NFPA® 1225

Standard for Emergency Services Communications

2022 Edition

NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING 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: 978-145592818-7 (Print)

ADDITIONAL IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

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 a new edition, may be amended with the issuance of Tentative Interim Amendments (TIAs), or be corrected by Errata. It is intended that through regular revisions and amendments, participants in the NFPA standards development process consider the then-current and available information on incidents, materials, technologies, innovations, and methods as these develop over time and that NFPA Standards reflect this consideration. Therefore, any previous edition of this document no longer represents the current NFPA Standard on the subject matter addressed. NFPA encourages the use of the most current edition of any NFPA Standard [as it may be amended by TIA(s) or Errata] to take advantage of current experience and understanding. An official NFPA Standard at any point in time consists of the current edition of the document, including any issued TIAs and Errata then in effect.

To determine whether an NFPA Standard has been amended through the issuance of TIAs or corrected by Errata, visit the "Codes & Standards" section at www.nfpa.org.

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® 1225

Standard for

Emergency Services Communications

2022 Edition

This edition of NFPA 1225, *Standard for Emergency Services Communications*, was prepared by the Technical Committees on Public Safety Telecommunicator Professional Qualifications and Public Emergency Service Communication, released by the Correlating Committee on Professional Qualifications, and acted on by the NFPA membership during the 2021 NFPA Technical Meeting held June 14–July 2. It was issued by the Standards Council on August 26, 2021, with an effective date of September 15, 2021.

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 1225 was approved as an American National Standard on September 15, 2021.

Origin and Development of NFPA 1225

This is the first edition of NFPA 1225; it consolidates NFPA 1061, *Standard for Public Safety Telecommunications Personnel Professional Qualifications*, and NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, into a single standard. The Standards Council approved the consolidation of NFPA 1061 and NFPA 1221 in April 2019. The two standards are separate and identifiable in NFPA 1225 for individual reference or adoption.

For this edition of NFPA 1225, the Committee on Public Safety Telecommunicator Professional Qualifications evaluated the job performance requirements for each position for validity to measure competency with the identified duties of each position. The committee identified the need for each position to maintain competency through professional development activities. To each position, the committee added the task of identifying fellow employees who exhibit signs and symptoms of emotional and behavioral distress. Updates to referenced standards were also identified by the committee.

The Committee on Public Emergency Service Communication made enhancements to all chapters addressing emergency services radio communications. Attention to maintaining the reliability of mission-critical communication was a prime focus of the committee. The committee recognized the role that Internet communication pathways play in emergency service communications. The committee created a separate chapter specific to in-building emergency responder communications enhancement systems to give stakeholders a centralized viewpoint of requirements for the systems and made refinements to definitions, permitting, system survivability, and system acceptance testing.

For more information about the ERRS consolidation project see nfpa.org/errs.

Correlating Committee on Professional Qualifications

William E. Peterson, *Chair*
Kissimmee, FL [M]
Rep. International Fire Service Training Association

Brian Baughman, Generac Power Systems Inc., WI [M]

Brian R. Brauer, University of Illinois Fire Service Institute, IL [E]
Rep. National Board on Fire Service Professional Qualifications

Derrick S. Clouston, North Carolina Department of Insurance, NC [U]

Gregory S. Cross, Texas A&M Engineer Extension Service, TX [SE]

Jason Dolf, Aerial Services Inc, IA [U]

Angus Maclean Duff, Consolidated Fire District 2, KS [U]

Richard A. Dunn, SC State Firefighters' Association, SC [E]

Alec Feldman, Fulcrum Consultants, Ireland [SE]
Rep. JOIFF-International Organisation for Industrial Hazard Management

Douglas P. Forsman, Fairfield Bay Fire Department, AR [L]

Richard Galtieri, Port Of Seattle Fire Department, WA [E]

Douglas R. Goodings, St. Clair Community College, Canada [SE]

Scott M. Gorgon, International Association of Fire Fighters (IAFF), DC [L]

R. Kirk Hankins, Fire Consulting & Case Review International, Inc., MO [U]
Rep. International Association of Arson Investigators, Inc.

Bill Slosson, Washington State Patrol, WA [E]

Philip C. Stittleburg, La Farge Fire Department, WI [L]
Rep. National Volunteer Fire Council

Matthew Brian Thorpe, North Carolina Office of the State Fire Marshal, NC [E]
Rep. International Fire Service Accreditation Congress

Charles "Randy" Watson, S-E-A, Ltd., GA [SE]

Michael J. Yurgec, Global Emergency Products, IL [M]

Alternates

Adam J. Goodman, S-E-A Limited, MD [SE]
(Alt. to Charles "Randy" Watson)

David W. Lewis, Odenton, MD [L]
(Alt. to Philip C. Stittleburg)

Robert W. Rand, Nat'l Board On Fire Service Prof. Qualifications, MA [E]
(Alt. to Brian R. Brauer)

Angela White, Wisconsin Technical College System, WI [E]
(Alt. to Matthew Brian Thorpe)

Nonvoting

Stephen P. Austin, Cumberland Valley Volunteer Firemen's Association, DE [L]
Rep. TC on Traffic Control Incident Management Professional Qualifications

Preet Bassi, Center For Public Safety Excellence, VA [C]
Rep. TC on Fire Service Analysts and Informational Technical Specialist

Alan W. Conkle, Ohio Association of Emergency Vehicle Technicians (OAEVT), OH [M]
Rep. TC on Emergency Vehicle Mechanic Technicians Professional Qualifications

John S. Cunningham, Nova Scotia Firefighters School, Canada [U]
Rep. TC on Fire Fighter Professional Qualifications

Jay Dornseif, III, Priority Dispatch Corporation, UT [M]
Rep. TC on Public Safety Telecommunicator Professional Qualifications

Richard C. Edinger, Chester, VA [SE]
Rep. TC on Hazardous Materials Response Personnel

Ronald R. Farr, Plainwell Fire Department, MI [C]
Rep. TC on Electrical Inspection Practices

Dave E. Hanneman, Self Employed, ID [SE]
Rep. TC on Incident Management Professional Qualifications

Daniel P. Heenan, Clark County Fire Department, NV [E]
Rep. TC on Fire Investigator Professional Qualifications

Orlando P. Hernandez, Texas State Fire Marshal's Office, TX [E]
Rep. TC on Rescue Technician Professional Qualifications

Ronald L. Hopkins, TRACE Fire Protection & Safety Consultant, Ltd., KY [SE]
Rep. TC on Fire Service Instructor Professional Qualifications

Robert J. James, UL LLC, IL [RT]
Rep. TC on Building Fire and Life Safety Director Professional Qualifications

Randy J. Krause, Port of Seattle Fire Department, WA [E]
Rep. TC on Fire Service Occupational Safety and Health

Peter J. Mulvihill, Reno, NV [SE]
Rep. TC on Fire Inspector Professional Qualifications

Randal E. Novak, Ames, IA [SE]
Rep. TC on Accreditation & Certification Professional Qualifications

Lawrence L. Preston, Maryland Fire and Rescue Institute, MD [E]
Rep. TC on Fire Officer Professional Qualifications

Jim Stumpf, Organizational Quality Associates, ID [SE]
Rep. TC on Wildfire Suppression Professional Qualifications

Robert D. Taylor, PRB Coal Users Group, IN [U]
Rep. TC on Industrial Fire Brigades Professional Qualifications

Nancy J. Trench, Stillwater, OK [M]
Rep. TC on Public Fire Educator Professional Qualifications

Paul Valentine, TUV SUD America Inc./Global Risk Consultants, IL [M]
Rep. TC on Fire Marshal Professional Qualifications

Robert Fash, 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 the management of the NFPA Professional Qualifications Project and documents related to professional qualifications for fire service, public safety, and related personnel.

Technical Committee on Public Safety Telecommunicator Professional Qualifications

Jay Dornseif, III, *Chair*
Priority Dispatch Corporation, UT [M]

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

Jason P. Gurian, Union County Emergency Services, NC [U]

April Heinze, National Emergency Number Association (NENA), VA [U]

Jacklyn Kilby-Richards, Town of Groton Emergency Dispatch/ Connecticut Fire Academy, CT [U]

Michelle Porter, Williamson County Emergency Communications, TX [E]

Paul Szoc, Keene Fire Department, NH [U]
Rep. International Municipal Signal Association

Kurt Weihs, SouthSound911/West Pierce Fire and Rescue/ Lakewood Fire Department, WA [L]

John C. Winstead, Nash Community College, NC [SE]

Robert Fash, 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 on the professional qualifications for public safety communications positions.

Technical Committee on Public Emergency Service Communication

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

Douglas M. Aiken, Lakes Region Mutual Fire Aid, NH [E]
William Ambrefe, City of Beverly, MA [E]
Derek Bergsten, City of Rockford, IL [E]
Joseph Francis Brooks, Boston Fire Department, MA [L]
Rep. International Association of Fire Fighters
Christopher Creamer, DynaFire, FL [IM]
Stephen Thomas Devine, FirstNet Built with AT&T, MO [IM]
Thomas DiBernardo, Florida Department Of Health, State Of Florida, FL [U]
Jay Dornseif, III, Priority Dispatch Corporation, UT [SE]
Jerry Eisner, RedSky Technologies Inc., IL [IM]
John A. Facella, Panther Pines Consulting, LLC, ME [SE]
Matthew Foley, SLS Consulting, Inc., MA [SE]
Kevin J. Fosso, Dane County Public Safety Communications, WI [U]
Jonathan Franklin, Signal Communications LLC, FL [IM]
April Heinze, National Emergency Number Association (NENA), VA [U]
Richard G. Kluge, Ericsson, NJ [U]
Rep. Alliance for Telecommunications Industry Solutions
Mark Krizik, Motorola, Inc., IL [M]
Minfei M. Leng, TX RX Systems Inc., NY [M]
Kenneth J. Link, Jr., US Department of Homeland Security, NJ [SE]
Tony R. Locatelli, Intrepid Electronic Systems, CA [IM]
Christopher H. Lombard, Seattle Fire Department, WA [U]
John Martyn, Zetron, WA [M]
Scott McCauley, Siemens Building Technologies, TX [M]
Rep. National Electrical Manufacturers Association
Nathan D. McClure, III, McClure Associates, VA [SE]
Casey McKenna, ADT Commercial, FL [M]
Carolina Y. Milan, Vandenberg AFB Emergency Communication Center, CA [U]
Bruce J. Moeller, University of Florida, FL [SE]
Brian Mosberian, Phoenix Fire Department, AZ [E]
James M. Mundy, Jr., Asset Protection Associates, Ltd., NY [SE]
Kevin R Nida, FirstNet Authority, CA [U]
Charles Packard, DFW Airport ITS, TX [IM]
Thomas J. Parrish, Telgian Corporation, MI [SE]
Alan Perdue, Safer Buildings Coalition, NC [U]
Richard Jay Roberts, Honeywell Fire Safety, IL [M]
Rep. Automatic Fire Alarm Association, Inc.
Timothy Ruiz, Code Consultants Inc, MO [SE]
Lawrence J. Shudak, UL LLC, IL [RT]
Evan E. Stauffer, Jr., Upper Chichester, PA [SE]
David Thompson, Honeywell, IN [M]
William J. Watters, Verisk Analytics/Insurance Services Office, Inc., NJ [I]
Ira Wiesenfeld, Ira Wiesenfeld & Associates, TX [SE]
David Winter, Fairfax County Fire And Rescue, VA [U]
Richard Woolf, Xtech Systems Inc., NY [IM]

Alternates

Greg M. Glenn, Pulse Signal Solutions, CA [SE]
(Alt. to John A. Facella)
Jeffrey G. Knight, City of Newton Fire Department, MA [U]
(Voting Alt.)
Benjamin Mellon, Seattle Fire Department, WA [U]
(Alt. to Christopher H. Lombard)
Raymond Patterson, Siemens Building Technologies, TX [M]
(Alt. to Scott McCauley)
Thomas Presnak, UL LLC, IL [RT]
(Alt. to Lawrence J. Shudak)
Randy Richmond, Zetron, Inc., TX [M]
(Alt. to John Martyn)
Sheryl A. Tricocci, Johnson Controls, GA [M]
(Alt. to Richard Jay Roberts)
Michael D. Varney, FirstNet, CT [U]
(Alt. to Kevin R. Nida)
Don R. Wise, DC Wise LLC, CA [SE]
(Alt. to Charles M. Berdan)

Robert Fash, 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 1225

Standard for

Emergency Services Communications

2022 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. 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 and extracted publications can be found in Chapter 2 and Annex G.

Chapter 1 Administration

1.1 Scope. This standard identifies the minimum job performance requirements (JPRs) for Public Safety Telecommunications Personnel, and provides minimum requirements for the installation, maintenance, and use of emergency services communications systems.

1.2 Purpose. The purpose of this standard is to specify the minimum job performance requirements (JPRs) for service as Public Safety Telecommunications Personnel and specify minimum requirements for systems, retransmissions, dispatching, performance levels and quality of installations for emergency services communications.

1.3* Application. This standard can be applied as follows:

(1) Chapters 1 through 11, and Annexes A, B, C, D, E, and G constitute the 2022 edition of NFPA 1061.
(2) Chapters 1 through 3, Chapters 12 through 23, and Annexes A, F, and G constitute the 2022 edition of NFPA 1221.

1.4 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.

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

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

1.5 Units. In this standard, equivalent values in SI units shall not be considered as the requirement, as these values can be approximate. *(See Table 1.5.)*

Table 1.5 U.S.-to-SI Conversions

Quantity	U.S. Unit/Symbol	SI Unit/Symbol	Conversion Factor
Length	inch (in.)	millimeter (mm)	1 in. = 25.4 mm
	foot (ft)	meter (m)	1 ft = 0.305 m
Area	square foot (ft^2)	square meter (m^2)	1 ft^2 = 0.0929 m^2

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,* 2021 edition.

NFPA 10, *Standard for Portable Fire Extinguishers,* 2022 edition.

NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2022 edition.

NFPA 37, *Standard for the Installation and Use of Stationary Combustion Engines and Gas Turbines,* 2021 edition.

NFPA 54, *National Fuel Gas Code,* 2021 edition.

NFPA 58, *Liquefied Petroleum Gas Code,* 2020 edition.

NFPA 70®, National Electrical Code®, 2020 edition.

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

NFPA 75, *Standard for the Fire Protection of Information Technology Equipment,* 2020 edition.

NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems,* 2021 edition.

NFPA 90B, *Standard for the Installation of Warm Air Heating and Air-Conditioning Systems,* 2021 edition.

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

NFPA 110, *Standard for Emergency and Standby Power Systems,* 2022 edition.

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2022 edition.

NFPA 220, *Standard on Types of Building Construction,* 2021 edition.

NFPA 731, *Standard for the Installation of Premises Security Systems,* 2020 edition.

NFPA 780, *Standard for the Installation of Lightning Protection Systems,* 2020 edition.

NFPA 1140, *Standard for Wildland Fire Protection,* 2022 edition.

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

NFPA 1600®, Standard on Continuity, Emergency, and Crisis Management, 2019 edition.

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

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

2.3 Other Publications.

2.3.1 APCO Publications. APCO International, 351 North Williamson Boulevard, Daytona Beach, FL 32114.

APCO ANS 2.106.1, *Public Safety Grade Site Hardening Requirements*, 2019.

2.3.2 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,* 2020.

2.3.3 FEMA Publications. Emergency Management Institute, 16825 S. Seton Ave., Emmitsburg, MD 21727.

IS 0100, *Introduction to the Incident Command System,* ICS 100, 2018.

IS 0200, *Incident Command System for Single Resources and Initial Action Incidents,* 2019.

IS 0700, *National Incident Management System (NIMS), An Introduction,* 2020.

IS 0800, *National Response Framework, An Introduction,* 2020.

National Incident Management System (NIMS), 2017.

2.3.4 IEEE Publications. IEEE, 3 Park Avenue, 17th Floor, New York, NY 10016-5997.

IEEE C2, *National Electrical Safety Code*, 2017.

2.3.5 IES Publications. Illuminating Engineering Society, 120 Wall Street, 17th Floor, New York, NY 10005.

IESNA HB-9-00, *The Lighting Handbook*, 10th edition, 2019.

2.3.6 NENA Publications. National Emergency Number Association, 1700 Diagonal Road, Suite 500, Alexandria, VA 22314.

NENA-ADM-000.23, *NENA Master Glossary of 9-1-1 Terminology*, 2020.

NENA/APCO ANS 2.105.1, *NG9-1-1 Emergency Incident Data Document (EIDD)*, 2017.

2.3.7 TIA Publications. Telecommunications Industry Association, 1320 North Courthouse Road, Suite 200, Arlington, VA 22201.

TIA-102.BAAA, *Project 25 FDMA Common Air Interface*, 2017.

TIA-102.BBAB, *Project 25 Phase 2 Two-Slot Time Division Multiple Access Physical Layer Protocol Specification,* 2009.

TIA-102.BBAC, *Project 25 Two-Slot TDMA Media Access Control Layer Specification,* 2019.

TIA-603, *Land Mobile FM or PM Communications Equipment Measurement and Performance Standards*, 2016.

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

UL 497C, *Standard for Protectors for Coaxial Communications Circuits,* 2001, revised 2017.

UL 752, *Standard for Bullet-Resistant Equipment,* 2005, revised 2015.

UL 2524, *Standard for In-Building 2-Way Emergency Radio Communication Enhancement Systems,* 2019.

2.3.9 US Government Publications. US Government Publishing Office, 732 North Capitol Street, NW, Washington, DC 20401-0001.

Homeland Security Presidential Directive 5, "Management of Domestic Incidents," February 28, 2003.

NIMS/ICS, *Emergency Responder Field Operations Guide,* 2011.

Presidential Policy Directive 8, "National Preparedness," March 30, 2011.

2.3.10 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®, 2020 edition.

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

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems,* 2022 edition.

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

NFPA 1000, *Standard for Fire Service Professional Qualifications Accreditation and Certification Systems,* 2022 edition.

NFPA 1002, *Standard for Fire Apparatus Driver/Operator Professional Qualifications,* 2017 edition.

NFPA 1021, *Standard for Fire Officer Professional Qualifications,* 2020 edition.

NFPA 1041, *Standard for Fire and Emergency Services Instructor Professional Qualifications,* 2019 edition.

NFPA 1561, *Standard on Emergency Services Incident Management System and Command Safety,* 2020 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 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 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, acknowledge a public alert.

3.3.3 Alphanumeric Devices. Paging receivers used as part of a radio alerting system 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 Annunciator. A unit containing one or more indicator lamps, alphanumeric displays, or other equivalent means in which each indication provides status information about a circuit, condition, or location. [**72,** 2022]

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

3.3.7 Automatic Call Distributor (ACD). Equipment that automatically distributes incoming calls to available public safety answering point (PSAP) attendants in the order in which the calls are received or that queues calls until an attendant becomes available.

3.3.8* Automatic Location Identification (ALI). The automatic display at the PSAP of the caller's telephone number, the address/location of the telephone, and supplementary emergency services information about the location from which a call originates.

3.3.9* Automatic Number Identification (ANI). A series of alphanumeric characters that informs the recipient of the source of an event.

3.3.10* Backbone. A communications cable in an in-building emergency responder communications enhancement system that carries radio frequency (RF) signals that are required to make the overall system operational from the donor antenna signal source, through the amplifiers. and up to the connection point of the distribution antenna cables.

3.3.11 Backbone Cable. Coaxial cable, optical fiber cable and other cables utilized within the backbone to acquire and distribute RF signals to the in-building emergency responder communications enhancement systems.

3.3.12 Backbone Cable Components. Splitters, couplers, and connectors utilized within the backbone to acquire and distribute RF signals to the in-building emergency responder communications enhancement systems.

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

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

3.3.15 Cable. A factory assembly of two or more conductors having an overall covering. [**70:**805.2]

3.3.16 Call. Any type of request for emergency assistance (RFEA), which is not limited to voice.

3.3.17 Call Answer. The condition when a call is delivered to and acknowledged by a telecommunicator or an auto greeting and two-way communication can begin.

3.3.18 Call Answer Interval. The elapsed time between call arrival and call answer.

3.3.19 Call Arrival. The condition when a call is presented to the PSAP customer premises equipment (CPE), which can include acknowledgment by an auto attendant.

3.3.20 Call Detail Recording (CDR). A system that provides metadata for each call, including ANI, the trunk number, and the answering attendant number, as well as the time of seizure, answer, and disconnect/transfer.

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

3.3.22 Certification. An authoritative attestment; 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,** 2022]

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

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

3.3.25 Coded Receivers. Paging receivers used as part of a radio alerting system that respond only to messages directed to a specific unit or to units in an assigned group.

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

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

3.3.28* Communications Officer. The individual responsible for the 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.

3.3.29* Communications System. A combination of devices, networks, applications, computers, and services.

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

3.3.31* 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.

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

3.3.33 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 users.

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

3.3.35 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]

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

3.3.37 Cybersecurity. The ability of any computing system, software program, or infrastructure to resist intentional interference, compromise, or incapacitation through the misuse of the Internet or public or private telecommunications systems, or similar conduct that harms interstate commerce or threatens public health or safety.

3.3.38 Data Security. Protection of the integrity of an organization's data resources to ensure that they are available to support the mission and that the data is not compromised.

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

3.3.40 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.

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

3.3.42 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.

3.3.43* Directory. A printed or virtual listing of telephone numbers.

3.3.44* 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.

3.3.45 Dispatcher. See 3.3.127, Telecommunicator.

3.3.46 Dispatching. See 3.3.54, Emergency Event Processing/Dispatching.

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

3.3.48* Distribution Antenna. A radio antenna that is specifically designed to radiate RF energy into a specific and limited building area, usually from a ceiling- or wall-mounted antenna.

3.3.49* Distribution Antenna Cable. A communications cable that carries RF energy in both directions along its length to distribution antennas in one or more places in a building.

3.3.50 Donor Antenna. Antennas used with in-building emergency responder communications enhancement systems that provide the connection between the wide area communications system of interest and the in-building system.

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

3.3.52* Emergency. A condition that endangers or is believed to endanger life or property and that requires the urgent response of an emergency response agency.

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

3.3.54* Emergency Event Processing/Dispatching. A process by which an event 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.

3.3.55 Emergency Incident. Any situation to which the emergency services organization responds to deliver emergency services, including rescue, fire suppression, emergency medical care, special operations, law enforcement, and other forms of hazard control and mitigation. [**1561,** 2020]

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

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

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

3.3.59* Emergency Services Communications System. A communications system dedicated to the receipt of events, the coordination and dispatch of first responder resources, and the management of resources and activities post-dispatch.

3.3.60 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.

3.3.61* Event. An emergency or other situation that requires action by an emergency response agency.

3.3.62* Event Data. Information related to an event that contains the physical location of the event, the callback number of the reporting party/system, and other explanatory information.

3.3.63* Frequencies. The particular waveband(s) at which a communications system broadcasts or transmits.

