect life.

A.9.3.4.1.10 Trunked radio systems often are configured with many more talkgroups than can be accommodated by available voice channels. During a system controller failure, radios devolve to particular repeater channels and operate conventionally, which could result in overcrowding or busy channels. The AHJ should require emergency services units to devolve to channels reserved specifically for emergency dispatch.

A.9.3.4.1.11 Handling requests by units that have been involved in recent conversations before processing and assigning channels to units not involved in any recent conversations is intended to keep current conversations from becoming fragmented by any delays that could be caused by a new user request for a channel.

A.9.3.4.1.16 The alert should have a different sound from any other audible alert capable of being generated by the field unit. This enables the end user to determine that the unit is out of contact with the system.

A.9.3.4.1.17 The disabling of a field unit should prevent the unit from monitoring any voice communications on any channel or talkgroup in the system. A disabled unit should not be able to transmit or otherwise join into any voice conversation on the system. This disabling function occurs while the field unit is on the system anywhere within RF coverage. The system should have the capability to automatically search for the unit multiple times, if so requested by the telecommunicator, and indicate when it succeeds in disabling the unit.

A.9.3.4.1.18 Remote talkgroup assignment is also known as dynamic regrouping. The system should include the ability to perform this function manually, as well as with a stored software plan, to allow for the automatic programming of many units into predetermined talkgroups. This preprogramming allows the saved plan to be initiated by the telecommunicator at any future time.

A.9.3.4.1.19 Telephone interconnect, while a popular selling point for trunked radio systems, represents a significant load on the system because it monopolizes one RF channel of the trunked system for the duration of the call. Multiple telephone calls can cause two-way voice users to receive busy indications from the system.

A.9.3.4.1.24 In the design and operation of a trunked radio system, dispatching of alarms has to have priority over all other communications and is equal in priority to emergency messages from the field. For this reason, when units are dispatched over radio, the necessary priority is high enough to require "ruthless preemption," which is the seizure and re-use of channels already in use by other conversations previously defined as lower in priority.

A.9.3.4.2 Digital trunked system subscriber units operating in the United States on the 700-MHz narrowband public safety spectrum and complying with TIA-102.BBAB and TIA-102.BBAC must also comply with ANSI/TIA-102.BAAA in order to operate on the required designated nationwide 700-MHz narrowband interoperability channels.

A.9.3.5 The NFPA 1221 committee is monitoring the development of the nationwide FirstNet project. FirstNet development was established by Congress when it enacted the Middle Class Tax Relief and Job Creation Act of 2012. This act required the development of a nationwide interoperable broadband network to enable all emergency service agencies to have improved data communications utilizing the new LTE broadband commercial technology. At the time this edition of NFPA 1221 was being revised, the development of the FirstNet system was in the preliminary stages. The committee will monitor the development of FirstNet for future inclusion in this standard.

A.9.3.6 The NFPA 1221 committee is monitoring the development of the nationwide FirstNet project. FirstNet development was established by Congress when it enacted the Middle Class Tax Relief and Job Creation Act of 2012. This act required the development of a nationwide interoperable broadband network to enable all emergency service agencies to have improved data communications utilizing the new LTE broadband commercial technology. FirstNet has a website: www.ntia.doc.gov/category/firstnet

A.9.3.6.12 Intrinsic safety (IS) is a protection concept associated with the rating of equipment for operation in potentially hazardous atmospheres. IS ratings take into account the nature

of the explosive atmosphere encountered — Class I being explosive gas atmospheres and Class II being explosive dust atmospheres — and the frequency or interval of the presence of such explosive atmosphere — continuously, intermittently, or abnormally. The frequency or interval of the presence of the explosive atmosphere determines the proper division (Division 1 or Division 2) or zone (Zone 0, Zone 1, or Zone 2) classifications that are applied to a particular IS rating. To determine the appropriate IS rating for portable radios, the AHJ identifies the expected explosive atmospheres likely to be encountered and the expected frequency or interval of the presence of such expected explosive atmospheres.