3.3.64 Frequency License Holder(s). The person(s) or entity(ies) that hold the license from the licensing authority of the country of jurisdiction for the frequencies being used by both the in-building emergency responder communications enhancement system and the emergency services communications system that it enhances.

3.3.65 Frequency Licensing Authority. The government authority in a country that issues licenses for the use of communication frequencies by authorized entities and individuals.

3.3.66 In-building Emergency Responder 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 communications within the building and between on-scene first responders and communications centers.

3.3.67 Incident Management System. The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for the management of assigned resources to effectively accomplish stated objectives pertaining to an incident.

3.3.68 Incident/Tactical Dispatcher. See 3.3.101.1.

3.3.69 Information Communication Technology (ICT) Security. Security of the integrity of the organization's data within the organization's normal use of that data, as well as security to prevent unauthorized external parties from attempting to access or damage the data using cyber attack techniques.

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

3.3.71 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.

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

3.3.73 Job Performance Requirement (JPR). A written statement that describes a specific job task, lists the items necessary to complete the task, and defines measurable or observable outcomes and evaluation areas for the specific task. [**1000,** 2022]

3.3.74 Link Budget. Engineering calculations that estimate the RF signal strength from a portable radio or other field device used by ERUs to the first responder communications fixed network (i.e., uplink) and the RF signal strength back from the first responder communications fixed network to the portable radio or other field device used by ERUs (i.e., downlink).

3.3.75* Logging Recorder. A device that records event and dispatch information.

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

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

3.3.78 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.

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

3.3.80 Monitoring for Integrity. Automatic monitoring of circuits and other system components for the existence of defects or faults that interfere with receiving or transmitting data related to an event.

3.3.81* Multi-Line Telephone System (MLTS). A system designed to aggregate more than one incoming voice communication channel for use by more than one telephone. This includes network- and premises-based systems.

3.3.82 Next Generation 9-1-1 (NG9-1-1). NG9-1-1 is an IP-based system comprised of managed emergency services IP networks (ESInets), functional elements such as applications, and databases that replicate traditional Enhanced 9-1-1 features and functions and provide additional capabilities. NG9-1-1 is designed to provide access to emergency services from all connected communications sources and to provide multimedia data capabilities for PSAPs and other emergency service organi-

zations. [NENA-ADM-000.23, *NENA Master Glossary of 9-1-1 Terminology*]

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

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

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

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

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

3.3.88 Path (Pathways). Any circuit, conductor, optic fiber, radio carrier, or other means connecting two or more locations. [**72,** 2022]

3.3.89 Perceptual Objective Listening Qualitative Analysis (POLQA). A method of automated voice quality testing for telecommunications systems. *(See A.20.3.10.)*

3.3.90 Permanent Visual Record (Recording). An immediately readable, not easily alterable record of all occurrences of a status change.

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

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

3.3.93* Private Branch Exchange (PBX). A system designed to connect to a local incumbent or competitive exchange carrier to allow telephone calls to be distributed to extensions to use a set of voice communication channels to make outbound calls.

3.3.94 Protective Signaling System. Any alarm or system of alarms designed to give notification or warning, whether audible at the location or at a central receiving area, of the existence of a probable emergency or other unusual occurrence that might involve life safety or property protection. [**601,** 2020]

3.3.95 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.

3.3.96 Public Alerting System (PAS). A system that creates, transmits, and displays a public alert message, 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.

3.3.97 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.

3.3.98 Public Safety Agency/Public Safety Organization. See 3.3.56, Emergency Response Agency (ERA).

3.3.99* Public Safety Answering Point (PSAP). A facility equipped and staffed to receive emergency and non-emergency calls requesting public safety services via telephone and other communication devices.

3.3.100 Public Safety 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.

3.3.101 Public Safety Communications Center Personnel.

3.3.101.1 ***Incident/Tactical Dispatcher.*** A person serving as a specialized telecommunicator who responds to the scene of an emergency, manages the flow of information from the command center to the communications center, and documents requests for and deployment of specialized teams, equipment, or agencies.

3.3.101.2* ***Public Safety Communications Manager/Director.*** A public safety communications professional who directs communications center staff by establishing operational procedures, managing center operations, and responding to constantly changing needs to provide essential emergency communications services.

3.3.101.3* ***Public Safety Communications Supervisor.*** The first-level public safety communications professional who provides leadership to employees through experience and training in order to achieve the agency's mission, standards, and goals.

3.3.101.4 ***Public Safety Communications Training Coordinator.*** The public safety professional who is responsible, in an administrative and technical capacity, for the development and implementation of a training program for the Public Safety Telecommunicator that will specifically meet the needs of the agency, in compliance with any state, federal, local or AHJ requirements for curriculum, reporting, and record keeping.

3.3.101.5 ***Public Safety Communications Training Officer (CTO).*** The first-line public safety communications professional who demonstrates superior conduct, professionalism, skills, and knowledge in the training of a new hire, accomplished through the use of adult learning principles using agency-defined training parameters in a classroom setting and through on-the-job and one-on-one interactions and simulations.

3.3.101.6 ***Public Safety Quality Assurance Coordinator.*** The public safety professional who is responsible for the coordination, upkeep, and maintenance of a formal quality assurance process as approved by the AHJ while ensuring that standards and procedures are adhered to and that delivered products or services consistently meet standards or performance requirements.

3.3.101.7 ***Public Safety Telecommunicator.*** The individual tasked by a public safety agency as the first of the first responders whose primary responsibility is to receive, process, transmit, and/or dispatch emergency and non-emergency calls for law enforcement, fire, emergency

medical, and other public safety services via telephone, radio, and other communication devices.

3.3.101.7.1 ***Public Safety Telecommunicator I (Call Taker).*** The individual who is the initial point of contact in obtaining service requests to facilitate the prioritization, preparation, and dissemination of allocated and appropriate resources; provides instruction pursuant to agency policy or protocol; makes independent decisions, conveys information, and provides referrals; works in cooperation with the Public Safety Telecommunicator II; and disseminates information that is paramount to ensuring the safety of the public and responders.

3.3.101.7.2 ***Public Safety Telecommunicator II (Radio Dispatcher).*** The individual who prioritizes, initiates, and coordinates the response of public safety agencies; manages the flow of incident-related information to and from field units or public safety resources; monitors the status of field units; and assigns additional resources as requested or required.

3.3.102 Public Switched Telephone Network (PSTN). An assembly of communications equipment and telephone service providers that utilize managed facilities-based voice networks (MFVN) to provide the general public with the ability to establish communications channels via discrete dialing codes. [**72,** 2022]

3.3.103 Qualified Telecommunicator. A person that has met the qualifications for a Telecommunicator II as defined in Chapter 5 and authorized by the AHJ.

3.3.104 Radiating Cable. A coaxial cable that distributes small amounts of RF energy along its length by means of periodic breaks in the shield surrounding the center conductor.

3.3.105* Radio Channel. A band of frequencies of a width sufficient to allow its use for radio communications. [**72,** 2022]

3.3.106* 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 it can access a land mobile radio-fixed repeater station or fixed trunking station to gain access to the communication system.

3.3.107* Radio Frequency. A measurement representing the oscillation rate of the electromagnetic radiation spectrum or electromagnetic radio waves.

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

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

3.3.110 Requester. Any person, device, machine, or system observing and reporting an event requiring emergency response.

3.3.111 Requisite Knowledge. Fundamental knowledge one must have in order to perform a specific task.

3.3.112 Requisite Skills. The essential skills one must have in order to perform a specific task.

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

3.3.114 RF-Emitting Device. An active or passive device that emits a radio frequency signal as part of an in-building emergency responder communications enhancement system.

3.3.114.1 ***Active RF-Emitting Device.*** Any type of circuit component that requires an ac or dc power source with the ability to electrically control electron flow or amplification of an RF signal, including, but not limited to, signal boosters, repeaters, bidirectional amplifiers, and fiber distributed antenna systems.

3.3.114.2 ***Passive RF-Emitting Device.*** A device that does not require an external ac or dc source of power for its operation and does not provide amplification of an RF signal, including, but not limited to, coax cable, couplers, splitters, and passive antennas.

3.3.115* RF System Designer. An individual who has the education, experience, training, and understanding of RF theory and application to design an in-building emergency responder communications enhancement system (ERCES) that complies with this standard and the requirements of the licensing authority of the country of jurisdiction.

3.3.116 Security Vestibule. A compartment 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.

3.3.117 Service Request. Any communication from the public or an agency that prompts action by a telecommunicator.

3.3.118 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.

3.3.119* 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.

3.3.120 Stored Emergency Power Supply System (SEPSS). A system consisting of an uninterruptible power supply (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 sources and provide desired switching of the load; and all necessary control equipment to make the system functional. [**111,** 2022]

3.3.121 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.

3.3.122 Supervisor. An individual responsible for overseeing the performance or activity of other members. [**1021,** 2020]

3.3.123 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, as well as the steps individual agencies should follow to request, activate, use, and deactivate each asset.

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

3.3.125 Task. A specific job behavior or activity. [**1002,** 2017]

3.3.126 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.

3.3.127 Telecommunicator. An individual whose primary responsibility is to receive, process, or disseminate information of a public safety nature via telecommunication devices.

3.3.128* Telematics. The combination of communications and information systems used to provide information or communications from a vehicle to a PSAP through a telematics service provider.

3.3.129 Telephone Number. A multidigit number corresponding to a specific voice connection for accessing that connection.

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

3.3.131 Transceiver. A combined transmitter and receiver radio unit.

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

3.3.133 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.

3.3.134* Two-Way Alphanumeric Devices. Paging transceivers used as part of a radio-alerting system 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.

3.3.135* Uninterruptible Power Supply (UPS). A device or system that provides quality and continuity of ac power through the use of a stored-energy device as the backup power source during any period when the normal power supply is incapable of performing acceptably. [**111,** 2022]

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

3.3.137* Voice Connection. A physical or virtual audio connection.

3.3.138 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 Public Safety Telecommunicator I —Professional Qualifications (NFPA 1061)

4.1 Administration.

4.1.1 Scope. Chapters 4 through 11 shall identify the minimum job performance requirements (JPRs) for public safety telecommunications personnel.

4.1.2 Purpose. Chapters 4 through 11 shall specify the minimum JPRs for service as public safety telecommunications personnel.

4.1.2.1 Chapters 4 through 11 shall define public safety telecommunications personnel.

4.1.2.2 The intent of Chapters 4 through 11 shall be to ensure that personnel serving as public safety telecommunications personnel are qualified.

4.1.2.3* Chapters 4 through 11 shall not address organization or management responsibility.

4.1.2.4 Chapters 4 through 11 shall not restrict any jurisdiction from exceeding or combining these minimum requirements.

4.1.2.5 JPRs for each level and position are the tasks personnel shall be able to perform in order to carry out the job duties.

4.1.2.6* Public safety telecommunications personnel shall remain current with the knowledge, skills, and JPRs addressed for each level or position of qualification.

4.1.3 Application. The application of Chapters 4 through 11 shall specify which requirements apply to public safety telecommunications personnel.

4.1.3.1 The JPRs shall be accomplished in accordance with the requirements of the authority having jurisdiction (AHJ) and all applicable NFPA standards.

4.1.3.2 JPRs shall not be required to be mastered in the order in which they appear.

4.1.3.3 The AHJ shall establish instructional priority and the training program content to prepare personnel to meet the JPRs of this standard.

4.1.3.4* Performance of each requirement of Chapters 4 through 11 shall be evaluated by personnel approved by the AHJ.

4.1.3.5* The JPRs for each level or position shall be completed in accordance with recognized practices and procedures or as defined by law or by the AHJ.

4.1.3.6 Personnel assigned to any duties defined in Chapters 4 through 11 shall meet all of the requirements specific to their position as defined in the relevant chapter prior to being qualified.

4.1.3.7 The AHJ shall provide personal protective clothing and the equipment necessary to conduct assignments.

4.1.3.8 JPRs involving exposure to products of combustion shall be performed in approved personal protective equipment (PPE).

4.1.3.9 Prior to training to meet the requirements of Chapters 4 through 11, personnel shall meet the following requirements:

(1)* Educational requirements established by the AHJ
(2) Age requirements established by the AHJ
(3) Medical requirements established by the AHJ
(4)* Job-related physical performance requirements established by the AHJ
(5)* Background investigation and character traits as established by the AHJ

4.1.3.10 Wherever in Chapters 4 through 11 the terms *rules, regulations, policies, procedures, supplies, apparatus, or equipment* are used, they shall be those of the AHJ.

4.1.3.11 Public safety telecommunications personnel shall meet all of the requirements defined by the National Incident Management System (NIMS) and the Incident Command System (ICS) as mandated by Homeland Security Presidential Directives 5 and 8 (see www.FEMA.gov) and as directed by the NIMS Integration Center.

4.1.3.12* For each level of progression as identified in Chapters 4 through 11, persons shall participate in continuing professional development activities to maintain competency with the JPRs covered in this standard for each level and position that the person is professionally qualified to perform.

4.2 General. The Public Safety Telecommunicator I shall receive and process service requests and disseminate information as defined in Sections 4.3 through 4.6.

4.3 Receiving Requests for Service.

4.3.1 Description of Duty. To process any request for public safety services.

4.3.2 Establish secure communications with the service requester, given a communication device, a means of collecting information, and a work station, so that a communication link with the requester is achieved.

(A)* Requisite Knowledge. Verbal communications process.

(B)* Requisite Skills. Operation and basic troubleshooting of communications systems and devices and application of verbal and listening skills in order to obtain accurate information.

4.3.3 Collect pertinent information, given a request for service, so that accurate information regarding the request is obtained.

(A) Requisite Knowledge. Local area dispatch protocol system(s) as defined by the AHJ.

(B)* Requisite Skills. Controlling the conversation utilizing established questioning and active listening techniques.

4.3.4 Utilize nonverbal communications, given a request for service through a communications device, so that accurate information regarding the request is obtained.

(A)* Requisite Knowledge. Nonverbal communication protocols.

(B)* Requisite Skills. Use of nonverbal communication devices.

4.4 Processing Requests for Service.

4.4.1* Description of Duty. Prepare data for dispatch or referral by evaluating, categorizing, formatting, and documenting the incident per established policies, procedures, or protocols.

4.4.2 Prepare records of public safety services requests, given agency policies, procedures, guidelines, and resources, so that the record is correct, complete, and concise.

(A) Requisite Knowledge. Policies, procedures, guidelines, and protocols established by the AHJ.

(B) Requisite Skills. Application of basic language and writing skills, interpreting and condensing information, basic computer skills, keyboarding, mousing, typing skills, and legible handwriting.

4.4.3 Utilize information provided by a service requester, given the policies, procedures, and guidelines of the agency, so that the request is accurately categorized and prioritized.

(A)* Requisite Knowledge. Incident categories, priority levels, and identification of potential threats, risks, and hazards.

(B) Requisite Skills. Basic comprehension and problem solving.

4.4.4* Determine incomplete, conflicting, or inconclusive information or data, given agency policies, procedures, guidelines, protocols, and resources, so that an allocation of resources is selected.

(A) Requisite Knowledge. Available resources, agency jurisdictions, and boundaries.

(B) Requisite Skills. Reading maps and charts and applying a global positioning system (GPS) to existing maps and resource lists.

4.4.5 Notify correct personnel about addition, deletion, and correction of data, given agency policies, procedures, guidelines, and protocols, so that documents, files, databases, maps, and resource lists are accurately maintained.

(A) Requisite Knowledge. Familiarity with maps, databases, and resource lists.

(B) Requisite Skills. Basic writing skills, legible handwriting, and basic computer skills.

4.5 Disseminate Requests for Services.

4.5.1 Relay instructions, information, and directions to the service requester, given agency policies, procedures, guidelines, and protocols, so that information appropriate to the incident is consistent with agency policies, procedures, guidelines, and protocols and results in resolution, referral, or response.

(A)* Requisite Knowledge. Availability of resources, policies, and procedures regarding prearrival instructions.

(B)* Requisite Skills. Voice control, provide directions, route callers, and operate communication devices.

4.5.2* Relay information to other public safety telecommunications personnel or entities, given processed data, so that accurate information regarding the request for service is provided.

(A) Requisite Knowledge. Policies, procedures, or guidelines as determined by the AHJ.

(B) Requisite Skills. Voice control, verbal skills, and basic computer skills.

4.5.3 Respond to requests for information, given an inquiry from the public or the media, so that the policies, procedures, and guidelines are followed.

(A) Requisite Knowledge. Policies, procedures, or guidelines as determined by the AHJ.

(B) Requisite Skills. Verbal and written skills.

4.6 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

4.6.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 5 Public Safety Telecommunicator II (NFPA 1061)

5.1 General. The Public Safety Telecommunicator II shall meet the job performance requirements in Chapter 4 for Public Safety Telecommunicator I and those defined in Sections 5.2 through 5.4 of this standard.

5.2 Receive Requests for Service.

5.2.1* Description of Duty. To manage information from multiple sources requiring requests for services or assistance.

5.2.2* Monitor public safety radio systems, given equipment used by the agency, so that information requiring action by the Public Safety Telecommunicator II is identified.

(A)* Requisite Knowledge. Basic radio systems, technology, and standard terminology used by the AHJ.

(B) Requisite Skills. Operation of radio equipment, differentiation between various audio stimuli, and effective listening abilities.

5.2.3* Monitor electronic data systems, given equipment used by the agency, so that information requiring action by the Public Safety Telecommunicator II is identified.

(A)* Requisite Knowledge. Response to audio and visual stimuli.

(B)* Requisite Skills. Basic computer skills and interpretation of visual symbols.

5.2.4 Monitor alarm systems, given equipment used by the agency, so that information requiring action by the Public Safety Telecommunicator II is identified.

(A) Requisite Knowledge. Familiarity with alarm equipment and system operation and technology.

(B) Requisite Skills. Interpretation of alarm system signals, data, or messages.

5.3 Process Requests for Service.

5.3.1 Description of Duty. Review and format data for dispatch or referral. Monitor resource status and determine units for deployment.

5.3.2 Validate incident information, given a request for service; available resources; and agency policies, procedures, guidelines, and protocols, so that an appropriate response is determined and a resource allocation prepared.

(A) Requisite Knowledge. Policies, procedures, guidelines, and protocols related to the allocation of resources and the duties and functions of response units.

(B) Requisite Skills. Interpretation of incident information.

5.3.3* Maintain location and status of units, given the resources available to the agency and utilizing the systems and equipment in the public safety communications center, so that the current availability, status, and safety of all deployable resources is known.

(A)* Requisite Knowledge. Capabilities and functions of personnel, units, and specialized equipment and tools and their availability and current location.

(B) Requisite Skills. Operation of public safety communications center systems and equipment used for maintaining status.

5.3.4 Categorize alarm information, given signals, messages, codes, and data, so that the information is properly interpreted in preparation for the allocation of resources.

(A) Requisite Knowledge. Operational principles, practices, procedures, guidelines, and protocols for alarm systems provided in the public safety communications center and agency policies related to alarm system operations.

(B) Requisite Skills. Basic computer skills, including keyboarding and mousing, and differentiation between multiple audiovisual stimuli.

5.3.5 Determine the priority of a service request, given information provided by other telecommunicators or field units and the agency policies, procedures, guidelines, and protocols, so that the priority of the request is defined.

(A) Requisite Knowledge. Policies, procedures, guidelines, and protocols related to call prioritization, incident categories, priority levels, and identification of potential threats, risks, and hazards.

(B) Requisite Skills. Operation of systems and aids provided in the public safety communications center for call prioritization, and decision-making skills.

5.3.6* Formulate a response, given the validated and prioritized request for service and the availability of deployable resources, so that the appropriate response is selected for the safety of responders.

(A) Requisite Knowledge. Procedures for the allocation or assignment of resources and requesting mutual aid.

(B) Requisite Skills. Operation of systems and aids provided in the public safety communications center.

5.4 Disseminate Requests for Service.

5.4.1* Description of Duty. Transmit and relay information or data to field units or other resources, given a request for service, that results in a notification for the response.

(A) Requisite Knowledge. Applicable Federal Communications Commission (FCC) rules; radio procedures and protocols; codes; agency policies, procedures, and guidelines; an incident management system, and the telecommunicator's role and function within the system.

(B) Requisite Skills. Voice control and operation of telecommunications equipment.

5.4.2* Initiate deployment of response units, given the validated and prioritized request for service and the agencies' telecommunications equipment, so that service request information is conveyed to units designated for response.

(A) Requisite Knowledge. All radio communications in compliance with the rules and regulations governing wireless communications in the country of operation; radio procedures and protocols; codes; agency policies, procedures, and guidelines; an incident management system; and the telecommunicator's role and function within the system.

(B) Requisite Skills. Voice control and operation of telecommunications equipment, public address (PA) systems, Internet protocol (IP) systems, and data terminals.

5.4.3 Relay service request information, given available resources and telecommunications equipment, so that all pertinent information is communicated to all responding units and agencies.

(A) Requisite Knowledge. All radio communications in compliance with the rules and regulations governing wireless communications in the country of operation; radio procedures and protocols; codes; agency policies, procedures, and guidelines; an incident management system, and the telecommunicator's role and function within the system.

(B) Requisite Skills. Voice control and operation of telecommunications equipment.

5.4.4 Gather supplemental information, given a service request, so that the current information is evaluated, prioritized, and relayed to response units or other personnel and agencies as needed.

(A) Requisite Knowledge. Agency policies, procedures, and guidelines and accessing other resources as requested.

(B)* Requisite Skills. Use of printed and electronic reference materials, databases, and emergency action plans.

5.4.5* Activate the community emergency action plan, given data indicating the likelihood or onset of a critical situation beyond the normal scope of operations, so that the implementation is timely and in accordance with agency policies, procedures, guidelines, and protocols.

(A) Requisite Knowledge. Understanding agency policies, procedures, and guidelines and accessing other resources as requested.

(B) Requisite Skills. Use of printed and electronic reference materials, databases, and emergency action plans.

5.4.6 Activate the public safety communication center emergency action plan, given internal emergency and agency policies, procedures, guidelines, and protocols, so that the integrity of the communications system is maintained and the safety of communications center personnel is achieved.

(A) Requisite Knowledge. Existing emergency and contingency plans for incidents within the public safety communication center.

(B) Requisite Skills. Use of predetermined mitigation and evacuation plans.

5.5 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

5.5.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 6 Incident/Tactical Dispatcher (NFPA 1061)

6.1 General.

6.1.1 The Incident/Tactical Dispatcher shall have the requisite knowledge of a telecommunicator in addition to the knowledge specific to the Incident/Tactical Dispatcher position.

6.1.2 This Incident/Tactical Dispatcher shall be knowledgeable of the National Incident Management System (NIMS), the Incident Command System (ICS), and a resource ordering system.

6.1.3 The Incident/Tactical Dispatcher shall have additional knowledge requirements for the following: responding to incidents; assuming the position's responsibilities; communicating effectively; ensuring the completion of assigned actions to meet identified objectives; and receiving, processing, and disseminating information.

6.1.4 The Incident/Tactical Dispatcher's duty shall involve utilizing the organizational structure, forms, and terminology of NIMS and the ICS according to the job performance requirements of Section 6.2.

6.2 Description of Duty. Apply ICS structure and terminology, given an incident or planned event utilizing the ICS and the NIMS/ICS, *Emergency Responder Field Operations Guide*, so that the ICS is identified, the locations and functions of each unit are understood, and the role of the Incident/Tactical Dispatcher is assumed.

6.2.1 Determine how to use a resource designation system, given an incident or planned event utilizing ICS and the NIMS/ICS, *Emergency Responder Field Operations Guide*, so that equipment typing and numbering are understood and the appropriate resources are used.

(A) Requisite Knowledge. ICS 100, *Introduction to the Incident Command System*; ICS 200, *Basic Incident Command System for Initial Response*; ICS 700, *An Introduction to the National Incident Management System*; ICS 800, *National Response Framework, an Introduction*; and any local, state, or federal mutual aid agreements.

(B) Requisite Skills. Filling out incident forms and documentation.

6.2.2 Prepare ICS forms, given an incident or planned event utilizing ICS and the NIMS/ICS, *Emergency Responder Field Operations Guide,* so that all interactions within the communications unit are documented accurately.

(A) Requisite Knowledge. ICS 100, *Introduction to the Incident Command System*; ICS 200, *Basic Incident Command System for Initial Response*; ICS 700, *An Introduction to the National Incident Management System*; ICS 800, *National Response Framework, an Introduction*; and any local, state, or federal mutual aid agreements.

(B) Requisite Skills. Filling out incident forms and documentation.

6.2.3 Utilize incident action plans (IAPs), given an incident or planned event utilizing ICS, the NIMS/ICS, *Emergency Responder Field Operations Guide*, and the IAP for the incident or event, so that the ICS organization is understood, the safety messages are adhered to, the division or group assignments are identified, and the communications plan is followed.

(A) Requisite Knowledge. ICS 100, *Introduction to the Incident Command System*; ICS 200, *Basic Incident Command System for Initial Response*; ICS 700, *An Introduction to the National Incident Management System*; ICS 800, *National Response Framework, an Introduction*; and any local, state or federal mutual aid agreements.

(B) Requisite Skills. Filling out incident forms and documentation.

6.2.4 Recognize existing mutual or automatic aid agreements, given an incident or planned event utilizing ICS and any existing agreements or contracts for automatic and mutual aid, so that resources are utilized appropriately and in accordance with these agreements.

(A) Requisite Knowledge. ICS 100, *Introduction to the Incident Command System*; ICS 200, *Basic Incident Command System for Initial Response*; ICS 700, *An Introduction to the National Incident Management System*; ICS 800, *National Response Framework, an Introduction*; and any local, state, or federal mutual aid agreements.

(B) Requisite Skills. Filling out incident forms and documentation.

6.3 Resource Ordering and Tracking. Utilize the standards and terminology of a resource ordering system according to the job performance requirements of 6.3.1 through 6.3.3.

6.3.1 Identify resource typing for aircraft, equipment, and overhead, given an incident or planned event utilizing ICS, the NIMS/ICS, *Emergency Responder Field Operations Guide*, and a list of resources assigned to the incident, so that all the resources are tracked as to their role or type and location and status.

(A) Requisite Knowledge. Mutual aid coordination system (MACS), a resource ordering system, and organizational structure at the local, state, or national level as appropriate.

(B) Requisite Skills. Computer use.

6.3.2 Utilize a resource ordering system, given an incident or planned event utilizing ICS and access to a resource ordering system, so that all the resources and event activity are tracked and the status is correct and visible to the system.

(A) Requisite Knowledge. MACS, a resource ordering system, and organizational structure at the local, state, or national level as appropriate.

(B) Requisite Skills. Computer use.

6.3.3 Work with outside agencies, given an incident or planned event utilizing ICS and a resource ordering system, so that all the participating agencies are aware of outstanding requests, pending requests, and requests that are unable to be filled.

(A) Requisite Knowledge. MACS, a resource ordering system, and organizational structure at the local, state, or national level as appropriate.

(B) Requisite Skills. Computer use.

6.4 Response to Incidents. Prepare for and respond to incidents to fulfill the job of Incident/Tactical Dispatcher according to the job performance requirements of 6.4.1 through 6.4.4.

6.4.1 Assemble a travel kit, given knowledge of potential circumstances in which an Incident/Tactical Dispatcher will be placed, so that he or she is able to function effectively in the position under most circumstances.

(A) Requisite Knowledge. Travel kit inventory information included in the Incident/Tactical Dispatcher class and ability to operate in austere conditions.

(B) Requisite Skills. Map reading and efficient packing skills.

6.4.2 Obtain requests for assignment, given an incident or planned event, so that the location, order and request number, and any routing information is obtained.

(A) Requisite Knowledge. Travel kit inventory information included in the Incident/Tactical Dispatcher class and ability to operate in austere conditions.

(B) Requisite Skills. Map reading and efficient packing skills.

6.4.3 Identify travel plans, given an incident or planned event, so that means of travel are identified and the best route information is used.

(A) Requisite Knowledge. Travel kit inventory information included in the Incident/Tactical Dispatcher class and ability to operate in austere conditions.

(B) Requisite Skills. Map reading and efficient packing skills.

6.4.4 Check in at an incident, given an incident or planned event, so that the individual is documented as being at the incident.

(A) Requisite Knowledge. Travel kit inventory information included in the Incident/Tactical Dispatcher class and ability to operate in austere conditions.

(B) Requisite Skills. Map reading and efficient packing skills.

6.5 Assume Position Responsibilities. Take on the job responsibilities of an Incident/Tactical Dispatcher according to the job performance requirements of 6.5.1 through 6.5.5.

6.5.1 Determine readiness for assignment, given an incident or planned event, so that the individual is prepared to begin work as soon as is needed for the event.

(A) Requisite Knowledge. Radio systems and terminology, telephone systems, and computer systems.

(B) Requisite Skills. Computer use and multitasking.

6.5.2 Show the availability and capabilities of resources, given an incident or planned event, so that the resources are able to function in the communications unit.

(A) Requisite Knowledge. Radio systems and terminology, telephone systems, and computer systems.

(B) Requisite Skills. Computer use and multitasking.

6.5.3 Gather, update, and apply situational information, given an incident or planned event, so that all the resources are tracked and the individual is able to respond quickly and efficiently to situations that might arise.

(A) Requisite Knowledge. Radio systems and terminology, telephone systems, and computer systems.

(B) Requisite Skills. Computer use and multitasking.

6.5.4 Build relationships with relevant personnel, given an incident or planned event, so that members of the communications unit can work as a team and so that other incident personnel are familiar with the needs of the communications unit.

(A) Requisite Knowledge. Radio systems and terminology, telephone systems, and computer systems.

(B) Requisite Skills. Computer use and multitasking.

6.5.5 Show the ability to use the tools necessary to complete an assignment, given an incident or planned event, so that all equipment and other available resources are utilized to their maximum efficiency.

(A) Requisite Knowledge. Radio systems and terminology, telephone systems, and computer systems.

(B) Requisite Skills. Computer use and multitasking.

6.6 Communicate as the Incident Directs. Receive and pass information accurately according to the job performance requirements of 6.6.1 through 6.6.3.

6.6.1 Gather relevant information during briefings and debriefings, given an incident or planned event, so that the individual and communications unit is aware of the current and future situations and plans.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Interpersonal communication.

6.6.2 Prepare documentation, given an incident or planned event, so that it is complete and the disposition is appropriate.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Interpersonal communication.

6.6.3 Determine work expectations, given an incident or planned event and input from a supervisor, so that communications are effective and work is completed.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Interpersonal communications.

6.7 Ensure Completion of Assigned Actions to Meet Identified Objectives. Perform tasks and processing requests according to the job performance requirements of 6.7.1 through 6.7.3.

6.7.1 React to situations, given an incident or planned event, so that the appropriate action is based on situational information and prescribed procedures.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, and demobilization procedures.

(B) Requisite Skills. Computer use and completion of forms.

6.7.2 Explain position duties to on-coming shifts, given an incident or planned event, so that there is a continuity of authority and knowledge.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, and demobilization procedures.

(B) Requisite Skills. Computer use and completion of forms.

6.7.3 Prepare for demobilization, given an incident or planned event, so that demobilization procedures are followed.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, and demobilization procedures.

(B) Requisite Skills. Computer use and completion of forms.

6.8 Receiving Information. Receive information from multiple sources according to the job performance requirements of 6.8.1 through 6.8.5.

6.8.1 Gather information by radio, given an incident or planned event, so that all pertinent information is obtained.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, IAP, and medical plans.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.8.2 Obtain information by telephone, given an incident or planned event, so that all pertinent information is gathered.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, IAP, and medical plans.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.8.3 Collect information in person, given an incident or planned event, so that all pertinent information is obtained.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, IAP, and medical plans.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.8.4 Paraphrase unit activity, given an incident or planned event, so that all appropriate ICS forms are completed in a timely manner.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, IAP, and medical plans.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.8.5 React to medical events, given an incident or planned event, so that all appropriate resources are dispatched and all appropriate personnel are notified.

(A) Requisite Knowledge. NIMS and ICS structure and terminology, Incident/Tactical Dispatcher position responsibilities, IAP, and medical plans.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.9 Processing Information. Process the information received according to the job performance requirements of 6.9.1 through 6.9.3.

6.9.1 Identify where information goes to people and agencies within and outside the incident, given an incident or planned event, so that the information is passed on quickly and efficiently.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.9.2 Identify information in weather reports, given an incident or planned event, so that the information can be passed on to the resources in the field when requested or directed.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.9.3 Recognize information in fire behavior reports and field interactions, given an incident or planned event, so that pertinent information contained in those reports on interactions can be relayed to personnel.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.10 Disseminating Information. Release information according to the job performance requirements of 6.10.1 and 6.10.2.

6.10.1 Record incident information, given an incident or planned event, so that the appropriate ICS forms are completed in an accurate and timely manner.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.10.2 Notify field resources of pertinent information via radio, telephone, or written message, given an incident or planned event, so that personnel are aware.

(A) Requisite Knowledge. NIMS and ICS structure and terminology and Incident/Tactical Dispatcher position responsibilities.

(B) Requisite Skills. Use of technology as provided by the AHJ.

6.11 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

6.11.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the

National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 7 Public Safety Communications Training Officer (NFPA 1061)

7.1* General. The Communications Training Officer (CTO) shall meet the job performance requirements defined in Sections 7.2 through 7.5 of this standard.

7.2 Personal Conduct.

7.2.1 Apply the AHJ's mission, given the mission statement and the principles of leadership as defined by the AHJ, so that duties are articulated both formally and informally.

(A) Requisite Knowledge. The values and ethics that form the basis of competency and AHJ practices and programs that define professional conduct.

(B) Requisite Skills. Operational and technological competence, as defined by the AHJ, and effective problem solving.

7.2.2 Project behavior, given the established code of ethics defined by the AHJ both formally and informally, so that the CTO serves as a role model.

(A) Requisite Knowledge. The values and ethics that form the basis of accepted behavior as defined by the AHJ.

(B) Requisite Skills. Self-restraint, discretion, a positive attitude, objectivity, and confidentiality.

7.2.3 Resolve conflicts, given established methods and procedures, so that disagreements are settled in a fair and objective manner for both parties.

(A) Requisite Knowledge. Conflict resolution models, relevant standard operating procedures, labor agreements, and other available resources.

(B) Requisite Skills. Mediation and negotiation.

7.3 Program Management.

7.3.1 Assemble course materials, given a specific topic, so that the lesson plan and all materials, resources, and equipment needed to deliver the lesson are obtained.

(A) Requisite Knowledge. The components of a lesson plan, policies and procedures for the procurement of materials and equipment, and resource availability.

(B) Requisite Skills. Basic computer skills.

7.3.2 Review and adapt instructional materials, given the materials for a specific topic, target audience, and learning environment, so that elements of the lesson plan, learning environment, and resources that need adaptation are identified.

(A) Requisite Knowledge. Recognition of student limitations, methods of instruction, types of resource materials, organization of the learning environment, and policies and procedures.

(B) Requisite Skills. Analysis of resources, facilities, and materials.

7.3.3 Prepare documentation and a file management system as prescribed by the AHJ, given the need to track trainee performance, so that accurate records are able to be referenced.

(A) Requisite Knowledge. Types of records and reports required and policies and procedures for processing records and reports.

(B) Requisite Skills. Basic computer skills, spreadsheet manipulation, and basic report writing and record completion.

7.4 Instructional Delivery.

7.4.1 The delivery of instructional sessions, given prepared course materials and environments, so that learning objectives are met.

(A) Requisite Knowledge. Prepared lesson plans specific to a topic, environmental advantages and limitations, and classroom management and safety.

(B) Requisite Skills. Use of instructional media and materials.

7.4.2 Provide on-the-job training, given an operating telecommunications position that can accommodate both the trainer and trainee, so that the CTO can observe and intervene as needed while the trainee interacts in a live environment and performs the duties for which they are being trained.

(A) Requisite Knowledge. Skill level of the trainee and safety of the caller in an emergency situation.

(B) Requisite Skills. The ability to recognize the use and limitations of any specialized dual-use telecommunications equipment and to assess the need to intervene when required.

7.4.3 The delivery of continuing education, given prepared course materials, so that competency levels are maintained in a consistent fashion.

(A) Requisite Knowledge. Training sunset dates for assigned employees, minimum requirements to maintain certification(s), prepared lesson plans specific to a topic, environmental advantages and limitations, and classroom management and safety.

(B) Requisite Skills. File management and use of instructional media and materials.

7.4.4 Schedule ride-along sessions with field personnel, given regular interaction with field units, so that the trainee gains insight into the duties, situations, and limitations experienced by the personnel who are being dispatched by that trainee.

(A) Requisite Knowledge. Personalities and duties of crews and safety.

(B) Requisite Skills. Basic scheduling.

7.5 Evaluation and Testing.

7.5.1 Administer oral, written, and performance tests, given the lesson plan, evaluation instruments, and the evaluation procedures of the agency, so that the testing is conducted according to procedures and the security of the materials is maintained.

(A) Requisite Knowledge. Test administration, agency policies, laws affecting records and disclosure of training information, the purposes of evaluation and testing, and performance skills evaluation.

(B) Requisite Skills. Use of skills checklists and oral questioning techniques.

7.5.2 Grade student tests — oral, written, or performance — given answer sheets and answer keys or skills checklists, so that the examinations are graded and secured.

(A) Requisite Knowledge. Procedures related to test security and record keeping.

(B) Requisite Skills. Grading and maintaining the confidentiality of scores.

7.5.3 Report test results, given a set of test answer sheets or skills checklists, a report form, and policies and procedures for reporting, so that the results are accurately recorded, the forms are forwarded according to procedure, and unusual circumstances are reported.

(A) Requisite Knowledge. Reporting procedures and interpretation of test results.

(B) Requisite Skills. Communication skills and basic coaching.

7.5.4 Provide feedback to the trainee, given comprehensive test and evaluation results, so that the trainee is able to distinguish correct performance.

(A) Requisite Knowledge. Interpersonal relations and AHJ policies and procedures.

(B) Requisite Skills. Presentation and conflict resolution.

7.5.5 Identify transition periods, given the completion of identified training goals, so that accurate recommendations for progression, remediation, or termination are achieved.

(A) Requisite Knowledge. Test and evaluation results, documented daily performance reports, reported policy violations, exemplary performance reports, and AHJ-defined minimum training requirements.

(B) Requisite Skills. Analysis of work performance and decision making.

7.6 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

7.6.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 8 Public Safety Communications Supervisor (NFPA 1061)

8.1* General. The Public Safety Communications Supervisor shall meet the requirements of Public Safety Telecommunicator II and meet the job performance requirements as defined in Sections 8.2 through 8.6.

8.2 Human Resource Management. Utilize human resources to accomplish assignments in an efficient, safe manner. Evaluate member performance and supervise personnel during emergency and nonemergency work periods according to the following job performance requirements.

8.2.1 Assign tasks or responsibilities to telecommunicators, given requests for service, so that all aspects of a request for service are handled in a proficient and professional manner.

(A) Requisite Knowledge. Verbal communications during emergency situations, techniques used to create assignments under stressful situations, and methods used to confirm understanding.

(B) Requisite Skills. The ability to condense instructions for frequently assigned tasks based on training, standard operating procedures, guidelines, or protocols as determined by the AHJ.

8.2.2 Evaluate telecommunicator actions to identify performance problems, given a telecommunicator with a situation requiring assistance and the member assistance policies and procedures, so that the situation is identified and so that the actions taken are within the established policies and procedures.

(A) Requisite Knowledge. The signs and symptoms of telecommunicator-related problems, causes of stress in public safety communications personnel, and the adverse effects of stress on the performance of public safety communications personnel.

(B) Requisite Skills. The ability to recommend a course of action for a telecommunicator in need of assistance.

8.2.3 Administer human resource policies and procedures, given a situation requiring action, so that the needs of the agency are met.

(A) Requisite Knowledge. Human resource policies and procedures.

(B) Requisite Skills. The ability to communicate orally and in writing and to document a situation and any actions taken toward a resolution.

8.2.4 Coordinate the completion of assigned tasks and projects by telecommunicators, given a list of projects and tasks pursuant to job requirements, so that assignments meet agency objectives.

(A) Requisite Knowledge. Delegation, project management, principles of supervision, and basic human resource management.

(B) Requisite Skills. The ability to plan, set priorities, and follow up.

8.3 Community Relations. Respond to inquiries from the community.

8.3.1 Initiate action on a citizen's question or concern, given policies and procedures, so that the question or concern is answered or referred to the correct individual for action and so that all policies and procedures are complied with.

(A) Requisite Knowledge. Interpersonal relationships and appropriate customer service techniques.

(B) Requisite Skills. The ability to effectively communicate with customers, peers, and others in a reasonable and logical manner.

8.4 Administration. Perform general administrative functions and coordinate the implementation of public safety communication center policies and procedures at the supervisor level.

8.4.1 Recommend changes to existing departmental policies, given a departmental policy, so that the policy meets the agency's changing needs.

(A) Requisite Knowledge. Existing policies and procedures and changes in day-to-day operations.

(B) Requisite Skills. The ability to evaluate existing policies and procedures for relevancy and to communicate recommended changes.

8.4.2 Implement changes to departmental policies, given a new or changed departmental policy, so that the policy is communicated to and understood by telecommunicators.

(A) Requisite Knowledge. Policies and procedures and changes in day-to-day operations.

(B) Requisite Skills. The ability to evaluate existing policies and procedures for relevancy, to communicate recommended changes, and to engage in written and oral communication.

8.4.3 Conduct routine administrative functions, given forms and record-management systems, so that the reports and logs are complete and the files are maintained in accordance with policies and procedures.

(A) Requisite Knowledge. Administrative policies and procedures and records management systems.

(B) Requisite Skills. Generating reports, analyzing data, using agency software programs, and communicating findings either orally or in writing.

8.5 Equipment and Systems Operations. Monitor the operational integrity of complex and interrelated systems, technologies, and processes that support emergency communications within the agency and take action as approved or directed by the AHJ.

8.5.1 Monitor the operating systems and interfaces, given the relevant policies, procedures, and monitoring tools, so that there is no degradation or interruption in service to ensure the continuity of operations.

(A) Requisite Knowledge. Systems operations, policies and procedures, and operation of the monitoring tools.

(B) Requisite Skills. Interpreting and communicating the findings of device indicators.

8.5.2 Coordinate equipment repairs with technical staff or appropriate resources, given a system malfunction or failure, so that the situation is remedied as defined and authorized by the AHJ.

(A) Requisite Knowledge. Equipment repair resource list and troubleshooting guides.

(B) Requisite Skills. Troubleshooting techniques.

8.6 Health and Safety. Integrate safety plans, policies, and procedures into daily activities in accordance with the requirements of the AHJ.

8.6.1 Apply safe practices in the public safety communications center as defined by the AHJ, given safety policies and procedures, so that all applicable reporting is completed, in-service training is conducted, and responsibilities are conveyed to personnel.

(A) Requisite Knowledge. The common causes of personal injury and accidents, safety policies and procedures, and basic workplace safety.

(B) Requisite Skills. The ability to identify and act to mitigate safety hazards.

8.6.2 Document the events leading up to and the potential causes of an accident, given an incident and any applicable forms, so that the incident is documented and reports are processed in accordance with policies and procedures.

(A) Requisite Knowledge. Procedures for reporting an accident and safety policies and procedures.

(B) Requisite Skills. The ability to document an accident in an accurate manner and to conduct interviews objectively.

8.7 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

8.7.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 9 Public Safety Quality Assurance/Improvement Personnel (NFPA 1061)

9.1* General. To qualify as Quality Assurance/Improvement Personnel, a candidate shall meet the job performance requirements defined in Section 9.2 through 9.7.1 of this standard.

9.2 Review Calls for Service. Perform or utilize human resources to accomplish assignments when reviewing calls for service. Evaluate communication center member performance during emergency and nonemergency work periods.

9.2.1 Conduct random review of calls for service received by communication center members, given a request for service or assistance, so that the request is received and prioritized, safety considerations are addressed, and the desired outcomes are conveyed in accordance with the information management system utilized by the AHJ.

(A) Requisite Knowledge. Verbal communication during emergency and nonemergency calls for service, techniques to verify and collect information under stressful and nonstressful situations, and methods for confirming those techniques.

(B) Requisite Skills. The ability to provide written or electronic reports for reviewed calls for service and to meet the minimum call review requirements utilized by the AHJ.

9.3 Feedback. Perform or utilize human resources to accomplish assignments to provide feedback to communication center personnel from reviewed calls for service.

9.3.1 Conduct a review of calls for service received by communication center members, given a call for service report, so that the desired outcomes are conveyed in accordance with the information management system utilized by the AHJ in a timely and accurate manner.

(A) Requisite Knowledge. Written and verbal communication.

(B) Requisite Skills. The ability to provide written and verbal communication in a generous, empathic, and calm demeanor using interpersonal skills in a methodical and organized manner to convey the desired results and using the information management system utilized by the AHJ.

9.4 Remediation.

9.4.1 Recommend action for member-related problems requiring remediation training, given a member with a situation requiring assistance and the member assistance policies and procedures, so that the situation is identified and the actions taken are within the established policies and procedures.

(A) Requisite Knowledge. The signs and symptoms of member-related problems, causes of stress in emergency services personnel, adverse effects of stress on the performance of emergency service personnel, and awareness of AHJ member assistance policies and procedures.

(B) Requisite Skills. The ability to recommend a course of action for a member in need of assistance.

9.5 Data Management. Coordinate communication center projects, research, and studies by organizing, retrieving, and filing calls for service data. This will necessarily involve working with data-processing personnel to meet state, national, and agency-related needs.