A.9.3.7 Emergency situations that result from large fires, transportation accidents, floods, severe storms, and other disasters often create a need for a temporary communications center to be located close to the scene of the disaster. Such a need is filled by a communications vehicle, sometimes called a mobile command post. The vehicle, which is a mobile command and control headquarters, serves as the hub from which the activities necessary to control an emergency situation can be directed and coordinated without dependence on the department's fixed communications center. Such activities for the control of emergencies include the efforts of local and outside departments and of other public safety organizations, such as police departments and emergency management agencies, in addition to public utilities. Proximity to the site of the disaster provides communications vehicle personnel and those in command with immediate access to the latest information in situations where changes occur rapidly. In addition, the ready availability of communications provides the means to call for additional help or to inform other jurisdictions of the situation. A communications vehicle should carry a variety of equipment that allows communication with other emergency response agencies, public safety organizations, and utilities. Other equipment that can increase the flexibility of the system includes cellular telephones. Some vehicles can be equipped for mobile relay operation that allows them to pick up transmissions of mobile units and to retransmit them to the communications center at higher power levels or on different frequencies. The communications vehicle can provide the following:

(1) Ability to exchange data messages between vehicles and communications centers or ERFs
(2) Improved command and control by television transmission of emergency activity to communications centers or ERFs
(3) Facsimile transmission of maps, preplans, and other written data
(4) Vehicle tracking and geographical locations, which can include global positioning system (GPS) receivers

A.9.3.8.1(2) A star microwave system is a system in which one central site is common with all microwave paths to multiple locations. See Figure A.9.3.8.1(2)(a).

A ring microwave system is a system in which the individual sites are connected in a linear or circular pattern. See Figure A.9.3.8.1(2)(b).

A.9.3.8.3.2 The intent of this requirement is to ensure that the design of the microwave system takes into account the possible presence of commercial broadcast equipment in the vicinity of the proposed microwave location. The microwave equipment and the commercial broadcast equipment can be co-located on the same physical site with shared or independent antenna support structures. The microwave equipment and the commercial broadcast equipment also can be located in close physical proximity of each other, with independent antenna support structures. In either case, the design of the microwave system at the site has to account for possible interference to and from the commercial broadcast equipment.

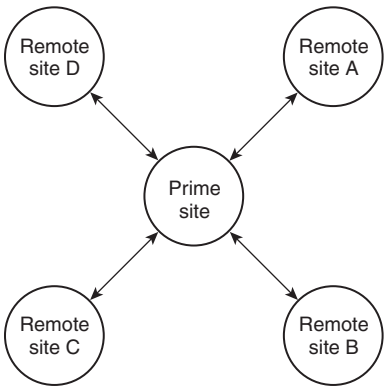

FIGURE A.9.3.8.1(2)(a) Star Microwave System.

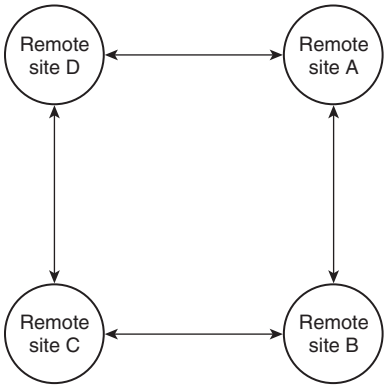

FIGURE A.9.3.8.1(2)(b) Ring Microwave System.

A.9.3.8.5.1 *Components,* in this context, refers to modular elements such as transmitters, receivers, modems, power supplies, switching devices, multiplexers, and service channels/orderwire equipment.

A.9.4.2.1 Paging systems not under the direct control of the AHJ are permitted to be used for administrative purposes but are not considered acceptable for use as a required dispatch system. Third-party paging systems not under the control of the AHJ often do not have the redundant design architecture to comply with 9.1.1.4. Third-party paging systems often rely on satellite communications, which have proved faulty in the past. Third-party paging systems might also employ first-in-first-out (FIFO) hierarchy for message delivery that can cause significant delays during periods of high usage, which is not considered suitable for emergency services communication.

A.9.4.2.7 This feature is implemented with an acknowledge/silence button, so that a user who is not present when the initial alert is received by the device will be prompted regarding the call.

A.9.4.2.11 These pre-programmed pager buttons can be used to notify the operations room that the user is responding, on-scene, or in service following the call.

A.9.4.2.12 The operations room, as the control point for the pagers, should have the ability to monitor the performance of the paging system, as well as the ability to display the messages directed to the telecommunicators.

A.9.4.3 Alerting receivers, sometimes also known as home receivers, can occasionally also be found at emergency responders' places of business. They typically operate from standard wall plug 120 VAC. The devices should include an integral backup battery with charging circuit to maintain operation when normal ac power is interrupted.