9.5.1 Collect calls for service data, given the goals and mission of the organization, so that communication center reports are timely and accurate.

(A) Requisite Knowledge. The information management system utilized by the AHJ.

(B) Requisite Skills. Written and verbal communication and state, national, and local agency computer software and reports utilized by the AHJ.

9.6 Continuing Education. Utilize communication center data and results from reviewed calls for service, along with the implementation of new communication center policies and procedures, to develop and deliver continuing education.

9.6.1 Direct communication center members during a training evolution, given a training evolution and training policies and procedures, so that the evolution is performed in accordance with safety plans efficiently and as directed.

(A) Requisite Knowledge. Verbal communication techniques to facilitate learning.

(B) Requisite Skills. The ability to distribute issue-guided directions to unit members during training evolutions.

9.7 Credentialing. Maintain certifications, licenses, accreditations, and performance benchmarks that are required by all communication center personnel and others required by the AHJ.

9.7.1 Schedule and recommend training, given the communication center personnel certification and other certification required by the AHJ, so that all personnel will meet and maintain all required training within the agency's established policies and procedures.

(A) Requisite Knowledge. Verbal communication during emergency and nonemergency calls for service, techniques used to verify and collect information under stressful and nonstressful situations, and methods of confirming those techniques.

(B) Requisite Skills. The ability to provide written or electronic reports on reviewed calls for service and to meet the minimum call review requirements utilized by the AHJ.

9.8 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

9.8.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual

when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 10 Public Safety Communications Training Coordinator (NFPA 1061)

10.1* General. The Communications Training Coordinator shall meet the requirements for Communications Training Officer and the job performance requirements defined in Sections 10.2 through 10.6 of this standard.

10.2 Program Management.

10.2.1 Recommend budget needs, given training goals, AHJ budget policy, and current resources so that the resources required to meet training goals are identified and documented. [**1041:**5.2.3]

(A) Requisite Knowledge. AHJ budget policy, resource management, needs analysis, sources of instructional materials, and equipment. [**1041:**5.2.3(A)]

(B) Requisite Skills. Resource analysis and preparation of supporting documentation. [**1041:**5.2.3(B)]

10.2.2 Gather training resources, given an identified need, so that the resources are obtained within established timelines, budget constraints, and according to AHJ policy. [**1041:**5.2.4]

(A) Requisite Knowledge. AHJ policies, purchasing procedures, and budget. [**1041:**5.2.4(A)]

(B) Requisite Skills. Records completion. [**1041:**5.2.4(B)]

10.3 Develop Curricula.

10.3.1 Create a lesson plan, given a topic, learner characteristics, and a lesson plan format, so that learning objectives, a lesson outline, course materials, instructional technology tools, an evaluation plan, and learning objectives for the topic are addressed. [**1041:**5.3.2]

(A) Requisite Knowledge. Elements of a lesson plan, components of learning objectives, instructional methodology, student-centered learning, methods for eliminating bias, types and application of instructional technology tools and techniques, copyright law, and references and materials. [**1041:**5.3.2(A)]

(B) Requisite Skills. Conduct research, develop behavioral objectives, assess student needs, and develop instructional technology tools; lesson outline techniques, evaluation techniques, and resource needs analysis. [**1041:**5.3.2(B)]

10.3.2 Modify an existing training topic, given an existing lesson plan, so that the topic remains relevant and the technology is updated to standards set by the AHJ.

(A) Requisite Knowledge. Thorough knowledge of the existing lesson plan, improvements in industry standards and equipment, and improvements in instructional media.

(B) Requisite Skills. Research skills.

10.3.3 Create a remediation strategy, given an evaluation report indicating the need for further training, so that trainees failing to meet the lesson plan standards are given additional training.

(A) Requisite Knowledge. Minimum accepted competency levels established by the AHJ, specific evaluation results of trainees recommended for remediation, and training strategies for varied learning styles.

(B) Requisite Skills. None.

10.4 Maintain Training Schedule and Staff.

10.4.1 Maintain a continuing education training schedule, given an established lesson plan, so that training is ongoing and that continuing education objectives are met.

(A) Requisite Knowledge. Lesson plan topics; certification expiration dates; and AHJ, state, and federal minimum training requirements/certifications.

(B) Requisite Skills. Prioritization and records management.

10.4.2 Schedule Communications Training Officers (CTOs) to conduct training, given a roster of certified CTOs, so that all CTOs are able to instruct regularly and maintain competency.

(A) Requisite Knowledge. A current list of classes instructed by all CTOs and the strengths and weaknesses of each trainer in regard to instructional skills.

(B) Requisite Skills. Personnel management, evaluation skills, and record keeping.

10.4.3 Schedule instructional sessions, given the AHJ's scheduling policy, instructional resources, staff, facilities, and timeline for delivery, so that the specified sessions are delivered according to department policy.

(A) Requisite Knowledge. AHJ, state, and federal minimum training requirements/certifications; scheduling processes; supervision techniques; and resource management.

(B) Requisite Skills. None.

10.4.4 Select instructional staff, given personnel qualifications, instructional requirements, and AHJ policies and procedures, so that staff selection meets AHJ policies and achievement of AHJ and instructional goals. [**1041:**6.2.4]

(A) Requisite Knowledge. AHJ policies regarding staff selection, instructional requirements, selection methods, the capabilities of instructional staff, and agency goals. [**1041:**6.2.4(A)]

(B) Requisite Skills. Evaluation techniques and interview methods. [**1041:**6.2.4(B)]

10.5 Document Training.

10.5.1 Administer a training record system, given AHJ policy and type of training activity to be documented, so that the information captured is concise, meets all AHJ and legal requirements, and can be accessed. [**1041:**6.2.2]

(A) Requisite Knowledge. AHJ policy, record-keeping systems, professional standards addressing training records, legal requirements affecting record keeping, and disclosure of information. [**1041:**6.2.2(A)]

(B) Requisite Skills. Development of records and report generation. [**1041:**6.2.2(B)]

10.5.2 Regularly review CTO reports and trainee evaluations, given regular reporting, so that training progress is monitored and negative trends are quickly recognized and corrected.

(A) Requisite Knowledge. The results of regular reports and evaluations.

(B) Requisite Skills. None.

10.6 Evaluation and Testing.

10.6.1 Develop student evaluation instruments, given learning objectives, learner characteristics, and training goals, so that the evaluation instrument measures whether the student has achieved the learning objectives. [**1041:**5.5.2]

(A) Requisite Knowledge. Evaluation methods, evaluation instrument development, and assessment of validity and reliability. [**1041:**5.5.2(A)]

(B) Requisite Skills. Evaluation item construction and assembly of evaluation instruments. [**1041:**5.5.2(B)]

10.6.2 Develop a class evaluation instrument, given AHJ policy and evaluation goals, so that students have the ability to provide feedback on instructional methods, communication techniques, learning environment, course content, and student materials. [**1041:**5.5.3]

(A) Requisite Knowledge. Training evaluation methods. [**1041:**5.5.3(A)]

(B) Requisite Skills. Development of training evaluation forms. [**1041:**5.5.3(B)]

10.6.3 Analyze student evaluation instruments, given test data, objectives, and AHJ policies, so that validity and reliability are determined and necessary changes are made. [**1041:**6.5.5]

(A) Requisite Knowledge. AHJ policies and applicable laws, test validity, reliability, and item analysis methods. [**1041:**6.5.5(A)]

(B) Requisite Skills. Item analysis. [**1041:**6.5.5(B)]

10.6.4 Construct a performance-based instructor evaluation plan, given AHJ policies and procedures and job requirements, so that instructors are evaluated at regular intervals, following AHJ policies. [**1041:**6.2.5]

(A) Requisite Knowledge. Evaluation methods, employment laws, AHJ policies, staff schedules, and job requirements. [**1041:**6.2.5(A)]

(B) Requisite Skills. Evaluation techniques, scheduling, technical writing. [**1041:**6.2.5(B)]

10.6.5 Present evaluation findings, conclusions, and recommendations to AHJ administrator, given data summaries and target audience, so that recommendations are unbiased, supported, and reflect AHJ goals, policies, and procedures. [**1041:**6.2.8]

(A) Requisite Knowledge. Statistical analysis and AHJ goals. [**1041:**6.2.8(A)]

(B) Requisite Skills. Presentation skills and report preparation following AHJ guidelines. [**1041:**6.2.8(B)]

10.6.6 Develop a program evaluation plan, given AHJ policies and procedures, so that instructors, course components, program goals, and facilities are evaluated, student input is obtained, and needed improvements are identified. [**1041:**6.5.4]

(A) Requisite Knowledge. Evaluation methods and AHJ goals. [**1041:**6.5.4(A)]

(B) Requisite Skills. Construction of evaluation instruments, technical writing. [**1041:**6.5.4(B)]

10.7 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

10.7.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 11 Public Safety Communications Center Manager/Director (NFPA 1061)

11.1* General.

11.1.1 The Public Safety Communications Center Manager/Director shall have the requisite knowledge of the positions in the public safety communications center.

11.1.2 The AHJ shall be able to request additional educational background, technical experience and the job performance requirements defined in Sections 11.2 through 11.5 of this standard.

11.1.3 The Public Safety Communications Center Manager/Director shall have the requisite knowledge of the organizational structure of both the department and the department's organizational structure within the AHJ; the geographical configuration and political influences within the boundaries; administration of the department's budget development and implementation; development and implementation of the department's policies and procedures; and management of all personnel within the communications center.

11.2 Human Resource Management.

11.2.1 Administer communication center members during daily operations, given minimum staffing levels established by the AHJ, so that the communication center meets the performance goals in accordance with local policies, procedures, and protocols established by the AHJ.

(A) Requisite Knowledge. The communication process for shift assignments, shift replacement, and emergent situations.

(B) Requisite Skills. The ability to coordinate shift coverage with peak needs, manage allocated time off, and follow labor/management agreements within the public safety communications center.

11.3 Public Safety Communications Center Operations.

11.3.1 Create operational plans to include daily activities, given an area of responsibility as determined by the AHJ, so that daily activities that include emergency procedures both outside the center and within the center following federal, state, provincial, and local guidelines — including any mission statement or goals — are met as established by the AHJ.

(A) Requisite Knowledge. Comprehensive understanding of operational plans, applicable legal requirements and regulations, and positive professional development opportunities.

(B) Requisite Skills. Verbal and written communications skills to develop, implement, and evaluate operational plans, federal legislation, and the local requirements necessary to manage the center and to encourage and support professional development.

11.4 Stakeholder Relationships.

11.4.1 Create a working relationship, given the varied stakeholders involved in a communications center, so that all stakeholders' concerns are met using positive feedback and a team environment.

(A) Requisite Knowledge. The needs of external stakeholders and the needs of the personnel within the center and an understanding of personal and governmental influences and other agencies that can affect operations within the center.

(B) Requisite Skills. The ability to communicate with stakeholders at an appropriate level, understand people and their agendas, administer discipline to internal stakeholders if necessary, and create a positive team environment.

11.5 Coordinate Technologies.

11.5.1 Understand the systems used within the communications center, given the updates and improvements to technology, so that a request for capital improvements can be added to the budget process.

(A) Requisite Knowledge. A basic understanding of what technology is used in the center, having a support network to advise of changing technology, and making appropriate recommendations.

(B) Requisite Skills. Technological understanding, communications skills, and the ability to translate the information into lay terms so that stakeholders can make informed decisions.

11.6 Fellow Employee Exhibiting Signs and Symptoms of Emotional and Behavioral Distress.

11.6.1 Identify signs and symptoms of emotional and behavioral health distress of an individual in crisis, given an individual exhibiting signs and symptoms of emotional and behavioral health distress in a peer setting and policies and procedures to be initiated with an awareness level education in emotional and behavioral health distress so that the emotional or behavioral health distress issue is recognized, confidentiality is maintained within the guidelines of the AHJ, communication is open, nonjudgmental awareness is retained, a department or community-based program is made accessible, and assistance is offered or an appropriate referral is initiated.

(A) Requisite Knowledge. Emotional and behavioral health distress signs and symptoms, such as anxiety, stress, depression, addictions, or suicidal thoughts or behaviors; knowledge of the programs within the department or within the community, including, but not limited to, employee assistance programs (EAP), community mental health programs, chaplains, and the National Suicide Prevention Lifeline to help an individual when emotional or behavioral health distress is noticed; and how to listen and when to communicate.

(B) Requisite Skills. The ability to approach an individual exhibiting signs of emotional or behavioral distress; to use empathic and listening skills; and to refer an individual to an EAP, community mental health program, chaplain, the National Suicide Prevention Lifeline, or an individual trained in emotional and behavioral health.

Chapter 12 Communications Centers (NFPA 1221)

12.1 Administration.

12.1.1 Scope.

12.1.1.1 Chapters 12 through 23 shall cover the installation, performance, operation, and maintenance of public emergency services communications systems and facilities.

12.1.1.2 Chapters 12 through 23 shall not be used as a design specification manual or an instruction manual.

12.1.2 Purpose. The purpose of Chapters 12 through 23 shall be as follows:

(1) To specify operations, facilities, and communications systems that receive events from the public
(2) To provide requirements for the retransmission of such events 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

12.1.2.1 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*.

12.1.2.2 Emergency reporting systems that are not covered by Chapters 12 through 23 shall be in accordance with *NFPA 72*.

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

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

12.1.3.1 The communication systems listed in Section 12.1.3 shall provide the following functions:

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

12.1.4 Retroactivity.

12.1.4.1 Unless otherwise noted, it is not intended that the provisions of Chapters 12 through 23 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.

12.1.4.2 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 Chapters 12 through 23.

12.1.4.3 The portions of this standard that shall be applied retroactively are listed in Table 12.1.4.3, Retroactivity.

12.2 General.

12.2.1* Communications centers and alternate communications centers shall comply with Chapter 12.

Table 12.1.4.3 Retroactivity

Chapter	Retroactive
1	N/A
2	N/A
3	Yes
12	12.2, 12.6.1, 12.6.2, 12.6.5–12.6.7
13	No
14	No
15	Yes
16	Yes
17	No
18	No
19	No
20	Yes
21	Yes
22	Yes
23	No

12.2.2* A comprehensive emergency management plan (CEMP) shall be in place for each communications center.

12.2.2.1 The CEMP shall comply with the applicable requirements of *NFPA 1600* and additional requirements specified in this document.

12.2.2.2 The AHJ shall review the CEMP for currency and applicability annually.

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

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

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

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

12.2.3 When provided, remote communications facilities shall comply with Section 12.11.

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

12.2.5 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).

12.2.5.1 Each center shall be provided with an alternate means of communication that is compatible with the alternate means of communication provided at the ERFs.

12.2.5.2 The alternate means shall be available to the telecommunicator in the event of failure of the primary communications system.

12.2.6* Each jurisdiction shall maintain an alternate communications center that meets the criteria in 12.2.6.1 and 12.2.6.2.

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

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

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

12.2.6.3.1 The plan shall include the ability to reroute incoming event and alarm traffic to the alternate center and to process and dispatch events at that center.

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

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

12.2.7* 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.

12.2.8 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).

12.2.9* Communications centers shall be designed to accommodate the staffing level necessary to operate the center as required by Chapter 15.

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

12.3 Exposure Hazards.

12.3.1 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.

12.3.2* 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.

12.3.3* The lowest floor elevation of the communications center shall be above the 500-year flood plain established by the Federal Emergency Management Agency.

12.4 Construction.

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

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

12.4.3 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.

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

12.4.5* Communications centers shall not be located below grade unless the elevation of the lowest floor in the facility is above the 500-year flood plain.

12.4.6 Communications centers located below grade shall comply with 11.7.3 of NFPA *101* and be specifically designed for the location.

12.4.7 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*.

12.4.8 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.

12.4.9 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 12.7.

12.4.9.1* 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.

12.4.10 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.

12.5 Climate Control.

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

12.5.1.1 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.

12.5.1.1.1* 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.

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

12.5.1.3* 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.

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

12.5.1.5* 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.

12.5.1.6 Backup or redundant HVAC units shall be capable of receiving power from all power sources required by Section 12.8.

12.5.1.7* 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.

12.5.1.8* Primary and backup HVAC systems shall be capable of operating from the normal power source required by 12.8.2 and the alternate power source required by 12.8.3.

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

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

12.6 Fire Protection.

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

12.6.2 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*.

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

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

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

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

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

12.7 Security.

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

12.7.2 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.

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

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

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

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

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

12.7.4 Where a communications center has windows, the requirements of 12.7.4.1 through 12.7.4.5 shall apply.

12.7.4.1 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.

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

12.7.4.3 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.

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

12.7.4.5* 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.

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

12.7.6 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).

12.7.7* As an alternative to 12.7.6, 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.

12.8 Power.

12.8.1 General. Each communications center shall be provided with a critical operations power system in compliance with *NFPA 70*.

12.8.1.1 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.

12.8.1.2 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.

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

12.8.1.4 In addition to the two power sources required by 12.8.1.2, a means for connecting a portable or vehicle-mounted generator shall be provided.

12.8.1.5* 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 12.8.3.2.

12.8.1.6* 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*.

12.8.2 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

12.8.3 Emergency Power Supply System.

12.8.3.1 The emergency power supply system shall consist of one or more engine-driven generators installed in accordance with *NFPA 70*.

12.8.3.2 Upon failure of primary power, transfer to the standby emergency supply system shall be automatic.

12.8.4* Engine-Driven Generators.

12.8.4.1 Engine-driven generators shall conform with the provisions of Chapter 4 of NFPA 37 and with NFPA 110.

12.8.4.2 Engine-driven generators shall conform with the provisions of NFPA 110, Type 10, Level 1, Class 72.

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

12.8.4.3* 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.

12.8.4.4 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.

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

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

12.8.4.6.1 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.

12.8.4.6.2 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 UL 752, *Standard for Bullet-Resistant Equipment*.

12.8.4.6.3 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.

12.8.4.7 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.

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

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

12.8.4.10 Natural gas installations shall comply with NFPA 54.

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

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

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

12.8.4.12.2 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.

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

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

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

12.8.4.15 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.

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

12.8.4.15.2 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.

12.8.5 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.

12.8.5.1 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.

12.8.5.2 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.

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

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

12.8.6 Surge Protective Devices (SPDs).

12.8.6.1* SPDs shall be provided in accordance with *NFPA 70*.

12.8.6.2 SPDs shall be installed in accordance with *NFPA 70* 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.

12.8.7* 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*.

12.8.8 Uninterruptible Power Supply (UPS) Systems.

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

12.8.8.2 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.

12.8.8.3* 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.)

12.8.8.4 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.

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

12.8.8.6 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.

12.8.8.7 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

12.9 Lighting.

12.9.1 General.

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

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

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

12.9.2 Emergency Lighting.

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

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

12.9.2.2 In addition to the requirement of 12.9.2.1, the operations room shall be equipped with redundant emergency lighting provided by individual unit equipment in accordance with *NFPA 70*.

12.9.2.3 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.

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

12.11 Remote Communications Facilities.

12.11.1 General.

12.11.1.1 Remote communications facilities, where provided, shall comply with Section 12.11.

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

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

12.11.2 Exposure Hazards.

12.11.2.1 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.

12.11.2.2* 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.

12.11.2.3 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.

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

12.11.2.5 Remote communications facilities shall be evaluated for wildland interface hazards in accordance with NFPA 1140.

12.11.3 Construction.

12.11.3.1 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.

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

12.11.3.3 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.

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

12.11.3.5 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.

12.11.3.6* Facilities located below grade shall be both of the following:

(1) Compliant with Section 11.7 of NFPA *101*
(2) Specifically designed for the location

12.11.3.7* 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*.

12.11.3.8* Interior floor finish inside a remote communications facility shall be of noncombustible material or comply with the requirements of NFPA *101* Class II for interior floor finish.

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

12.11.3.10 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.

12.11.4 Climate Control.

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

12.11.4.1.1 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.

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

12.11.4.1.3 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.

12.11.4.1.4 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.

12.11.4.1.5 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.

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

12.11.5 Fire Protection.

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

12.11.5.2 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*.

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

12.11.5.3 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.

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

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

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

12.11.6 Security.

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

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

12.11.6.3 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 UL 752, *Standard for Bullet-Resistant Equipment*.

12.11.6.4 The AHJ shall determine which type of door is most appropriate for each location.

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

12.11.6.6* Exterior walls shall provide resistance to direct small arms fire equivalent to Level 4 as defined in UL 752, *Standard for Bullet-Resistant Equipment*.

12.11.6.7* 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).

12.11.6.8* As an alternative to 12.7.6, 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.

12.11.6.9* 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.

12.11.7 Power.

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

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

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

12.11.7.2 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

12.11.7.3 Emergency Power Source.

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

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

12.11.7.4 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 12.8.4.

12.11.7.5* Engine-Driven Generators. Engine-driven generators shall comply with the requirements of NFPA 110 and the requirements of 12.8.4.

12.11.7.6* 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 12.8.5.

12.11.7.7 Surge Protective Devices (SPDs).

12.11.7.7.1 SPDs shall be provided in accordance with *NFPA 70*.

12.11.7.7.2* SPDs shall be provided in accordance with *NFPA 70* 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.

12.11.7.8* 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*.

12.11.8 Lighting.

12.11.8.1 General.

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

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

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

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

12.11.8.2 Emergency Lighting.

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

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

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

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

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

Chapter 13 Communication and Signal Wiring (NFPA 1221)

13.1 Circuit Construction and Arrangement.

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

13.1.2 As an alternative to 13.1.1, installation of outdoor circuitry shall be in accordance with IEEE C2, *National Electrical Safety Code*, where approved by the AHJ.

13.1.3 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.

13.1.3.1 Alternate communications centers shall comply with the requirements of Chapter 12.

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

13.1.5 Record drawings shall be provided as required by Chapter 21.

13.1.6 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.

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

13.1.8 The combination of public emergency services communication and signaling (C&S) circuits in the same cable with other circuits shall comply with 13.1.8.1 and 13.1.8.2.

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

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

13.2 Circuit Conductors.

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

13.2.2 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.

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

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

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

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

13.2.7 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.

13.3 Underground Cables.

13.3.1 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.

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

13.3.2 Underground cables installed in ducts, vaults, and manholes shall comply with 13.3.2.1 through 13.3.2.2.

13.3.2.1 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.

13.3.2.2 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.

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

13.3.4 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.

13.3.5 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.

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

13.3.7 Cable ends shall be sealed against moisture.

13.3.8 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.

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

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

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

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

13.4 Aerial Cable and Wire Construction.

13.4.1 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.

13.4.2 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.

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

13.4.4 Support of aerial cables shall comply with 13.4.4.1 and 13.4.4.2.

13.4.4.1 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

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

13.4.4.3 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.

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

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

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

13.4.8 Aerial cables extending down poles shall comply with 13.4.8.1 through 13.4.8.4.

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

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

13.4.8.3 The installation shall prevent water from entering the conduit.

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

13.5 Wiring Inside Buildings.

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

13.5.1.1 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.