A.9.6.2.1.1 Extensive searches and discussions with cable manufacturers have not been able to identify a source of listed 2-hour-rated coaxial or fiber cables. Listed fire-rated 75 ohm coaxial cables for security cameras exist but are not adaptable to distributed antenna systems operating at much higher radio frequencies. Coaxial cable with characteristics similar to low loss 50 ohm, ½ in. (13 mm) diameter, coaxial cables are available in plenum and riser ratings. Past installations have used these plenum and riser rated coaxial cables prior to this Code.

The fiber component of fiber-optic cables melts at temperatures well below the 1825°F (996°C) test specification for listed 2-hour cable.

Using 2-hour-rated cable enclosures throughout each floor of most structures is impractical, especially when added to existing structures.

[**72:**A.24.3.13.8.1]

A.9.6.2.1.3 Examples of 2-hour-rated enclosures could include stairwells and elevator hoistways for first responders–use elevators.

[**72:**A.24.3.13.8.3]

A.9.6.3 U.S. Army Technical Manual TM 5-811-3, *Electrical Design: Lightning and Static Electricity Protection*, provides additional guidance.

A.9.6.7 The use of radio communication enhancement systems has become prevalent throughout the United States. Safety features and flexibilities of radio systems include the following:

(1) Full building coverage is allowed to facilitate communications from any point within the building, in case access to the wires' two-way communications system is compromised.
(2) Communications can be conducted between emergency responders in the field to allow quicker dissemination of safety and emergency information.
(3) Emergency responders typically carry individual radios, allowing the responders to provide information or request assistance individually, which can be important if crew members become separated during an incident.
(4) Radio systems permit "fire fighter or public safety officer down" emergency calls in case of injury — by the push of a single button, a call is placed to a central location to initiate a roll call to determine which emergency responder has been injured and requires assistance. Radio systems can employ an emergency call where, by the push of a single button, an emergency responder call can be given prioritized system access to allow wide-range communication.
(5) The AHJ can determine whether the in-building coverage is for tactical on-site communications, for communications to an off-site dispatch center, or both.

A.9.6.8 Many radio systems are in use by public safety agencies in the United States. A number of them have different operational characteristics. A prescribed signal strength measurement might not produce usable voice communications for all systems (VHF, UHF, 700/800 MHz, analog, P-25, 4 slot TDMA, 2 slot TDMA, etc.). Requiring the AHJ to provide operational parameters required for usable voice communications for the systems in use eliminates possible confusion regarding the specified value, as determined by the AHJ. A better indicator of proper system performance and coverage is to use the DAQ audio quality measurement system whether the signals are either analog or digital.

A.9.6.8.1 It is recommended that systems be designed for DAQ 3.4.

A.9.6.10.2 There is an ongoing national effort to eliminate current interference issues between cellular carriers and public safety bands in the 800-MHz band. This effort could revise the actual frequencies for public agencies within this band. The public safety radio enhancement system design should be capable of being changed to accommodate updated frequencies to allow maintenance of the minimum system-design criteria. Two-way radio communication enhancement systems that are used to comply with the requirements of Section 9.6 shall be tested in accordance with 11.3.9and 11.3.9.1.

A.9.6.11.1 Radio licensing authorities in some countries have distinctions between consumer-grade and industrial-grade two-way radio communications enhancement systems. The intent of these distinctions is to ensure that industrial grade devices are used in public facilities, instead of consumer devices, which are usually held to a lower technical standard, and may not be required to be certified by or registered with the radio licensing authority. The AHJ should become cognizant of these differences operating in his or her country and jurisdiction, and be certain that the devices used in his or her system are suitable to the purpose of a system used and depended upon by public safety users. For example, in the United States, the FCC published *Use and Design of Signal Boosters Report and Order 13-21*, which took effect in March 2014, and established requirements for consumer-grade and industrial-grade signal boosters. Additionally, under FCC regulations, some industrial signal boosters are Part 90 signal boosters used for public safety land mobile radio systems (as opposed to those used for public cellular wireless carriers), which include type A signal boosters (channelized) and type B signal boosters (broadband). Type B devices must be registered with the FCC before being used because of the potential for broadband devices to cause interference if improperly installed.

A.10.1.1 The AHJ should consider the performance requirements of this standard, particularly the time requirements of Section 7.4, in their decision making regarding the use of CAD.