13.5.2* 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)
(6) Metallic cable trays

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

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

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

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

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

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

13.5.5.3 Communications and signal circuits where installed in junction terminal boxes, enclosures, or other approved termination devices, shall be identified by the use of a distinctive color on covers or doors of such devices.

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

13.5.6 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*.

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

13.5.8 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.

13.5.9 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.

13.5.10 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

13.6 Surge Protection.

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

13.6.1.1 Grounded and ungrounded conductors that enter a communications center shall be protected by a surge-protective device (SPD).

13.6.1.2 Equipment grounding conductors and bonding jumpers shall not be connected to the SPD.

13.6.1.3* Wired communications circuits shall have an SPD installed at the point of entrance to the communications center.

13.6.1.4 Each conductor that enters a communications center from a partially or entirely aerial line shall be protected by an SPDs.

13.6.1.5 A surge protective device shall be required on all alternating-current electrical power circuits providing power to communications center equipment.

13.6.1.5.1 Surge protective devices for alternating-current power circuits shall have either audible alarm status notification or a dry contact circuit for remote notification status.

13.6.1.6 A surge protective device shall be required on all external metallic antenna cabling that directly terminates to communications center equipment.

13.6.1.7 A surge protective device is required on any data or signal communication circuits that are terminated between the fire alarm control system and communications center equipment.

13.6.2 All SPDs shall be connected to the single-point facility ground in accordance with *NFPA 70*.

13.6.3 The SPDs shall be either located in proximity to or combined with the cable terminals.

13.6.4 SPDs shall be designed and listed for the specific application.

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

13.6.6 All SPDs shall be accessible for maintenance and inspection.

13.6.7* Where the SPDs are located outside in damp or wet locations, their enclosures shall be watertight or protected from the weather.

13.6.8 Where the SPDs are located indoors, they shall be installed in a minimum NEMA Type 1 enclosure or enclosure listed for the unit.

13.6.9 At the junction points of open aerial conductors and cable, each conductor shall be protected by an SPD in accordance with 13.6.9.1 and 13.6.9.2.

13.6.9.1 The SPD shall be weatherproof or protected from the weather.

13.6.9.2 A connection shall be provided between the SPD ground and any metallic sheath and messenger wire.

13.6.10 Two-conductor cable circuits shall be protected by SPDs at intervals of approximately 2,000 ft (610 m).

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

13.7 Fuses.

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

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

13.7.3 Fuses shall be located only at the power source.

13.8 Grounding.

13.8.1* 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*.

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

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

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

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

Chapter 14 Emergency Response Facilities (NFPA 1221)

14.1 General. A primary and a secondary means of dispatch notification shall be provided at the ERF and comply with 14.1.1 and 14.1.2.

14.1.1 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.

14.1.2 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.

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

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

14.2 Commercial Telephone.

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

14.2.2* 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.

14.3 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.

14.3.1 Sprinkler systems shall comply with NFPA 13.

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

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

14.5 Lighting.

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

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

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

14.6.1 Circuit protection shall be in accordance with Section 13.6.

14.6.2 Lightning protection shall be in accordance with Section 12.10.

Chapter 15 Operations (NFPA 1221)

15.1 Management.

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

15.1.1.1 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.

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

15.1.1.2 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.

15.1.1.3 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.

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

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

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

15.2 Telecommunicator Qualifications and Training.

15.2.1 Telecommunicators shall meet the qualification requirements of Chapters 4 through 11 as appropriate for their position.

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

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

15.2.3 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

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

15.2.5 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.

15.2.6 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 Chapters 4 through 11, and Section 15.2.

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

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

15.3 Staffing.

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

15.3.1.1* The AHJ shall ensure that there are sufficient telecommunicators available to effect the prompt receipt and processing of alarms and events needed to meet the requirements of Section 15.4.

15.3.1.2* 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.

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

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

15.3.3 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.

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

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

15.3.4.2 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.

15.4 Operating Procedures.

15.4.1* Ninety-percent of events received on emergency lines shall be answered within 15 seconds, and 95 percent of events shall be answered within 20 seconds. *(For documentation requirements, see 21.5.2.)*

15.4.1.1 Compliance with 15.4.1 shall be evaluated monthly using data from the previous month.

15.4.2 Where emergency events are transferred, the transfer process shall not exceed 30 seconds 90 percent of the time.

15.4.2.1 The events shall be transferred directly to the telecommunicator.

15.4.2.2 The initial recipient of the call shall remain on the line until the receiving agency answers the call.

15.4.2.3 Transferred calls shall be evaluated monthly using data from the previous months.

15.4.3* Call processing time shall include the time from call answer to initial notification of the responding ERU(s).

15.4.4* Emergency event processing for the highest prioritization level emergency events listed in 15.4.4.1 through 15.4.4.2 shall be completed within 60 seconds, 90 percent of the time.

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

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

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

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

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

15.4.4.4 The following types of calls shall be exempted from the requirements of 15.4.4:

(1) Joint responses with law enforcement (involving weapons)
(2) Hazardous materials incidents
(3) Technical rescue

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

(1) Language translation
(2) TTY/TDD
(3)* Incomplete location
(4) SMS message to 9-1-1
(5) Calls received from outside the normal area of responsibility and/or service area
(6) Calls requiring use of a PSAP registry or similar tool to determine the appropriate PSAP and/or transfer location
(7) Calls received during a significant disaster that severely and significantly depletes available resources, impacts local infrastructure, and could result in changes to normal dispatcher procedures (disaster mode)

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

15.4.6 Any communication center that processes a medical event shall provide emergency medical dispatch.

15.4.7 For medical events where a patient is determined to be unconscious/unresponsive and not breathing, one of the following shall take place:

(1) Bystander CPR shall be confirmed.
(2) Telephone CPR shall be initiated by a telecommunicator qualified in emergency medical dispatch and continued until emergency responders arrive at the patient.

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

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

15.4.10* Records of the dispatch of emergency response units to events 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) En route 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

15.4.11* 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.

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

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

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

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

15.4.14.2* 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

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

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

15.4.16 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.

15.4.17 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 12.2.6.3
(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
(10) Procedures for handling non-voice emergency events

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

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

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

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

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

15.4.20 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

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

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

15.5 Time.

15.5.1 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.

15.5.2 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.

15.5.3 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.

15.5.4 All timekeeping devices not capable of being synchronized with the master time source shall be maintained within 60 seconds of the master time source.

15.6 Recording.

15.6.1 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

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

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

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

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

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

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

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

15.7.1 Compliance with Section 15.7 shall be evaluated monthly using data from previous months.

15.7.2 Monthly compliance shall include measured individual performance and shift or center performance.

Chapter 16 Telephones (NFPA 1221)

16.1* Receiving Equipment. The provisions of Chapter 16 shall apply to facilities and equipment that are needed to receive events.

16.2 9-1-1.

16.2.1 The primary emergency telephone number for use of any person seeking police, fire, medical, rescue, and other emergency services shall be 9-1-1, or another dedicated three-digit number for emergencies outside of North America.

16.2.2 Where 9-1-1 service is not available or in case of a failure of the 9-1-1 system, the requirements in 16.2.2.1 through 16.2.2.5 shall be met.

16.2.2.1 A specific telephone number shall be assigned for calls requesting emergency services.

16.2.2.2 The telephone number shall be publicized as an emergency telephone number.

16.2.2.3 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.

16.2.2.4 A separate telephone connection with a telephone number that is not publicly listed shall be maintained for communication with other emergency service agencies and receipt of off-premise monitored alarms.

16.2.2.5* A separate number shall be assigned for business (i.e., nonemergency) use.

16.2.3 Directory Listings. The text and symbols shown in Figure 16.2.3(a) through Figure 16.2.3(c) shall appear on the inside front cover or the page facing the inside front cover of the directory.

16.2.3.1 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.

16.2.3.2 The following listings and telephone numbers shall appear as follows in any directory listing emergency telephone numbers:

(1) Fire and rescue services, as follows:
    (a) To report an emergency, 9-1-1 or [fire number] if 9-1-1 is not available
    (b) Nonemergency purposes, [business number]
(2) Law enforcement, as follows:
    (a) To report an emergency, 9-1-1 or [police number] if 9-1-1 is not available
    (b) Nonemergency purposes, [business number]

FIRE

[*FIRE NUMBER*]

or, where available,

FIRE

FIGURE 16.2.3(a) Directory Listing for Fire Department.

POLICE

[*POLICE NUMBER*]

or, where available,

POLICE

FIGURE 16.2.3(b) Directory Listing for Police Department.

EMERGENCY MEDICAL SERVICES

[*EMERGENCY MEDICAL SERVICES NUMBER*]

or, where available,

EMERGENCY MEDICAL SERVICES

FIGURE 16.2.3(c) Directory Listing for Emergency Medical Services.

(3) Emergency medical services, as follows:
   (a) To report an emergency, 9-1-1 or [emergency medical number] if 9-1-1 is not available
   (b) Nonemergency purposes, [business number]

16.2.3.3 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 16.2.3.

16.2.3.4 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 16.2.3 through 16.2.3.2.

16.2.3.5* Where an ERF that is not continuously staffed by trained telecommunicators is listed in the directory, callers shall be provided with a recorded message that refers them to 9-1-1 or the alternate emergency telephone number when calls to the listed telephone number are not answered.

16.3 Reliability.

16.3.1 The 9-1-1 system shall be designed so that no single point of failure can prevent calls from being answered.

16.3.2 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.

16.3.3 The communications center shall be capable of receiving caller contact and location information from sources identified in Section 16.1.

16.4 Equipment and Operations. Voice connections shall be provided as follows:

(1) The primary method of notification of emergency calls shall be 9-1-1.
(2)* Connection capacity for 9-1-1 shall be provided as required for the volume of calls handled to provide a P.01 grade of service (GOS).
(3) Capacity shall allow for at least two concurrent emergency calls to be processed.
(4) Additional emergency lines shall be provided as required for the volume of calls handled to provide P.01 grade of service (GOS).
(5) Additional capacity shall be provided for the normal business (i.e., nonemergency) telephone number(s) as needed.
(6) The capacity to make an outbound call shall be maintained at all times.
(7) Separate telephone lines shall be provided as required in Section 16.2.

16.4.1 The AHJ shall ensure that the published emergency telephone numbers are answered prior to nonemergency telephone numbers.

16.4.1.1 When all emergency telephone numbers are in use, requests for emergency assistance shall be routed to either other predetermined telephone numbers that are approved by the AHJ or to a predesignated PSAP/alternate site.

16.4.1.2 Overflow calls to the business telephone number shall not overflow to the designated emergency telephone number.

16.4.2* When a PSAP receives a request for emergency assistance for a location that is not in its jurisdiction or a call for an agency not under the control of the communications center,

the telecommunicator shall transfer the call directly to the responsible communications center.

16.4.2.1 The telecommunicator shall remain connected to the caller until it is certain that the transfer has been made to the communications center.

16.4.2.2 The telecommunicator shall transfer the caller and the location information, where possible, instead of processing and relaying the information to the responsible communications center.

16.4.3 All designated emergency telephone numbers shall be recorded in accordance with Chapter 12 of this standard.

16.4.4* If an incoming call on any designated emergency number is not answered within 60 seconds, notification shall be automatically sent to a device or workstation approved by the AHJ.

16.4.5* With regard to automated voice alarms, as permitted by the AHJ, the communications center shall adhere to the following requirements:

(1) Separate, unlisted telephone number(s) shall be provided to receive such alarms.
(2) Such voice alarms shall not be permitted to connect to the telephone numbers required by Chapter 16.

16.4.6 Automated data alarms that are received by the communications center through a dial-up telephone service — as permitted by the AHJ — shall adhere to the following requirements:

(1) Separate, unlisted telephone number(s) shall be provided to receive such alarms.
(2) Such data alarms shall not be permitted to connect to the telephone numbers required by Chapter 16.

16.4.7* Where the communications center is permitted to receive automated data alarms through electronic means, the AHJ shall determine the delivery mechanism and follow the associated standards.

16.4.8 All telecommunicator positions that are available for receiving emergency calls shall have equipment capable of receiving and transmitting TDD/TTY, SMS, and real-time text data.

16.5 Alternative Routing.

16.5.1* 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.

16.5.2 Where the AHJ requires that overflow calls to emergency numbers be routed to alternative telephone numbers within the communication center, the alternative telephone numbers shall be monitored for integrity and recorded as required by this standard.

16.5.3 Where a communication center operates on a part-time basis, an automatic alternative routing plan shall be put in place that ensures the rapid routing of calls to the designated alternate communication center.

16.5.4 Any call that has not been answered after 20 seconds shall be automatically routed to one of the following:

(1) A designated alternate communication center
(2)* A holding queue, as follows:
(a) When in the queue, the callers shall receive a recorded message informing them that they have reached the communication center, including a TDD/TTY recorded message.
(b) The system shall periodically remind callers to the communications center who are in the 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.

16.6 Multiple Line Telephone Systems (MLTS).

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

16.6.2* 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.

16.6.3* 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.

16.6.3.1 The ALI associated with the ANI used by 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, floor, and room/zone.

16.6.4 An MLTS manager shall not install, configure, or maintain an MLTS to engage in local termination of 9-1-1 calls except as permitted by the AHJ and 16.6.4.1.

16.6.4.1 The facility and operation answering a diverted 9-1-1 call from an MLTS shall adhere to the requirements within this standard.

Chapter 17 Dispatching Systems (NFPA 1221)

17.1 Fundamental Requirements of Events Dispatching Systems.

17.1.1* General.

17.1.1.1 An event dispatching system shall be designed, installed, operated, and maintained to provide for the receipt and retransmission of events.

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

17.1.1.3 The required number of dispatching circuits shall be in accordance with 17.1.1.3.1 through 17.1.1.3.3.

17.1.1.3.1 Jurisdictions that receive 730 events 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 events.
(2) The failure of any component of the primary circuit shall not affect the operation of the secondary circuit and vice versa.

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

17.1.1.3.3* A circuit that terminates at a telephone handset only shall not be considered as fulfilling the requirements for a dispatch circuit. *(See 17.2.2.2.)*

17.1.1.4 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 17.1.2 through 17.1.2.4.3
(2)* Nontrunked voice radio channel with duplicate system elements, with the following features:
    (a) Monitored for integrity as required by 17.1.2.6
    (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 17.1.2 through 17.1.2.5.2, 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 17.1.2 through 17.1.2.5.2
    (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 17.1.2 through 17.1.2.4.3, excluding the following:
    (a) Telephone connection through a public-switched telephone network
    (b) Nondedicated phone lines
(6) Trunked radio system in compliance with 17.1.1.4(2) or 17.1.1.4(4)

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

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

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

17.1.1.6* 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.

17.1.1.7 Events shall be retransmitted to ERFs or to ERUs in the field from the location at which events are received.

17.1.1.7.1 Events transmitted from the communications center shall be automatically received at ERFs and ERUs.

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

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

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

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

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

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

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

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

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

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

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

17.1.2.4.2 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.

17.1.2.4.3 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.

17.1.2.5 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.

17.1.2.5.1 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.

17.1.2.5.2 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 17.1.2.4 through 17.1.2.5.2, that actuates and sounds in accordance with the type of dispatch circuit that is being monitored.

17.1.2.6* 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.

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

17.1.2.7 Any secondary dispatch circuit utilizing elements not under the ownership or control of the AHJ (e.g., the Internet) shall have a mechanism in place to monitor for the confirmation of the receipt of alarm.

17.2 Wired Dispatching Systems.

17.2.1 Wired Circuits — General.

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

17.2.1.2 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.

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

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

17.2.1.3.2 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.

17.2.1.4 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.

17.2.1.5 In jurisdictions where fewer than 730 events 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.

17.2.1.6 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.

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

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

17.2.1.9 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

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

17.2.1.11 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.

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

17.2.2 Telephone Circuits.

17.2.2.1 A telephone circuit that is used as one of the dispatch circuits shall meet the requirement in 17.1.1.4.

17.2.2.2 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).

17.3 Radio Dispatching Systems.

17.3.1 General.

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

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

17.3.1.2.1 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.

17.3.1.2.2* Radio system outdoor coverage shall be sufficient to provide a delivered audio quality (DAQ) of 3.4 for analog or digital systems.

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

17.3.1.4* At a minimum, the tactical communications channel identified in 17.3.1.3 shall be capable of operating in analog simplex mode.

17.3.1.5* Trunked system talk groups shall be permitted to be used to provide on-scene tactical communications if desired by the AHJ, but the provisions of 17.3.1.3 and 17.3.1.4 shall still apply.

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

17.3.1.7 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 primary channel is being used.

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

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

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

17.3.2 Signaling and Control Systems.

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

17.3.2.2 Signaling and control systems shall use both polling and automatic transmission communications methods and shall support redundant designs as required in 17.1.1.4.

17.3.2.3 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 17.3.2.2.
(2) If the primary network connection 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.

17.3.3 Conventional Two-Way Voice Systems.

17.3.3.1* Analog System Requirements. Systems shall be equipped with a coded squelch system to minimize the reception of out of system on-channel signals interference.

17.3.3.2 Digital Conventional System Requirements. Digital conventional systems shall comply with TIA-102.BAAA, *Project 25 FDMA Common Air Interface.*

17.3.3.3 Call Indicator. A call indicator shall be provided for each conventional channel controller from the control center console to indicate when the channel is busy.

17.3.4 Trunked Two-Way Voice Systems.

17.3.4.1* Signaling Channel Concept.

17.3.4.1.1 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 affected.

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

17.3.4.1.3 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.

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

17.3.4.1.5* Mobile and portable units shall be capable of being programmed with scanning of trunked talkgroups and conventional channels, with a user-selectable priority, as approved by the AHJ.

17.3.4.1.6 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.

17.3.4.1.7 Channel access time in single-site systems, assuming a channel is available, shall be less than 0.5 second.

17.3.4.1.8* Priority Levels.

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

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

17.3.4.1.9* Emergency Priority.

17.3.4.1.9.1 All field units in the system shall be capable of gaining access to the system within 0.5 second of activation of an instantaneous emergency switch.

17.3.4.1.9.2 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.

17.3.4.1.10* Failure of Trunking System.

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

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

17.3.4.1.10.3 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.

17.3.4.1.11* Queuing of Request for Voice Channel.

17.3.4.1.11.1 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.

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

17.3.4.1.11.3 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.

17.3.4.1.11.4 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.

17.3.4.1.12 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.

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

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

17.3.4.1.15 Continuous Talkgroup Affiliation Notification.

17.3.4.1.15.1 The system shall broadcast a continuous update of the talkgroup channel assignments to all field units whose radios are turned on and are within the system's coverage area.

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

17.3.4.1.16* Whenever a field unit leaves the coverage of the signaling channel and attempts to access the system using the push-to-talk (PTT) button, a distinctive audible alert shall be sounded so that the user knows that they are outside the system's coverage area.

17.3.4.1.17* Individual Unit Disable.

17.3.4.1.17.1* Hardware and software that allow disablement of any mobile or portable unit(s) currently operating on the system shall be provided for the system security in case units become lost or stolen.

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

17.3.4.1.17.3 Hardware and software that allow re-enablement of a disabled mobile or portable radio unit(s) currently operating on the system shall be provided.

17.3.4.1.18* The system shall allow AHJ authorized personnel to initiate a change in the operating talkgroup of any field unit from a system manager terminal.

17.3.4.1.19* 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.

17.3.4.1.20 Monitoring for Integrity.

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

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

17.3.4.1.20.3 A means shall be provided that is capable of recording system problems as they occur, including type of problem, date, and time.

17.3.4.1.21 Console Call Indicator.

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

17.3.4.1.21.2 When a channel is selected, the call indicator shall flash when audio is being received from a field unit.

17.3.4.1.22 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.

17.3.4.1.23 Console Trunked Busy Indication.

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

17.3.4.1.23.2 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.

17.3.4.1.24* Console Dispatch Preemption.

17.3.4.1.24.1 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 event.

17.3.4.1.24.2 If necessary, the requirement of 17.3.4.1.24.1 shall be met by preemption of the lowest-priority communication on the system at the time of attempted access to the talkgroup.

17.3.4.1.25 The telecommunicator shall have the following capabilities:

(1) The telecommunicator shall be able to designate a higher tactical priority for certain talkgroups that are controlled at their workstation.

(2) Designation of higher tactical priority shall be achieved by means of a switch on that talkgroup appearance.

17.3.4.2* Digital Trunked System Requirements. Digital trunked systems shall comply with TIA-102.BAAA, *Project 25 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 Two-Slot TDMA Media Access Control Layer Specification*, and shall meet the requirements in 17.3.4.1.

17.3.5* Two-Way Mobile Equipment.

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

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

17.3.5.3 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.

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

17.3.5.5 Mobile radios shall be capable of multiple-channel operation to enable on-scene simplex radio communications that are independent of dispatch channels to meet the requirements of 17.3.1.3.

17.3.5.6 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

17.3.6* Two-Way Portable Equipment.

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

17.3.6.2 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.

17.3.6.3 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.

17.3.6.4 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.

17.3.6.5 Portable radios shall be capable of multiple-channel operation to enable on-scene simplex radio communications that are independent of dispatch channels to meet the requirements of 17.3.1.3.

17.3.6.6 Portable radios shall be designed to allow channels to be changed and other radio functions controlled while emergency response personnel are wearing gloves of the type used in emergency response functions.

17.3.6.7 The channel change and radio selection functions shall be tested with, at a minimum, a large-sized glove.

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

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

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

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

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

17.3.6.13* 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.

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

17.3.8 Backhaul Microwave Systems.

17.3.8.1 General Requirements. Microwave radio systems used for backhaul 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.
(6) Each microwave hop shall be designed to meet or exceed a one-way end-to-end annual quality performance of 99.995 percent at the required capacity.
(7) Each microwave hop shall be designed to meet or exceed a one-way end-to-end annual reliability performance of 99.999 percent at the required capacity.

17.3.8.2 Recovery and Protection.

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

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

17.3.8.2.3 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.

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

17.3.8.3 Electromagnetic Interference.

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

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

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

17.3.8.5 Microwave System Network Management.

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

17.3.8.5.2 Fault and Failure History Log.

17.3.8.5.2.1 The microwave radio shall maintain an electronic file that records the date, time, and type of fault/action of all fault and failure conditions and switching actions.

17.3.8.5.2.2 The file shall be downloadable for on-site review and for electronic communication to others at remote locations.

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

17.3.8.5.4* External Alarms. Each microwave radio assembly shall accommodate at least four external site/housekeeping alarm inputs.

17.4 Radio Alerting Systems.

17.4.1 General.

17.4.1.1 Primary 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

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

17.4.1.3 Where portable two-way radio equipment is used to receive events, such units shall be equipped to receive a coded alert.

17.4.2 Radio Paging Systems and Pagers.

17.4.2.1* A primary paging system shall be under the direct control of the AHJ where used as a method of emergency dispatch.

17.4.2.2 No part of a primary paging system shall utilize the public Internet for any portion of its operation when used as a method of emergency dispatch.