A.10.1.2 This will provide a seamless transition so that call tracking will be complete from the call receipt phase through the dispatch phase, permitting the performance objectives in Section 7.4 to be fully measured. The AHJ should work with the telecommunications providers to ensure that all data elements required by the CAD are provided by the 9-1-1 system.

A.10.1.2.1 The CAD system should be capable of accepting text-based emergency call data. Where such ability is provided, the CAD system should incorporate the text-based emergency call data into the CAD call-for-service record.

A.10.2 A secondary dispatch method can include a separate isolated system, a manual system, printed backup books, visual display boards, or other methods as approved by the AHJ.

A.10.3.5 There is a danger that routine traffic and unintended network faults can affect the ability of critical parts of the CAD system to communicate with each other, unless the CAD system and any other critical dispatch system components are segregated from the general network and a strict screening program is in place to protect the CAD.

A.10.4.1.1 Other data elements that could be used, based on the functionality needed by the AHJ, are the following:

(1) Units responding from sending agency
(2) Status changes from units (ongoing)

A.10.4.4 Other systems could includeintelligent transportation systems, SMART building management systems, pre-fire/pre-incident software systems, and so forth.

A.10.5.3.2 Insufficiency can be the result of a brownout (defined as a condition where the voltage supplied to the system falls below the specified operating range) or the loss of one or more but not all of the phases of the power supply.

A.10.5.6 Resources can include but are not limited to ERUs, individuals, equipment, or other assets.

A.10.5.6.1 Examples of safeguards include placing source code, documentation, and flow charts into escrow.

A.10.5.7.2 The requirements for audible notification for all text message activations regarding alarms or other emergencies apply even if there are other methods of notification installed and used at the ERF.

A.10.6.1 Memory storage, random access memory (RAM), network throughput, etc., should accommodate the call volume, call types, and other sizing parameters that are required by the AHJ.

A.10.6.4 The 2-second requirement envisions a worst-case scenario with a heavily loaded system during the busiest periods. Response time under average conditions should be much less.

A.10.6.6 A power-fail recovery capability is the ability of the system, upon restoration of power, to reboot and arrive at its previous state. This allows restoration of system function without requiring telecommunicators to leave their positions.

A.10.7 Backups can be accomplished on tape, DVD writer, or disk storage arrays in a redundant array of independent disks (RAID) configuration. The AHJ should establish a schedule for the routine backup of data as well as periodic testing of the stored data system for effectiveness and completeness. Incorporating multiple backup methods is preferred, augmented by off-site storage of backup files.

A.10.8.1.6 Examples are commercial alarm monitoring centers and telematics centers. An alternate method of receiving alarms is needed in the event the system fails. This can be a telephone, a memorandum of understanding (MOU) with another PSAP, or even a duplicate system within the PSAP.

A.10.8.3 The AHJ should determine the data required to be logged for use by the operations room.

A.10.8.5 For the purpose of this subsection, any administrative display screens and keyboards beyond those required for telecommunicator workstations that are not considered essential to the receipt and dispatch of emergencies could be considered as spare display screens and keyboards.

A.10.11.2.2 Store and forward technology can provide this functionality.

A.10.11.5.4 Additional functionality could include the ability to download updates for the MDC operating system and applications using a wireless data communication system that is secure in accordance with the provisions of Chapter 13.

A.11.3.9 Test Procedures. The test plan should ensure testing throughout the building. Test procedures should be as directed by the AHJ.

Note: Testing procedures typically are done on a grid system. A grid is overlaid onto a floor area to provide 20 grid cells. Grid cells are provided with definite minimum and maximum dimensions. For most buildings, using a minimum grid dimension of 20 ft (6.1 m) and a maximum grid dimension of 80 ft (24.4 m) will suffice to encompass the entire floor area. Where a floor exceeds 128,000 ft^2 (11,900 m^2), which is the floor area that can be covered by the maximum grid dimension of 80 ft (24.4 m), it is recommended that the floor be subdivided into sectors each having an area less than or equal to 128,000 ft^2 (11,900 m^2), and each sector be tested individually with 20 grid cells in each sector. Signal strength measurements should be taken at the center of each grid and should be performed using standardized parameters as specified in the note in 0.3.9.4. The delivered audio quality (DAQ) scale is a universal standard often cited in system designs and specifications, using the following measures:

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

The DAQ scale comes from TIA TSB-88, *Wireless Communications Systems Performance in Noise and Interference-Limited Situations*. A DAQ test is preferred to absolute RF signal levels for two reasons: the DAQ test is easier to administer than RF signal levels, and DAQ is useful regardless of the type of modulation or system technology used (analog or digital). It measures what really matters — how the signal sounds to the user — regardless of manufacturer specifications.