17.4.2.3 Page-encoding equipment, where used as a method of primary emergency dispatch, shall be located in the communications center or an associated public safety radio system site.

17.4.2.4 A primary paging system shall comply with the general requirements for radio systems as outlined in this document.

17.4.2.5 Pagers shall audibly indicate a low-battery condition.

17.4.2.6 Alphanumeric pagers shall support the maximum text message that can be sent from the communications center.

17.4.2.7* Coded receivers shall audibly indicate the presence of an unacknowledged message.

17.4.2.8 Alphanumeric devices and two-way alphanumeric devices shall audibly indicate the presence of an unread message.

17.4.2.9 Two-way alphanumeric devices shall automatically transmit an acknowledgment when the device has received and stored a message.

17.4.2.10 Two-way alphanumeric devices shall automatically transmit an acknowledgment when the responding user has read the message.

17.4.2.11* Two-way alphanumeric devices shall be capable of providing and transmitting multiple-choice replies, manually selected by the user.

17.4.2.12* Status of the two-way alphanumeric devices, including messages sent and acknowledged, shall be monitored in the operations room.

17.4.3* Alerting Receivers. Where radio alerting receivers are used to receive emergency dispatch messages, they shall be provided with two sources of power.

17.5 Outside Audible Alerting Devices.

17.5.1 Outside audible alerting devices used to indicate an emergency shall be located to alert all emergency response personnel expected to respond.

17.5.2 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.

17.5.3 Compressed Air Alerting Devices.

17.5.3.1 Compressed air alerting devices shall have a distinctive tone.

17.5.3.2 If coded, the duration of the blast shall be neither less than 0.5 second nor longer than 1.5 seconds, with silent intervals of 1 to 1.5 times the blast duration.

17.5.3.3 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 is capable of being sounded.

17.5.4 Compressors shall have the capacity to fill storage tanks to working pressure within 30 minutes.

17.5.4.1 Piping of ferrous materials shall be provided with scale traps that are accessible for cleaning.

17.5.4.2 All piping shall be arranged to allow inspection and repair.

17.5.5 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.

17.5.5.1 The communications center shall be equipped for IP-enabled two-way communications with the ERUs using IP-enabled devices as determined by the AHJ.

17.5.5.2 IP-enabled devices shall be capable of fully charging the battery while in use.

17.6 Non-AHJ-Owned Alerting Devices and Infrastructure.

17.6.1 Secondary alerting devices shall be permitted to utilize commercial networks or components.

17.6.2 Non-AHJ-owned devices shall be permitted to be used as secondary alerting devices only if they can meet the requirements in 17.6.2.1 through 17.6.2.4.

17.6.2.1 Commercial network providers shall certify, to the AHJ, that components utilized in secondary alerting circuits have redundant power supplies.

17.6.2.2 Commercial network providers shall certify, to the AHJ, that utilized infrastructure components are hardened to APCO ANS 2.106.1, *Public Safety Grade Site Hardening Requirements*.

17.6.2.3 Secondary alerting systems, utilizing commercial network elements, shall provide the AHJ acknowledgement that such messaging was received by the destination device.

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

Chapter 18 In-Building Emergency Responder Communications Enhancement Systems (NFPA 1221)

18.1 General.

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

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

18.2 Approval.

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

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

18.3* System Design.

18.3.1 Enclosures.

18.3.1.1 Battery systems used for the emergency power source shall be contained in a NEMA 3R or higher-rated cabinet.

18.3.1.2 All repeater, transmitter, receiver, signal booster components, optical-to-RF and RF-to-optical converters, and external filters shall be contained in a NEMA 4– or NEMA 4X–type enclosure(s).

18.3.1.3 Batteries that require venting shall be stored in NEMA 3R–type enclosures.

18.3.2* Oscillation Detection and Control. Signal boosters used in emergency responder communications enhancement systems shall have built-in oscillation detection and control circuitry to reduce gain and maintain operation.

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

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

18.3.3 Mounting of the Donor Antenna(s).

18.3.3.1 To maintain proper alignment with the system designed donor site, donor antennas shall meet one of the following:

(1) Antennas shall be permanently affixed on the building.
(2) Where approved, antennas shall be mounted on a movable sled with a visible sign stating "Movement or repositioning of this antenna is prohibited without approval from the AHJ."

18.3.3.2 If a donor antenna exists, isolation shall be maintained between the donor antenna and all inside antennas to a minimum of 20 dB above system gain.

18.3.3.3 The antenna installation shall also be in accordance with the applicable requirements of the building code for weather protection of the building envelope.

18.3.4 Communication Antenna Density.

18.3.4.1* In-building emergency responder communication enhancement systems shall be designed to minimize the near-far effect.

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

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

18.4* Lightning Protection. Systems shall have lightning protection that complies with 18.4.1 through 18.4.4.

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

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

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

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

18.5 Testing Requirements. Systems that are used to comply with the requirements of Chapter 18 shall be tested in accordance with 20.3.10 and 20.3.10.1.

18.6 Non-Interference and Non-Public Safety System Degradation.

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

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

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

18.7 Approval and Permit.

18.7.1 Plans, including, but not limited to, specifications, link budget, and other information required by the AHJ and frequency license holder(s), shall be submitted for approval prior to installation.

18.7.2* Written authorization by the frequency license holder shall be required upon initial installation and prior to activation of the emergency responder communications enhancement system.

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

18.8* Radio Coverage.

18.8.1 Radio coverage shall be provided throughout the building as a percentage of floor area as specified in 18.8.3 and 18.8.4.

18.8.2 The system shall adhere to the maximum acceptable propagation delay standard provided by the AHJ.

18.8.3 Critical areas, including fire command centers, fire pump rooms, exit stairs, exit passageways, elevators, 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.

18.8.4 General building areas shall be provided with 95 percent floor area radio coverage.

18.8.5 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 by the radio licensing authority to achieve the required adequate radio coverage.

18.8.6 Radio enhancement systems shall be designed to support two portable radios simultaneously transmitting on different talk paths or channels, where the AHJ has required the radio enhancement system to support more than one channel or talk path.

18.9* Signal Strength and Quality.

18.9.1* Downlink. A minimum downlink signal shall be sufficient to provide a minimum of DAQ 3.0 for voice communications using either narrowband, analog, or digital P25 signals or wideband LTE digital signals throughout the coverage area. *(See A.20.3.10.)*

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

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

18.10 Donor Antenna. If a donor antenna exists, isolation shall be maintained between the donor antenna and all inside antennas to a minimum of 20 dB above system gain.

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

18.11.1 List of Assigned Frequencies. The AHJ and the frequency license holder(s) shall each maintain a list of all downlink/uplink frequency pairs for distribution to system designers.

18.11.2* Frequency Changes.

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

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

18.12 System Components.

18.12.1* Component Approval, Certification, and Listing.

18.12.1.1 RF-emitting devices and cabling used in the installation of in-building emergency responder communications enhancement systems shall be approved by the AHJ and the frequency license holder.

18.12.1.2 All RF-emitting devices shall have the certification of the radio licensing authority of that country and be suitable for public safety use prior to installation.

18.12.1.3 All repeaters, transmitters, receivers, signal-booster components, remote annunciators and operational consoles, power supplies, and battery charging system components shall be listed and labeled in accordance with UL 2524, *Standard for In-Building 2-Way Emergency Radio Communication Enhancement Systems*.

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

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

18.12.3 Component Requirements.

18.12.3.1 All cables shall be installed in accordance with Chapters 7 and 8 of *NFPA 70*.

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

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

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

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

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

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

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

18.13 Power Sources. At least two independent and reliable power sources shall be provided for all RF-emitting devices and any other active electronic components of the system: one primary and one secondary.

18.13.1 Primary Power Source. The primary power source shall be all of the following.

(1) Supplied from a dedicated branch circuit
(2) Permanently connected
(3) Compliant with *NFPA 72*
(4) Protected from overvoltage

18.13.2 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
(3) A 2-hour standby battery and connection to the facility generator power system, providing the facility generator power system can support the complete system load for 12 hours

18.13.3 Monitoring Integrity of Power Sources. Monitoring the integrity of power sources shall be in accordance with 17.1.2.2.

18.14 System Monitoring.

18.14.1 Fire Alarm System.

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

18.14.1.2 The system shall comply with all of the following:

(1) Monitoring for integrity of the system shall comply with Chapter 10 of *NFPA 72*.

(2) System supervisory signals shall include the following:
   (a)* Signal source 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) Active system component failure
(3) Power supply supervisory signals shall include the following for each RF-emitting device and active system components:
   (a) Loss of normal ac power
   (b) Failure of battery charger
(4) The communications link between the fire alarm system and the in-building emergency responder communications enhancement system shall be monitored for integrity.
(5) Where approved by the AHJ, a single supervisory input to the fire alarm system to monitor all system supervisory signals shall be permitted.

18.14.2 Dedicated Annunciation.

18.14.2.1 A dedicated annunciator shall be provided within the fire command center to annunciate the status of all RF-emitting devices and active system component locations.

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

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

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

18.15 Technical Criteria.

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

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

18.15.3 The AHJ technical information documents shall be accessible to emergency responder communications enhancement system design personnel.

18.15.4 The AHJ technical information documents shall contain, but not be limited to, the following:

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

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

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

Chapter 19 Computer-Aided Dispatching (CAD) Systems (NFPA 1221)

19.1 General.

19.1.1* Computer-aided dispatching (CAD) systems, when required by the AHJ, shall conform to the items outlined in this chapter.

19.1.2* 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.

19.1.2.1* The CAD interface shall accept a transfer of 9-1-1 emergency call data from the customer premise equipment (CPE) to the CAD system.

19.1.2.2 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.

19.2* 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.

19.3 Security.

19.3.1 CAD systems shall utilize different levels of security to restrict unauthorized access to sensitive and critical information, programs, and operating system functions.

19.3.2 The AHJ shall have the ability to control user and supervisor access to the various security levels.

19.3.3 Physical access to the CAD system hardware shall be limited to authorized personnel as determined by the AHJ.

19.3.4 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.

19.3.5* CAD systems shall provide network isolation necessary to preserve bandwidth for the efficient operation of the system and processing of events.

19.3.5.1 The CAD system shall provide measures to prevent denial-of-service attacks and any other undesired access to the CAD portion of the network.

19.3.5.2 CAD systems shall employ antivirus software where necessary to protect the system from infection.

19.4 Event Data Exchange.

19.4.1 The CAD system shall have the capability to allow event data exchange between the CAD system and other CAD systems.

19.4.1.1 The method for data exchange shall be the NENA/APCO ANS 2.105.1, *NG9-1-1 Emergency Incident Data Document (EIDD).*

19.4.1.2* It shall be up to the AHJ to decide whether or not to use or display this information.

19.4.1.3 The sending dispatchers shall be able to send and receive administrative (not tied to an incident) messages to the receiving dispatchers.

19.4.2 The CAD system shall have the capability to allow event data exchange between the CAD system and supervising stations.

19.4.3 The CAD system shall have the capability to allow event data exchange between the CAD system and 9-1-1 databases.

19.4.4* The CAD system shall have the capability to allow event data exchange between the CAD system and other systems as required and approved by the AHJ.

19.4.5 CAD systems that are connected to third-party systems to receive events directly shall have agreements in place with the third-party providers to monitor the system for integrity.

19.5 CAD Capabilities.

19.5.1 The installation of a CAD system in emergency service dispatching shall not negate the requirements for a secondary dispatch circuit.

19.5.2 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.

19.5.3 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 Section 12.8).*

19.5.3.1 The SEPSS shall be capable of supporting the critical loads for no less than 60 minutes.

19.5.3.2* The SEPSS shall receive its power from circuit(s) that are automatically connected to the emergency generator, as specified in 12.8.3, in the event of a power failure or insufficiency.

19.5.4 All characters shall be visible in a lighted room without being affected by the glare of ambient lighting.

19.5.5 Printers.

19.5.5.1 The system shall support as many printers as the AHJ deems necessary for its operation.

19.5.5.2 Logging or utility functions shall be assignable to any printer under system control.

19.5.5.3 A spare printer shall be available.

19.5.5.4 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.

19.5.6* Software that is a part of the CAD system shall provide data entry; provide resource recommendations, notification, and tracking; store records relating to all events and all other calls for service and status changes; and track those resources before, during, and after events, preserving records of those events and status changes for later analysis.

19.5.6.1* 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.

19.5.6.2 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.

19.5.7 Where the CAD system is a primary or secondary dispatch circuit for ERFs and ERUs, it shall provide an audible notification of events and shall be permitted to provide a visual notification of events and other calls for service.

19.5.7.1 If voice announcement is used, it shall be preceded by an audible warning or alerting signal that differentiates the event or emergency from any other voice messages carried by the system.

19.5.7.2* If text messages are used, they shall be accompanied by audible warning or alerting signal(s) that notify ERF or ERU personnel that an event or emergency message has been transmitted.

19.6 Performance.

19.6.1* The system shall accommodate the call volume, call types, and other sizing parameters required by the AHJ.

19.6.2 The system shall recommend units for assignment to calls.

19.6.2.1 The system shall ensure that the optimum response units are selected.

19.6.2.2 The CAD system shall allow the telecommunicator to override the CAD recommendation for unit assignment.

19.6.2.2.1 The CAD system shall automatically log that the recommendation was overridden manually by the telecommunicator.

19.6.2.3 The CAD system shall have the ability to prioritize all system processes so that emergency operations take precedence.

19.6.3 The system shall detect faults and failures.

19.6.3.1 The system shall automatically perform all required reconfiguration as a result of the faults or failures.

19.6.3.2 The system shall queue a notification message to the supervisor and any designated telecommunicator positions.

19.6.4* 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.

19.6.5 The system shall be available and fully functional 99.95 percent of the time, excluding planned maintenance.

19.6.6* The system shall include automatic power-fail recovery capability.

19.7* Backup. The system shall include a data backup system, utilizing either removable media or independent disk storage arrays dedicated to the backup task.

19.8 Redundancy.

19.8.1 The failure of any single component shall not disable the entire system.

19.8.1.1 The CAD system shall provide automatic switchover in case of failure of the required system component(s).

19.8.1.2 Manual intervention by telecommunicators or others shall not be required.

19.8.1.3 Notwithstanding the requirements of 19.8.1.1, the system shall provide the capability to manually initiate switchover.

19.8.1.4* Systems that utilize redundant server and workstation configurations shall 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.

19.8.1.5 Systems that utilize distributed processing, with workstations in the operations room also providing the call processing functions, shall be considered to meet 19.8.1.4, 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.

19.8.1.6* 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.

19.8.2 Monitoring for Integrity.

19.8.2.1 The system shall continuously monitor the CAD interfaces for equipment failures, device exceptions, and time-outs.

19.8.2.2 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.

19.8.3* The system shall log system messages and transactions.

19.8.4 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 21.7.

19.8.5* 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.

19.9 Storage Network.

19.9.1* The system shall provide on-line storage that meets all of the functional and performance requirements of this standard for programs and data.

19.10 Information Transmittal.

19.10.1 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.

19.10.2 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.

19.10.3 Mobile units shall communicate with the CAD system at a minimum rate of 9600 bits per second.

19.10.4 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.

19.11 Mobile Data Computers (MDCs).

19.11.1* MDCs and associated equipment shall be manufactured for the environment in which they are to be used.

19.11.2 System Availability.

19.11.2.1 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

19.11.2.2* If communication between MDCs and CAD has failed, messages in transit shall not be lost.

19.11.3 Emergency messages to MDCs shall take priority over other messages.

19.11.3.1 The MDC shall immediately display an indication of an emergency message.

19.11.3.2 The emergency message shall be accompanied by an audible indication from the MDC of sufficient volume to overcome ambient noise.

19.11.3.3 Vehicles equipped with printers shall have the capability to print emergency messages.

19.11.3.4 Displayed emergency messages shall not be automatically replaced by other messages.

19.11.3.5 The MDC shall display emergency information with a minimum use of multipage display.

19.11.4 Nonemergency Messaging.

19.11.4.1 A manual acknowledgment feature shall be provided to indicate that a message sent from the operations room has been viewed.

19.11.4.2 An MDC shall display vehicle status as currently registered within the CAD system.

19.11.5 Equipment and Operation.

19.11.5.1 The MDC shall not require external power to maintain programmed functions.

19.11.5.2 Required connections between the MDC and other essential system components shall be fastened so as to not come loose under normal operating conditions.

19.11.5.3 The MDC shall allow a single action by the operator to initiate an emergency response status change.

19.11.5.4* 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

19.11.5.5 The MDCs shall have a last-in-first-out (LIFO) feature that allows the user to recall the last 10 messages received.

19.11.5.6 Each MDC shall be capable of receiving single, group, or all-call messages.

19.11.5.7 Keyboard.

19.11.5.7.1 The bottoms of detachable keyboards shall have nonskid surfaces.

19.11.5.7.2 The illumination of the keyboard shall be adjustable by the user.

19.11.5.7.3 The keyboard design shall prevent malfunction caused by foreign materials.

19.11.5.7.4 Keyboard malfunctions shall not adversely affect the MDC, the MDC system, the MDC interface, or the CAD system.

19.11.5.8 Display Screens.

19.11.5.8.1 All information shall be visible in direct sunlight conditions.

19.11.5.8.2 The display screen shall be stable and free of unintentional motion.

19.11.5.8.3 Characters shall have a uniform appearance on all parts of the screen.

19.11.5.9 Mobile printers shall provide the following functionality:

(1) The ability to power on and off
(2) A visual indication that the unit is energized

19.12 Integrated Mapping Interface.

19.12.1* The CAD system shall have the ability to interface with a map display system.

19.12.2 The map display system interface shall have the ability to accept spatial positioning data for calls for service and units from CAD.

19.12.3 The map display system interface shall have the ability to position an indicator on the map based on the provided spatial information.

Chapter 20 Testing (NFPA 1221)

20.1 General.

20.1.1 Tests and inspections shall be made at the intervals specified in this standard.

20.1.2 All equipment shall be restored to operating condition after each test or alarm for which the equipment functioned.

20.1.3 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.

20.1.4 Procedures that are required by other parties and that exceed the requirements of this standard shall be permitted.

20.1.5 The requirements of this chapter shall apply to both new and existing systems.

20.2 Acceptance Testing.

20.2.1 New equipment shall be provided with operation manuals that cover all operations and testing procedures.

20.2.2 All functions of new equipment shall be tested in accordance with this chapter and the manufacturers' specifications before being placed in service.

20.2.3 All cables shall be tested in accordance with this chapter where installed with all taps and splices made.

20.2.3.1 Before connection to terminals, cables shall be tested for insulation resistance.

20.2.3.2 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.

20.2.4 The frequency, modulation, power output, and receiver sensitivity and selectivity shall be tested and recorded when any radio is installed or repaired.

20.2.5 Microwave acceptance testing shall be performed.

20.3 Operational Testing.

20.3.1 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.

20.3.2 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 20.3.2, 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 20.3.2, 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.

20.3.3 Alerting Means. Outside audible alerting devices, radio, telephone, or other means for alerting emergency response personnel shall be tested as required by the AHJ.

20.3.4 Radio and Voice Amplification Circuits. All primary and secondary radio and voice amplification circuits shall be subjected to a voice test twice daily.

20.3.5 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.

20.3.6 Emergency Lighting. Emergency lighting shall be tested in accordance with NFPA *101*.

20.3.7 Stored Emergency Power Supply System/Uninterruptible Power Supply (SEPSS/UPS). An SEPSS/UPS shall be tested in accordance with NFPA 111.

20.3.8 TDD/TTY. The TDD/TTY system shall be tested daily.

20.3.9 Emergency Equipment and Supplies. Emergency equipment and supplies, including self-contained breathing apparatus, flashlights, and medical equipment, shall be tested at least annually or in accordance with the applicable NFPA code or standards.

20.3.10* Test and Inspection of In-Building Emergency Responder Communications Enhancement Systems. Where in-building emergency responder communications enhancement system 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.

20.3.10.1 Initial Acceptance Test Requirements.

20.3.10.1.1 All new systems shall be initially acceptance tested to verify that the system as installed meets the performance requirements of Section 18.9.

20.3.10.1.2 Qualifications of testing personnel shall be submitted to the AHJ for approval and acceptance.

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

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

20.3.10.2 Periodic Visual Inspection of Systems.

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

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

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

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

20.3.10.2.3 Periodic Testing of Systems.

20.3.10.2.3.1 All systems shall be operationally tested at least annually to confirm system operation during normal operations.

20.3.10.2.3.2 Annual operational tests shall include the following:

(1) At least one quantitative DAQ test shall be in accordance with 18.9.1 and 18.9.2 on each floor. Where the floor area exceeds 128,000 ft^2 (11,900 m^2), additional quantitative tests shall be performed.
(2)* Signal boosters shall be tested to verify that the gain is the same as it was during the initial installation and acceptance or set to optimize the performance of the system.
(3) Backup batteries and power supplies shall be tested under load for a period of 1 hour.
(4) Other active components shall be checked to verify operation within the manufacturer's published specifications.
(5) All required supervisory monitoring signals shall be tested.
(6) A spectrum analyzer or other suitable test equipment shall be utilized to ensure spurious oscillations are not being generated by the subject signal booster.
(7) Where a donor antenna is used, isolation in accordance with Section 18.10 shall be verified.
(8) An inspection shall be made to evaluate if the building structural changes or alternations that have been made

impact the communications coverage of the system as required in Section 18.8.

20.3.10.2.3.3 At least every five years systems shall be quantitatively tested to ensure that the system still provides the required DAQ values in accordance with Section 18.9.

20.3.10.2.3.4 The five-year test shall also confirm that there has been no deviation of coverage more than 5 percent from the initial installation documentation.

20.3.10.2.4 Deviation of more than 5 percent shall result in additional evaluations to determine if any system modifications are required to bring the system into conformance with the coverage required in Section 18.9.

20.3.10.2.5 The five-year test shall confirm that there have been no changes in the frequencies utilized for the proper operation of the system.

20.3.10.2.6 The AHJ can require additional testing if the system fails to operate during normal operations at frequencies shorter than five years or if radio system conditions change.

20.3.10.2.7 Inspection and Testing Documentation.

20.3.10.2.7.1 All visual inspection and testing reports shall be documented in a format acceptable to the AHJ in writing.

20.3.10.2.7.2 All reports shall be retained for the life of the system in either paper or electronic form and be made available to the AHJ upon request.

20.3.11 Periodic microwave systems testing shall include throughput and reliability.

20.4 Power.

20.4.1 Emergency and standby power systems serving the communications center shall be tested in accordance with NFPA 110.

20.4.2 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.

20.4.3 The battery voltage during operation, including charge, discharge, and float, shall be maintained within the limits recommended by the battery manufacturer.

Chapter 21 Records (NFPA 1221)

21.1 General. Complete records to ensure operational capability of all dispatching system functions shall be maintained.

21.2 Installation.

21.2.1 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

21.2.2 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

21.2.3 Changes and Additions. Changes or additions shall be recorded in accordance with 21.2.1 and 21.2.2.

21.3 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
(5) A record of software licenses, software versions, and patches utilized with the equipment.