The minimum allowable DAQ for each grid cell typically is three. Not more than two nonadjacent grid cells should be allowed to fail the test. In the event that three of the areas fail the test, or if two adjacent areas fail the test, in order to be more statistically accurate the testing grid resolution should be doubled. This would require decreasing the size of the grids to one-half the dimension used in the failed test to a minimum of

10 ft (3 m) and a maximum of 40 ft (12.2 m). Further, to cover the same floor area, the number of grids is quadrupled to 80 grids. No more than eight nonadjacent and/or five adjacent grid cells should then be allowed to fail the test.

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

Measurement Parameters. DAQ levels should be measured to ensure the system meets the criteria of 9.6.7 according to parameters as directed by the AHJ.

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

(1) Receive antennas of equal gain to the agency's standard portable radio antenna, oriented vertically, with a centerline between 3 ft to 4 ft (0.9 m to 1.2 m) above floor
(2) Levels recorded while walking an "X" pattern, with the center of the pattern located approximately in the center of each grid area
(3) The linear distance of each side of the "X" equal to at least 10 percent of the length of the grid's side and a minimum length of 10 ft (3 m)
(4) Measurements sampled in averaging mode to include a minimum of one sample per each 5 ft (1.5 m) traveled recorded with not less than five samples per measurement recorded per side of the "X".

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

Note: Typically, acceptance tests are required by the AHJ prior to building occupancy. As-built drawings should be provided including all system design parameters, other information required from the DAQ level and commissioning tests, including a full report with grid locations, DAQ measurements, and RF emitting device or system component gain values. The acceptance test typically entails a random test by the AHJ of radio communication in various portions of the building, especially including the critical areas. The AHJ can review any test documentation and ensure that the findings of the commissioning test with respect to DAQ levels and gain values are supported by the acceptance test.

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

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

Annual Tests. The AHJ should be notified in advance and should direct annual test procedures and requirements. Note: Typically, annual tests require several items to be checked. RF emitting devices and system components should be tested to ensure that the gain is the same as it was at initial installation and acceptance. Backup batteries and power supplies should be tested under load for 1 hour to verify that they will operate properly during a power outage.

License or Certification of Personnel. All system designs, installation, testing, and maintenance should be conducted, documented, and signed by an acceptable manufacturer or person in possession of a current radio licensing authority license, industry certification, professional electrical engineering license, or as required by the AHJ.

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

A.13.1 Security issues for communications center data systems include the following:

(1) Security of data from outsiders
(2) Security of data from inappropriate access and modification from insiders
(3) Denial-of-service attacks
(4) Equipment and infrastructure failures that impede or prevent access to data

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

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

Data systems give employees access to a wide variety of departmental data that were not easily available before. Agency rules and regulations should be modified to specifically address the misuse of data as a breach of the confidentiality agreement used by the agency. With the move to Internet protocol

(IP)–based networks for both the core network for land mobile radio systems as well as IP-based telephony and IP-based Next Generation 9-1-1, it is important that a new holistic approach to data security be taken. "Defense in depth" is an approach in which security is not resolved purely on a technical level but is also addressed across personnel and operations in a holistic risk management methodology. Therefore it is imperative that agencies implement a layered defense that will span the entire enterprise and is not purely technology focused. These defense-in-depth strategies are outlined in Table A.13.1.

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

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

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

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

A.13.1.3 All employees are responsible for maintaining security. Employment contracts, collective bargaining agreements, personnel manuals, and departmental directives should enforce this requirement. However, some personnel have primary responsibility for security, and these employee positions should be specified in the plan. Duties of these employees should include the following:

(1) Analyzing the agency's security exposure
(2) Regular and/or automatic monitoring for security compliance
(3) Routine auditing
(4) Archiving of security events or incidents for auditing or study

A.13.1.4 Recent events have revealed that a common thread in many attacks the adversary gains the credentials (user name and password) of legitimate users and is able to gain unfettered access to the IT systems as a result. This is especially true of agencies that have experienced advanced persistent threats (APTs) from determined adversaries. The Department of Homeland Security (DHS) provides a user education program called "Stop.Think.Connect" (www.dhs.gov/stopthinkconnect), which can be used as a foundation for such user training.