21.3.1 For software-based systems, access to site-specific software shall be provided to the AHJ.

21.3.2 The AHJ shall be responsible for maintaining the records for the life of the system.

21.3.3 Paper or electronic media shall be permitted.

21.4 Training Records. Training records shall be maintained for each employee as required by the AHJ.

21.5 Operational Records.

21.5.1* Call and dispatch performance statistics shall be compiled and maintained in accordance with Section 15.4.

21.5.2 Statistical analysis for call and dispatch performance measurement shall be done monthly and compiled over a 1-year period.

21.5.2.1 A management information system (MIS) program shall track incoming calls and dispatched events and provide real-time information and strategic management reports.

21.5.3 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

21.6 Maintenance Records.

21.6.1 Records of maintenance, both routine and emergency, shall be kept for all alarm-receiving equipment and alarm-dispatching equipment.

21.6.2 All maintenance records shall include the date, time, nature of maintenance, and repairer's name and affiliation.

21.7 Retention of Records.

21.7.1 Records required by Sections 21.2, 21.3, 21.5, and 21.6 shall be maintained for the life of the affected equipment.

21.7.2 Records that are required by Sections 15.4, 15.6, 20.3, and 21.5 shall be maintained for 2 years or as required by law or by the AHJ.

21.7.3 Where call detail recording (CDR) is provided, records shall be maintained for 2 years or as required by law or by the AHJ.

21.7.4 Capacity shall be provided for the storage of a minimum of 100 days of history log data.

21.7.4.1* History log data shall be deleted or overwritten based on a policy established by the AHJ.

Chapter 22 ICT Security (NFPA 1221)

22.1* Information Communication Technology (ICT) Security Plan.

22.1.1 Communications centers shall develop, implement, and utilize a comprehensive defense-in-depth process and plan to ensure data security.

22.1.2 The defense-in-depth approach shall comply with both of the following:

(1) Encompass people, technology, and operations
(2) 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

22.1.3 The plan shall include a policy statement from the AHJ detailing the requirements and goals of the plan.

22.1.4* The plan shall require the assignment of responsibilities for the performance of security functions.

22.1.4.1 The AHJ shall appoint a person to be the security officer to oversee the security aspects of the public safety communications center and public safety radio network as herein covered by this standard.

22.1.4.2 The security officer outlined in 22.1.4.1 shall ensure that the provisions of this chapter and other such security provisions for these systems as adopted by the AHJ will be maintained.

22.1.5* The plan shall specify both of the following:

(1) Training and education requirements for employees
(2) A continuing education plan component

22.1.5.1 The education requirements shall include at least annual training for all staff who access computer-based systems to include all of the following:

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

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

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

22.1.7* 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 events 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.

22.1.8* The communications center shall implement computer and network security provisions to prevent attacks or unauthorized access to the center's computers, servers, and networks.

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

22.1.8.2 These guidelines shall be all of the following:

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

22.1.8.3 Communications center equipment and networks that are connected to the Internet shall require the use of a firewall to prevent malicious access from unauthorized entities.

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

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

22.1.8.5* The AHJ shall create a plan for password management that, at a minimum, defines acceptable password complexity, frequency of password changes, and rules regarding safeguarding of passwords.

22.1.8.6* The AHJ shall have a plan to deal with DoS attacks against the public safety communications center.

22.1.8.7 The AHJ shall have a procedure to ensure that HIPAA information handled in the communications center or by public safety agencies on their radio networks is protected according to federal HIPAA requirements.

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

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

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

22.1.9.3 The AHJ shall consider whether firmware updates are necessary.

22.1.10* 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, in the event of theft, alteration, or denial of access to mission-critical data.

22.1.10.1 At minimum all servers necessary for the operation of the communications center, or the public safety radio communications networks, shall be backed up periodically on a schedule to be determined by the AHJ.

22.1.10.2* The backups of 22.1.8.1 shall be on separate media not connected to any network and stored in a location to be determined by the AHJ.

22.1.10.3 AHJs shall determine appropriate disaster recovery procedures for cloud storage of mission-critical information for communications centers and public safety radio networks in the event that the cloud storage security is compromised or the information stored in the cloud is unavailable for a period of time.

22.1.10.4* AHJs shall create a plan to deal with a ransom-ware attack on its systems and mission-critical information.

22.1.11* The AHJ shall implement communications center and wireless communications system logging and auditing provisions to allow for the investigation of security or operational problems.

22.1.12* The AHJ shall implement a vulnerability management process to assess the ability of the public safety communications systems, including communications centers, wireless networks, and wired IT networks to operate while under stress or cyber attack.

22.1.13* 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.

22.2* 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.

22.3 Testing Records. Testing records of the plan shall be maintained in accordance with Section 21.7.

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

Chapter 23 Public Alerting Systems (NFPA 1221)

23.1* General. Public alerting systems (PASs) initiated by communications centers shall meet the requirements specified in this chapter.

23.1.1 All PASs and related components shall comply with national, state, provincial, and local rules and regulations governing PASs and related system components.

23.1.2 The AHJ shall develop and maintain standard operating procedures for when and how the systems are to be used.

23.1.3 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).

23.1.4* 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.

23.1.5 An upgrade installed to a PAS shall be backward compatible with existing systems.

23.1.6 All PASs shall provide for the ability to operate in the event of a localized or widespread power outage for a period of time as determined by the AHJ.

23.2 Security.

23.2.1 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.

23.2.2 The AHJ shall enforce security procedures to prevent the misuse of sensitive information.

23.2.3 PASs shall be designed, installed, and maintained to prevent unintended or unauthorized activation in accordance with Chapter 22.

23.3* 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.

23.4 Permitted Systems.

23.4.1 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)
(8) Integrated private fire alarm/mass notification systems (as covered by *NFPA 72*) with interface connections to a PAS
(9) Private/public exterior billboards or electronic message boards

23.4.2 The AHJ shall be permitted to use alternate communications systems that meet the immediate need for communicating with the public.

23.5* Public Alerting System Alerting Appliances (PASAAs). PASAAs shall be capable of the following:

(1) Receiving an alert data message (ADM) from a PAS
(2) Process, convert, and retransmit the alert data message (ADM) to a system or system of devices for audible, visual, or textual messaging
(3) Providing an audible alert in response to an ADM that meets the audible characteristics of an alarm as defined in *NFPA 72*

(4) Providing a visual alert signal in response to an ADM that meets the following requirements, if equipped:
   (a) The signal shall be a flashing light that is red, clear, amber, or blue in color.
   (b) The signal shall provide a textual alert message in response to an ADM.
(5) 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.
(6) Providing a local visual 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.1.3 Any AHJs incorporating NFPA 1061, NFPA 1221, or any combination of the two, can replace those references with chapters and still reference similar content. For example, if an AHJ incorporated the 2018 edition of NFPA 1061 (i.e., in accordance with 2018 edition of NFPA 1061), and they wish to update to the latest information, they can do so by incorporating Chapters 1 through 11, and Annexes A, B, C, D, E, and G of the 2022 edition of NFPA 1225 (i.e., in accordance with Chapters 1 through 11, and Annexes A, B, C, D, E, and G of the 2022 edition of NFPA 1225).

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. Events received by electronic signal — that is, fire alarm boxes, central station alarms, and automatic crash notifications.

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.3.3.8 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 the latitude and longitude.

A.3.3.9 Automatic Number Identification (ANI). Automatic number identification is typically used in two disparate systems in emergency communications. First, ANI is a telephone number associated with the access line from which a call originates. Second, in two-way radio communications, ANI can be associated with the radio device that is active on the voice communication channel.

A.3.3.10 Backbone. Damage to a backbone cable or backbone cable components will disable the in-building emergency responder communications enhancement system through much or all of the building and, as a result, it should be identified and protected when installed in a building in accordance with 18.12.3. The backbone could be fiber-optic, copper, or coaxial cable, but it does not radiate RF energy along its path.

A.3.3.21 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.3.3.24 Circuit. Specific types of circuits include dispatch, local, and tie circuits.

A.3.3.27 Communications Center. Examples of the 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
(3) Communications within the ERA and between different ERAs

A.3.3.28 Communications Officer. The position is a function that falls under the logistics section of the Incident Command System.

A.3.3.29 Communications System. Devices can include telephones, radios, sensors, cameras, and any other instruments capable of capturing and communicating data. Networks can include both hard-wired and wireless infrastructure. Applications can include computer programs that collect, aggregate, and disseminate information. Computers can be in any form

factor, including personal devices, tablets, laptops, desktops, servers, clusters, and main frame servers.

Services can include private and commercially available voice and data transmission capabilities and applications as commercially available services. A communications system can include multiple interconnected and integrated communication systems.

A.3.3.30 Comprehensive Emergency Management Plan (CEMP). In some jurisdictions, a CEMP could also be known as a disaster management plan.

A.3.3.31 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.3.3.39 Delivered Audio Quality (DAQ). DAQ levels are as follows:

(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.3.3.43 Directory. Because directories can cover multiple jurisdictions, the name of the jurisdiction or community served by the directory should be indicated.

A.3.3.44 Dispatch Circuit. A dispatch circuit was formerly called an alarm circuit.

A.3.3.48 Distribution Antenna. A distribution antenna is typically nondescript in appearance so as not to disturb the décor of the area. It is also outside the pathway survivability requirements.

A.3.3.49 Distribution Antenna Cable. It is typically a coax cable or radiating cable that connects to distribution antennas and is outside of the heat and fire protection provided by any firewalls or other means. Distribution antenna cables typically feed one or more distribution antennas in a building to provide specific coverage. When designing the layout of the distribution antenna cables, the RF system designer should consider the impact that the loss of a specific distribution antenna cable could have on the overall operation of the in-building emergency responder communications enhancement system and its coverage area.

A.3.3.52 Emergency. The AHJ of the responding agency can determine which types of events qualify as emergencies.

A.3.3.54 Emergency Event Processing/Dispatching. This term includes caller interrogation and resource selection (the determination of which emergency response unit will respond) up to the start of the emergency response facility notification process.

A.3.3.56 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.3.3.57 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.3.3.59 Public Safety Emergency Communications System. A public safety emergency communications system consists of any technology or system utilized for the reporting, detection, coordination, dispatching, monitoring, or tracking of emergency incidents or emergency response resources, and the support of related activities.

A.3.3.61 Event. All incoming calls on designated emergency telephone lines should be considered emergency events until answered by a telecommunicator. If a telecommunicator determines that the reason for the call is not an emergency as defined in 3.3.52, the call will not count against the performance requirements of Section 15.4. A trouble or supervisory signal is not an indication of an event. *(See also 3.3.132, Trouble Signal.)*

A.3.3.62 Event Data. Other explanatory information can include, but is not limited to, sensor types, alarm types, and access information.

A.3.3.63 Frequencies. Emergency service agencies utilize many different frequencies and modulation technologies to communicate. Frequencies and modulation technologies might include, but not be limited to wavebands, such as very high frequency (VHF), ultra high frequency (UHF), 700/800 MHz, broadband, long-term evolution, etc. When evaluating in-building emergency responder communications enhancement system coverage capabilities, it is important to identify all frequencies and modulation technologies being utilized by and assigned to the public safety agencies of the jurisdiction as detailed in Section 18.11. For example, in the US, the public safety agencies in a jurisdiction might have an 800 MHz trunked land mobile radio system and might also utilize broadband services as a method of their on-scene communications. This could include the nationwide public safety broadband network supported by the FirstNet Authority and other broadband commercial carrier networks.

A.3.3.72 IP-Enabled Device. An IP-enabled device is not a land mobile radio narrowband device. Examples include smart phones, tablets, and laptop computers.

A.3.3.75 Logging Recorder. Event and dispatch information could include voice, ANI, ALI, dispatch records, date, time, and other incident-specific details. A logging recorder is normally a multichannel device that keeps a semipermanent record of all data and media associated with an event.

A.3.3.81 Multi-Line Telephone System (MLTS). The term *multi-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-based and call-server-based solutions, including network-based and premises-based systems (e.g., Centrex and Voice over Internet Protocol, as well as PBX, hybrid, and key telephone systems, as classified by the FCC under Part 68 requirements).

A.3.3.83 Notification. Notification can be made by either electronic or mechanical means.

A.3.3.93 Private Branch Exchange (PBX). The PBX system was first developed to allow a private entity to connect the tele-

phone 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).

A PBX also allows extension-to-extension telephone calls without connecting to the public switched telephone network.

A.3.3.99 Public Safety Answering Point (PSAP). A PSAP is a facility at which emergency calls are first answered, assessed, triaged, classified, and prioritized. The FCC further defines a primary PSAP as a facility to which 9-1-1 calls are routed directly from the 9-1-1 control office. A secondary PSAP is defined as a facility to which 9-1-1 calls are transferred from a primary PSAP.

A.3.3.101.2 Public Safety Communications Manager/Director. The public safety communications manager/director supervises the coordination and prioritization of all the activities of the public safety telecommunications center. The management of communications center operations includes, but is not limited to, preparation of documentation for contractual requirements, budgets, legislative actions, policies and procedures, and guidelines affecting public safety communications personnel.

A.3.3.101.3 Public Safety Communications Supervisor. A supervisor promotes individual and organizational performance to achieve the agency's mission, standards, and goals through leadership and training to provide the highest possible level of public safety communications services. First-level supervision indicates the person who provides direct oversight of the telecommunicators on the shift.

A.3.3.105 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,** 2022]

A.3.3.106 Radio Control Station. 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.

A.3.3.107 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.3.3.108 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 it is not housed in a building, equipment is usually located in prefabricated enclosures to provide weather protection.

A.3.3.113 Response Unit. Some examples of response units include patrol cars, ambulances, rescue vehicles, pumpers, ladder trucks, elevating platforms, service vehicles, marine units, supervisor vehicles, tow trucks, motor assistance vehicles, construction equipment, mass transit vehicles, and personnel assigned a unique identification number or name used for dispatches.

A.3.3.115 RF System Designer. The frequency license holder(s) and the AHJ should evaluate the competency level of the RF system designer's skills and experience. This can be achieved by requiring certification of in-building emergency responder communications enhancement system training issued by an approved organization or approved school and documented training by the manufacturer of the equipment being installed.

Additionally, some jurisdictions could require the RF system designer to have a valid FCC general radio operator's license or the equivalent from the licensing authority. The technology and tools used by designers has moved well past where a radio telephone operator's license provides sufficient training, in and of itself. Several organizations, including the National Institute for Certification in Engineering Technologies (NICET), are developing training programs for designers.

The certifying entities should have an established formal complaint and appeals process to address situations in which the RF system designer's work creates serious safety issues for ERUs or the citizens they serve.

Several factors to consider when evaluating a RF system designer include, but are not limited to, the following:

(1) Predictive modeling software is often utilized in the design of an in-building ERCES. The designer should be trained and certified by the predictive modeling software manufacturer beyond a basic competency level and should retain that competency via continuing education.
(2) The designer should provide evidence that they have detailed knowledge of RF design. This can include knowledge of link budgets in both directions; the impact of excessive amplification on area RF noise levels and the possibility of system self-oscillation; the near-far problem within the structure; the ability to precisely define installation and adjustment parameters to installers; the ability to verify via testing that an installation meets the original design criteria; and the ability to assist in troubleshooting system or interference problems.
(3) The designer should conform to ethical practices, quality assurance practices, certification or licensing by recognized outside authorities, and the presence of ongoing continuing education in RF design.

A.3.3.119 Standard Operating Procedures (SOPs). In some jurisdictions, SOPs are also known as standard operating guidelines (SOGs).

A.3.3.128 Telematics. Vehicle systems can include GSM, GPRS, SMS, GPS, and vehicle telemetry.

A.3.3.134 Two-Way Alphanumeric Devices. Two-way alphanumeric devices do not have the capability to provide voice messages.

A.3.3.135 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, (e.g., batteries). The inverter in the static UPS also includes components for power conditioning.

A.3.3.136 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.3.3.137 Voice Connection. Examples of voice connections include the following:

(1) Centralized automatic message accounting (CAMA) trunks
(2) Voice over Internet Protocol (VoIP)
(3) Digital subscriber line (DSL)
(4) Hotline
(5) Landline
(6) Line
(7) Party line
(8) Phone line
(9) Private line
(10) Subscriber line
(11) Telephone line
(12) Toll line
(13) Trunk line
(14) WATS line

A.4.1.2.3 Organization and management responsibilities should be addressed by the agency that personnel represent. The authority having jurisdiction should define the agency requirements for progression to positions of management responsibility. The agency can delegate additional duties or other responsibilities without being considered management.

A.4.1.2.6 The committee recognizes the importance of formal and continuing education and training programs to ensure that personnel at the various response levels maintain current knowledge, skills, and abilities. Continuing education and training programs can be developed or administered by local, state, provincial, or federal agencies, as well as by professional associations and accredited institutions of higher education. The methods of learning could include areas of technology, refresher training, skills practices, and knowledge application to standards. The subject matter should directly relate to the requirements of this standard.

A.4.1.3.4 It is recommended, where practical, that evaluators be individuals who are not directly involved as instructors for the requirement being evaluated.

A.4.1.3.5 The acceptance of nationally recognized governance, although it is not law, should be considered when practices and procedures are applied.

A.4.1.3.9(1) Training requirements and certifications of individuals working in the public safety communications center should be defined by this standard or any other industry standard that is applicable. All individuals filling the positions defined by this standard, even on a part-time or temporary basis, should meet all minimum qualifications, training requirements, and standards applicable to the position and should meet all local, state, and federal certification requirements.

The committee recognizes the need for formal training programs to provide the necessary skills and knowledge to perform the job of the telecommunicator.

These programs can be developed or administered by local, state, provincial, or federal agencies, as well as by professional associations.

In many jurisdictions, part of this formal training includes some form of on-the-job training. *(See Annex E for a discussion of the considerations of the training of enhanced telecommunicator skills.)*

A.4.1.3.9(4) Medical and physical requirements that are job-related and in compliance with the Equal Employment Opportunity Act, the Americans with Disabilities Act, and other applicable legal requirements should be developed by the AHJ. The AHJ is required under the Americans with Disabilities Act to identify the functional requirements for the performance of the job. The AHJ should consider the physical arrangement of the workspace and the various pieces of equipment required for operation by the employee. Specific medical and physical abilities are required to perform essential functions of the job.

They include, but are not limited to, the following:

(1) *Hearing.* Distinguish, differentiate, and respond to multiple audible stimuli from personnel or equipment, such as a telephone, radio, or alarm
(2) *Sight.* Distinguish, differentiate, and respond to multiple visual stimuli such as printed documents, CRT displays, and indicator lights
(3) *Manual dexterity.* Operate radios, computers, and other equipment used in a telecommunications center
(4) *Speech.* Clearly convey verbal messages utilizing telecommunication devices

The public safety telecommunicator is the initial contact for managing requests for services provided by public safety agencies. Decisions are made based on incoming and updated information. The ability to receive information audibly is essential to the job. Additionally, much emphasis is placed on visual ability and manual dexterity. Identification of audio and visual cues, incoming telephone lines, 9-1-1 screens, incident cards/screens, messages, requests, memorandums, and so forth, is imperative for performing the required job duties.

The committee has identified the following behavioral characteristics or traits that the hiring or certifying authority might want a candidate to be able to exhibit:

(1) Adjusting to various levels of activity
(2) Displaying appropriate personal behavior
(3) Accepting constructive feedback
(4) Remembering and recalling information
(5) Displaying tolerance
(6) Functioning under stress
(7) Maintaining confidentiality

A.4.1.3.9(5) An individual should meet the cognitive and psychomotor skill requirements for reading, spelling, speech, mathematics, basic language, written communication, listening, and basic computer skills in addition to other requirements developed by the AHJ.

The committee recommends that the following skills be considered by the AHJ for the telecommunicator candidate:

(1) Ability to spell
(2) Basic reading skills
(3) Basic math calculation

(4) Ability to speak clearly
(5) Basic writing skills
(6) Manual dexterity
(7) Ability to follow written and verbal instructions
(8) Ability to alphabetize and catalog
(9) Keyboarding and mousing skills as required
(10) Multi-tasking
(11) Quick decision-making
(12) Teamwork
(13) Critical thinking
(14) Customer service skills
(15) Problem solving
(16) Interpersonal communication skills

A.4.1.3.12 Remaining professionally competent is important for any practitioner. In the rapidly changing and developing field of the fire service, this is particularly important. The AHJ might consider establishing a path by which members can demonstrate continued JPR compliance and competency through continuing education or practice within the field consistent with current duties. It is recommended that any such program consider the following factors:

(1) Demonstrated and documented knowledge of and competence with additions and/or revisions to the latest editions of the standards
(2) Documented training and education (including online) related to the changes to the standards since the last certification
(3) Documented experience in the field (i.e., emergency operational experience for firefighters, fire officers, instructors, etc.)
(4) Demonstrated and documented performance of duties, which might include a skills assessment
(5) Annual performance appraisals
(6) Documented teaching and instruction related to the field
(7) Commendations, awards, or recognition for the performance of related duties

Other items for consideration can include the following:

(1) Memberships in professional organizations, including any positions held or special activities involved in the membership
(2) Published articles in trade journals, web-based publications, and other information distribution avenues
(3) Research and development activities related to the field
(4) Documented attendance at relevant conferences and training events

The above list is not all-inclusive, and other factors specific to the field should be considered.

A.4.3.2(A) For additional information on the verbal communication process, see Annex D.

A.4.3.2(B) The Public Safety Telecommunicator I should be capable of operating, testing, troubleshooting, and maintaining the continuity of the communication system. The Public Safety Telecommunicator I might also be required to switch to and operate backup components or alternative systems.

A.4.3.3(B) This could also include managing situations such as excited or hysterical callers, callers speaking foreign languages, suicidal callers, and other calls requiring special handling, including mass casualty and weapons of mass destruction incidents.

A.4.3.4(A) Nonverbal communication protocols include American Sign Language (ASL) syntax. The telecommunicator should also know common abbreviations used in nonverbal communication. Individuals who are hearing or speech impaired often use ASL syntax while communicating via a telecommunications device for the deaf/teletype (TDD/TTY) or text phone. ASL is a separate language that uses English words but has its own rules for syntax and sentence construction.

A.4.3.4(B) The Americans with Disabilities Act (ADA) requires equal access to emergency services by individuals with speech and hearing impairments. This most often takes the form of a TDD/TTY or text phone using Baudot tone or ASCII code. Other nonverbal devices include computers, digital terminals, analog devices, alarm systems, fax machines, and other mechanical or electronic media.

A.4.4.1 This should be done according to 16.4.2.1. The PSAP should remain on the line until it is certain that the transfer has been completed.

A.4.4.3(A) The Public Safety Telecommunicator I is expected to question callers regarding potential threats, risks, and hazards that responders can encounter. Examples include details pertaining to the involvement of weapons, hazardous materials, violent subjects at the scene, unsafe conditions en route to or at the scene, and so forth.