A.13.1.5 The goal of any information system is to restrict access to the following persons:

(1) Those who are authorized to use the system
(2) Those who have a need to know
(3) Those who are responsible for auditing the system to ensure that policies and regulations are implemented appropriately
(4) Those who are accountable for the actions of users who use and administer the system

Access control seeks to ensure confidentiality of information and integrity of information with role-based access control. With the philosophy that access control should involve the implementation of least privileges with authentication, authorization, and accountability (AAA), it is imperative that agencies leverage products and services that assist with access control and provide a layered defense in addition to the system's physical and environmental security. For very sensitive access to the network or certain computers and databases, two-factor authentication (something you know and something that you possess) is recommended.

Comprehensive procedures for the maintenance of data security should include the following:

(1) Policies and procedures that specify the process and that authorize or deny access to the data system
(2) Policies for reviewing access to the system when employment status changes (promotion, demotion, discharge)
(3) Password security rules (aging, privacy, sharing issues)
(4) Differentiated access control within the system for different users
(5) Encryption and key control
(6) Maintenance of data security during disposal (paper shredding, hard disk destruction)

Table A.13.1 Defense-in-Depth Strategies

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

Encryption. As used in P25, land mobile radios should follow the guidelines outlined in the Department of Homeland Security (DHS) Office of Emergency Communications *Guidelines for Encryption in Land Mobile Radio Systems.* Use of proprietary forms of encryption, or analog encryption on analog radios, is not of sufficient strength to meet law enforcement or EMS HIPAA requirements.

Impersonation/Inappropriate Use. A key component within information assurance and access control is identity assurance, which addresses the risk associated with identity impersonation and inappropriate account use. The communications system should integrate authentication appliances and associated tokens to provide the confidence to system owners that users accessing the critical infrastructure or communicating remotely as in Virtual Private Network (VPN) Remote Access are trusted entities through the use of two-factor (or strong) authentication by which the user must provide three bits of information: account name, account password (something they know), and the token ID (something they have).

Additionally, the system should log all transactions and user activity, allowing administrators to utilize it as an auditing, accounting, and compliance tool.

Subscriber Unit Authentication. The authentication of subscriber units (radios) before being authorized access to the critical communication system is necessary for several reasons, the most significant being the primary method of communication and necessity of continuous availability, the wide geographical wireless mobility, and the use of data on today's land mobile radio systems. In the past, concern has focused on the ability of nonagency personnel monitoring communications, which has pushed the capability of encrypted voice communications, but it only addresses the risks associated with confidentiality and integrity to a small degree. Without ensuring that radios and their users are allowed to be on the network and the talkgroups assigned to them, the system responds with "denial of service" because a false radio is assuming a valid radio's identity (lack of availability), false information is being placed on a trusted network (lack of integrity), and data are being stolen remotely (lack of confidentiality). It is therefore necessary to authenticate radios to the wireless system at a minimum and that they be mutually authenticated with systems that have a high level of risk and/or interoperability.

A.13.1.6 The core of an information system is the network that permits the sharing of information between systems. This makes it a prime medium for infiltration but also an excellent source for preventing and detecting unauthorized behavior. It is critical to implement multiple components of network security to address the myriad risks associated with IP networks, including access control lists, perimeter firewalls, network intrusion detection, and link encryption. Many third-party integrated service routers are also capable of supporting advanced security operating systems that permit not only the link encryption but also a software-based full firewall for additional network security.

The use of IP-enabled devices has created a new class of threats to public safety because the devices can provide unprecedented access to sensitive data. They can introduce malware into a public safety IP-based system, causing numerous problems that affect the ability to dispatch efficiently, including denial-of-service attacks. As a result, IP-enabled public safety devices require user access controls to ensure only authorized use. Also, in the event that an IP-enabled public safety device is lost or stolen, that device needs to have provisions for disabling it, similar to those outlined in 9.3.4.1.18. Further, IP-enabled public safety devices used by law enforcement agencies must also adhere to federal standards for access to sensitive law enforcement databases.

A.13.1.7 Computer systems have become not only the primary resource for storing information but also the primary workhorse for users to perform their jobs; therefore they have also become a primary objective for intruders for either data gathering or destruction. This makes a computer system the end point for security, and it requires layers to be built around it to minimize the risks associated with intruders accessing the information contained within the computer or with the trusted capability placed at their disposal.

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

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

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

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