A.4.4.4 Special or unusual circumstances are most often typified by hang-up calls or silent calls. These circumstances should be handled by following the procedures, policies, or guidelines of the AHJ.

A.4.5.1(A) Pre-arrival instruction protocols will be provided based on the policies, procedures, or guidelines of the AHJ.

The functions of the Public Safety Telecommunicator might include the use of predetermined questions, pre-arrival telephone instructions, and pre-assigned actions that are integral parts of the responsibility to prioritize calls and assist in the stabilization of a situation.

A pre-arrival reference system should be in a uniform format that is an accessible and reproducible document based on current guidelines and administrative protocols.

A.4.5.1(B) Voice control includes the ability to maintain a balanced tone, modulation, volume, and inflection while communicating.

A.4.5.2 In some jurisdictions the on-duty telecommunicator could be responsible for both call taking and dispatching. Other entities can include social service agencies, utilities, other emergency service providers, or other governmental units. Resolution might be accomplished by referral to, or response by, one of these agencies.

A.5.2.1 These sources can include other telecommunicators, field units, or electronic devices.

A.5.2.2 See Chapter 17 for information on alert tones.

A.5.2.2(A) The Public Safety Telecommunicator II should be capable of operating, testing, troubleshooting, and maintaining the continuity of the communication systems, including radio codes, unit identifiers, emergency alert tones, and the phonetic alphabet. The Public Safety Telecommunicator II might also be required to switch to and operate backup components or alternative systems.

A.5.2.3 These systems might include computer-aided dispatch systems, recording systems, automatic vehicle tracking systems, mobile data systems, and computer systems linking the telecommunicator with other agencies.

A.5.2.3(A) This can include familiarity with computer operations and technology.

A.5.2.3(B) This can also include data system messages.

A.5.3.3 Deployable resources include those individuals, equipment, and specialized units that are dispatched by the agency.

A.5.3.3(A) See Chapter 15 on operations.

A.5.3.6 This action is not a static decision but rather a dynamic process that changes and evolves during the handling of an event. The Public Safety Telecommunicator II is required to make many decisions that might not change the action originally initiated. Factors that cause changes to decisions or actions are the receipt and processing of additional information or updates. The Public Safety Telecommunicator II makes necessary decisions and takes actions that will result in the appropriate assignment of resources, emphasizing the safety of the public and the response units. *(See Figure A.5.3.6.)*

A.5.4.1 The public safety telecommunicator should operate within the incident management system prescribed by the AHJ as is defined in NFPA 1561. The telecommunications equipment used by public safety agencies is widely varied. The term *telecommunications equipment* includes all equipment in use by an agency for alerting or notifying response units and the continued exchange of information between those units and the communications center. Examples include computer-aided dispatch (CAD) systems, mobile data terminals, two-way radios, paging systems, alerting devices, telegraph systems, telephone systems, voice alerting and PA systems, and data terminals.

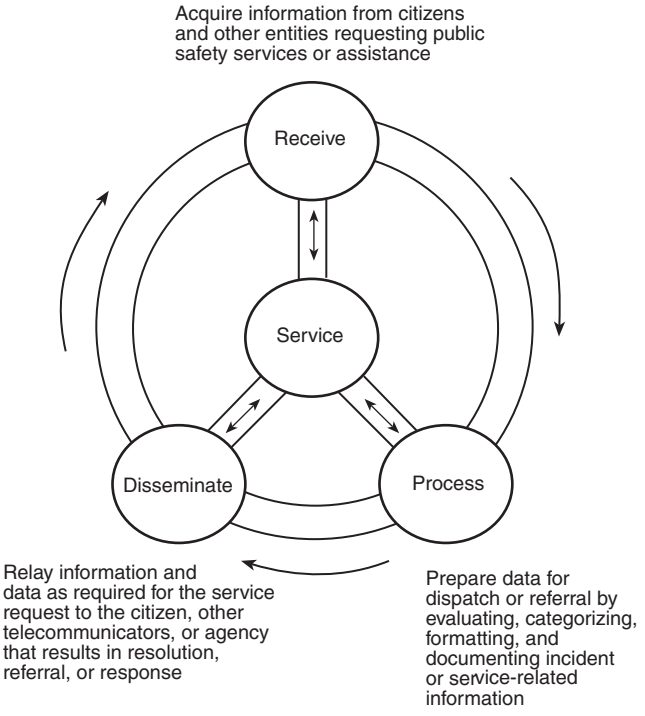


FIGURE A.5.3.6 Model of Processing a Request for Service.

A.5.4.2 In the case of unfounded service requests, hang-up calls, or invalid locations, the telecommunicator should make every effort to reverify the accuracy of a location or the validity of a service request within the policies established by the AHJ.

A.5.4.4(B) Supplemental information could include relevant databases and documentation that might be internal or external to the agency available to provide ongoing support to response units.

Emergency plans should be developed in accordance with *NFPA 1600*.

A.5.4.5 Situations beyond the normal scope of operation could include a major crime occurrence, major fire, mass casualty incidents, weapons of mass destruction, and man-made or natural disasters.

A.7.1 It is important to consider APCO ANS 3.101.3, *Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO),* when establishing the job performance requirements for this position.

A.8.1 It is important to consider APCO ANS 3.102.2, *Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor,* when establishing the job performance requirements for this position. It is recommended that the supervisor also meet the requirements of the Public Safety Communications Training Officer.

A.9.1 It is important to consider APCO ANS 3.106.2, *Core Competencies and Minimum Training Standards for Public Safety Communications Quality Assurance Evaluators (QAE),* when establishing the job performance requirements for this position.

A.10.1 It is important to consider APCO ANS 3.104.2, *Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator,* when establishing the job performance requirements for this position.

A.11.1 It is important to consider APCO ANS 3.109.1, *Core Competencies and Minimum Training Standards for Public Safety Communications Manager/Director,* when establishing the job performance requirements for this position.

A.12.1.3 Telematics provide emergency communications from either a person requesting emergency assistance or an autonomous request such as an automatic crash notification (ACN). The communication request is routed to a PSAP from a third-party telematics service provider. The TSP can contact the PSAP through dedicated 9-1-1 trunk or ALI-supported telephone system. Communications types to the PSAP could include automatically generated incident location, automatically generated incident location with data, or voice communications with automatically generated incident location with data.

A.12.2.1 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 man-made 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 neces-

sary 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.12.2.2 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. Where there is no local CEMP, or are no CEMPs applicable to the PSAP, the PSAP would need to develop its own.

A.12.2.2.3 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.12.2.2.4 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.12.2.2.5 Tactical interoperable communication plan (TICP) templates are available at dhs.gov/safecom.

A.12.2.6 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.12.2.6.2 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.12.2.6.3.2 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.12.2.6.4 This requirement is intended to ensure that emergency communications systems will continue to operate, even if the primary communications center is completely destroyed.

A.12.2.7 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.12.2.9 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.12.3.2 Consideration should also be given to hazards associated with falling trees, antennas, or other similar structures.

A.12.3.3 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 choose a site significantly above the 100-year floodplain elevation.

A.12.4.5 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.12.4.9.1 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.12.5.1.1.1 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.12.5.1.2 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.12.5.1.3 US Army Technical Manual TM 5-602-1, *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.12.5.1.5 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.12.5.1.7 Examples of equipment include packaged cooling systems and components such as chillers, compressors, condensers, supply air fans, and return air fans.

A.12.5.1.8 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.12.5.1.9 Air intakes should be installed and maintained in accordance with DHHS (NIOSH)Publication Number 2002-139, *Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*.

A.12.7.3 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.12.7.4.5 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.12.7.5 This applies whether the wall in question is provided with windows or not.

A.12.7.7 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 Buildings*, for additional guidance.

A.12.8.1.5 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 12.

A.12.8.1.6 An example of control wiring that would be required to receive COPS treatment would be the remote generator annunciation wiring.

A.12.8.4 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.12.8.4.3 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.12.8.4.12 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.12.8.4.12.1 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.12.8.6.1 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 US Army Technical Manual TM 5-690, *Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*, The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, *Executive Report*, or at other sources.

A.12.8.7 Additional guidance can be obtained from US Army Technical Manual TM 5-690, *Grounding and Bonding in Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities*.

A.12.8.8.1 Storage batteries preferably should be located on the same floor as the operating equipment.

A.12.8.8.3 When sizing an ESS, consideration should be given to the potential for increased electrical loads as the center grows over time.

A.12.10 US Army Technical Manual TM 5-811-3, *Electrical Design: Lightning and Static Electricity Protection*, provides additional guidance.

A.12.11.2.2 Consideration should also be given to hazards associated with falling trees, antennas, and other similar structures.

A.12.11.2.4 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.12.11.3.6 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.12.11.3.7 A common example of such material is gypsum wallboard.

A.12.11.3.8 Examples of noncombustible floor materials are concrete, aluminum, and steel.

A.12.11.5.4 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.12.11.5.6 FM Global Property Loss Prevention Data Sheet 9-19, *Wildland Fire*, provides additional engineering guidance.

A.12.11.6.5 Such locations could include interior courtyards, light wells, and the like.

A.12.11.6.6 Department of Defense UFC 4-023-07, *Design to Resist Direct Fire Weapons Effects*, provides useful guidance.

A.12.11.6.7 Department of Defense UFC 4-022-02, *Selection and Application of Vehicle Barriers*, provides additional guidance.

A.12.11.6.8 Department of Defense UFC 4-023-03, *Design of Buildings to Resist Progressive Collapse*, provides additional guidance.

A.12.11.6.9 For the more information on central stations, refer to *NFPA 72*. For guidance on intrusion detection systems (IDS) see Department of Defense UFC 4-021-02, *Electronic Security Systems*.

A.12.11.7.5 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.12.11.7.6 Examples are motorized intake air louvers, fans supplying cooling or combustion air, fuel transfer pumps, and coolant pumps.

A.12.11.7.7.2 Refer to A.12.11.5.4.

A.12.11.7.8 Additional guidance is contained in US 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.12.11.8.1.2 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.12.11.9 US 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.13.1.1 Refer to *NFPA 70* for examples of installations that are and are not covered by *NFPA 70*.

A.13.5.2 Environmental conditions could exist that necessitate the use of rigid nonmetallic conduit.

A.13.6.1.3 Examples of SPD 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 SPD criteria for telephone lines can be found in the Telcordia Technologies publication TR-NWT-001361, *Generic Requirements for Gas Tube Protector Units (GTPUs)*.

A.13.6.7 The term *watertight* is typically used in conjunction with Enclosures Types 4, 4X, 6, and 6P. [**70:**Table 110.28 Informational Note No. 1]

A.13.8.1 Sensitive electronic equipment includes computers, telecommunications equipment, and two-way radio systems.

A.14.2.1 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.14.2.2 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.14.6 Local area network (LAN) computer and telephone cable are examples of communications conductors.

A.15.1.2 In the case of equipment such as repeaters, transmitters, towers, and generators, access needs to be available at all times.

A.15.2.2 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.15.3.1.1 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 affect the prompt receipt and processing of alarms in accordance with Section 15.4. Telecommunicator staffing is an important issue in achieving prompt receipt and processing of events. 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 events.

A.15.3.1.2 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.15.3.2 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 firefighter 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.

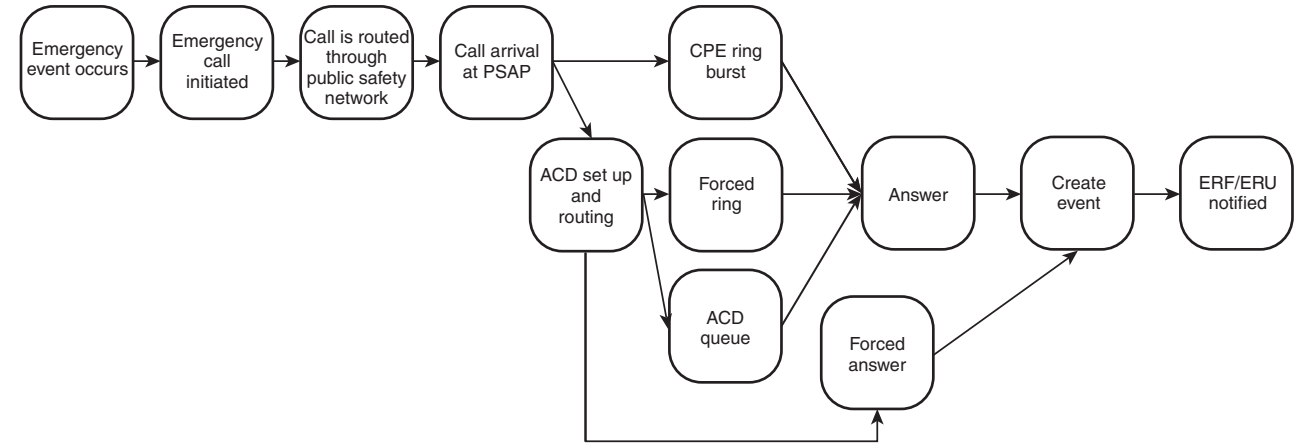
A.15.3.4 The supervisor position(s) in the communications center are provided in addition to the telecommunicators positions. Although supervisory personnel are intended to be available for problem solving, the supervisor position is permitted to be a working position.

A.15.4.1 Statistical analysis for performance measurement should be completed over a period of 1 month as shown in Figure A.15.4.1(a) and Figure A.15.4.1(b).

A.15.4.3 PSAPs, 9-1-1 authorities, and responder agencies should look at the processing times in a comprehensive manner. Transfers, especially multiple transfers, have the impact of making compliance with the overall processing time standard nearly impossible. Given the life safety implications for critical incidents, PSAPs should make every effort to reduce/eliminate transfers, thereby reducing the amount of time required to answer, process, transfer, and dispatch alarms. Potential strategies to reduce transfers include consolidation, either physical or virtual, CAD to CAD integrations, improved wireless call routing, and improved compliance with call answering standards. See Figure A.15.4.1(a).

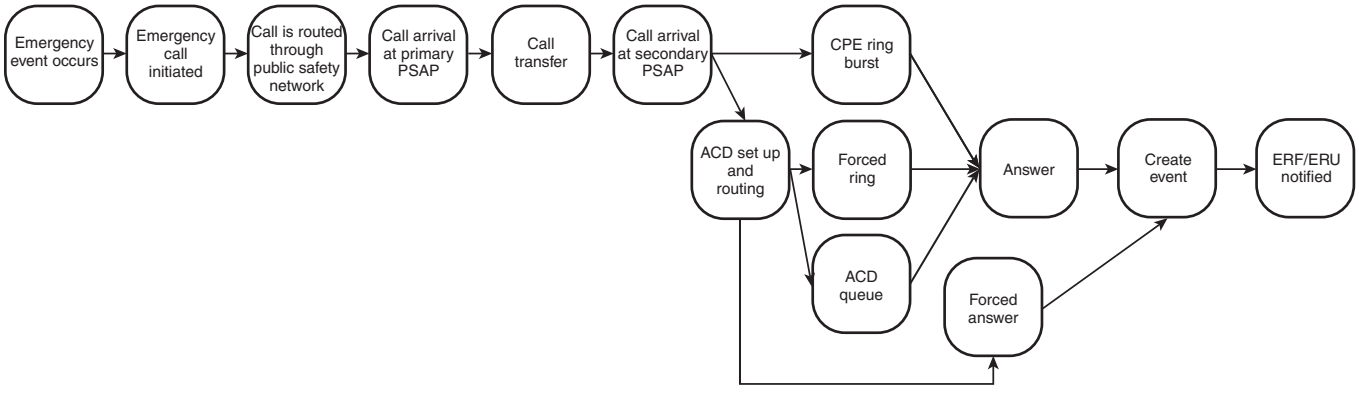
Where the communications center is a secondary PSAP, every effort should be made to assess transfer performance consistent with 15.4.2 for all primary PSAPs who routinely transfer calls to the communications center. See Figure A.15.4.1(b).

A.15.4.4 Events 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 events 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.



Detection	Transmission		Time to answer	Event processing
Varies	<1 second	<3 seconds	≤15 seconds 90% ≤20 seconds 95%	≤60 seconds 90%

FIGURE A.15.4.1(a) Event Timeline Where Primary PSAP Is Communications Center.



Detection	Transmission	Transfer	Time to answer	Event processing
Varies	≤4 seconds	≤30 seconds 90%	≤15 seconds 90% ≤20 seconds 95%	≤60 seconds 90%

FIGURE A.15.4.1(b) Event Timeline Where Primary PSAP Is Other Than Communications Center.

A.15.4.4.5(3) Each agency has access to different technology and location tools and references. In many cases, additional location interrogation or questioning is required by the call taker. Scenarios to consider when determining whether incomplete location information is a mitigating circumstance can include the following:

(1) The caller does not know or cannot provide the full address.
(2) The caller does not know or cannot provide the full address, but the call taker received the call with a Phase 2 location.
(3) The call comes in as Phase 1 (cell tower address), and the call taker has to rebid to get a Phase 2 location.
(4) The call taker must use technology tools to find a location (e.g., search engines, third-party location services, CAD history, motor vehicle database).
(5) The caller says "hold on" while looking for an address.
(6) The caller can provide a common business name but does not have the physical address.
(7) The caller needs guidance or direction in finding an address.
(8) The location interrogation takes longer than a specified time frame (e.g., automatic exemption after specific time frame).

A.15.4.5 The following types of calls where there is an imminent threat to public safety should be included in the highest prioritization level:

(1) Active shooter/hostile event
(2) Domestic violence with weapons
(3) Officer-involved shooting
(4) Robbery in progress
(5) Other calls as determined by the AHJ

A.15.4.10 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.15.4.11 The audible warning or signal is typically a distinctive tone.

A.15.4.13 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.15.4.14 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 F.)*

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.15.4.14.2 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.15.4.14.2(3) Extended operations can include long-term disaster recovery, security at major events, or criminal justice surveillance.

A.15.4.18 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, *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-102.BAAA, *Project 25 FDMA Common Air Interface*.

A.15.4.18.1 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.15.4.18.2 Exercising this plan identifies areas that need improvement.

A.15.4.21 Procedures for handling telecommunication relay services (TRS) calls should be included in the SOPs.

A.15.6.1(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.15.7 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.16.1 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 (Wi-Fi) all use voice over Internet protocol (VoIP).

Receiving equipment should be able to answer the following type of calls or events:

(1) *Voice to 9-1-1.* Incoming requests for assistance from devices capable of sending and receiving voice
(2) *Text to 9-1-1.* Incoming requests for assistance from devices capable of sending and receiving SMS or real-time text messages
(3) *Video to 9-1-1.* Incoming requests for assistance from devices capable of sending and receiving video
(4) *Static Images to 9-1-1.* Incoming requests for assistance from devices capable of sending static images
(5) *Machine to 9-1-1.* Incoming requests for assistance from devices capable of machine-to-machine communications

A.16.2.2.5 A separate telephone number listed in the 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. That location can be the same communications center as 9-1-1 operations.

A.16.2.3.5 A voice connection terminating at an unstaffed ERF and provided with a recorded message should not be used to meet the intent of the telephone number listed in the directory and assigned for business (i.e., nonemergency) use as specified in 16.2.3.2.

A.16.4(2) 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.16.4.2 There are existing means to determine the location-appropriate communications center such as the NENA Enhanced PSAP Registry and Census.

A.16.4.4 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.16.4.5 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.16.4.7 Standards include NENA i3; APCO/CSAA ANS 2.101.2, *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)*; and others.

A.16.5.1 See *NFPA 1600* for additional guidance.

A.16.5.4(2) The AHJ can approve a queuing system for calls on emergency numbers. Such systems often need the additional approval of regional, county, or state authorities.

A.16.6.1 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.16.6.2 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.16.6.3 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.17.1.1 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. Events can be reported to the communications center where the telecommunicator can start a siren or operate an air horn to indicate that there is an event. 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 telephone lines. In emergency response agencies that have an emergency response facility desk attendant, the 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.17.1.1.3.2 In jurisdictions receiving fewer than 730 events per year (average of two events per 24-hour period), a second dedicated dispatch circuit might not be necessary.

A.17.1.1.3.3 When an event 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.17.1.1.4(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.17.1.1.4(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.17.1.1.5.1(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.17.1.1.5.1(2)(a) In 17.1.1.5.1(2)(a)ii, a separate receiver is not required for each ERU.

A.17.1.1.5.1(3)(a) In 17.1.1.5.1(2)(a)(i), 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.17.1.1.6 The audible warning or signal is typically a distinctive tone.

A.17.1.2 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.17.1.2.1 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.17.1.2.6 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.17.2.1.1 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 27.5.2 of *NFPA 72*).

A.17.3.1.1 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.17.3.1.2.2 It is recommended that the system be designed for DAQ of 3.4.

A.17.3.1.3 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.17.3.1.4 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.17.3.1.5 The intent of 17.3.1.5 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.17.3.1.6 This does not prohibit the use of field-deployed portable repeater systems.

A.17.3.2.3(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.17.3.3.1 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.17.3.4.1 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.17.3.4.1.5 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.17.3.4.1.8 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.17.3.4.1.9 The emergency level of priority is intended for use only when immediate communications are necessary to preserve safety or protect life.

A.17.3.4.1.10 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.17.3.4.1.11 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.17.3.4.1.16 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.17.3.4.1.17 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.17.3.4.1.17.1 Several reasons for disablement can be a stuck microphone, the unit is out of frequency, or the unit is lost.

A.17.3.4.1.18 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.17.3.4.1.19 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.17.3.4.1.24 In the design and operation of a trunked radio system, dispatching of events 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.17.3.4.2 Digital trunked system subscriber units operating in the United States on the 700-MHz narrowband public safety spectrum and complying with TIA-102.AABF-D, *Project 25 Link Control Word Formats and Messages New Technology Standards Project — Digital Radio Technical Standards*, and TIA-102.BBAC, *Project 25 Two-Slot TDMA MAC Layer Specification*, must also comply with TIA-102.BAAA, *Project 25 FDMA Common Air Interface*, in order to operate on the required designated nationwide 700-MHz narrowband interoperability channels.

A.17.3.5 The 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 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.17.3.6 The 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: ntia.doc.gov/category/firstnet

A.17.3.6.13 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.17.3.7 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.17.3.8.1(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.17.3.8.1(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.17.3.8.1(2)(b).

A.17.3.8.3.2 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

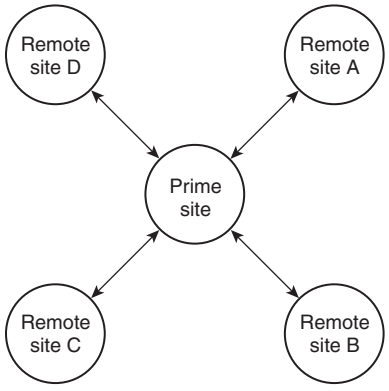


FIGURE A.17.3.8.1(2)(a) Star Microwave System.

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.

A.17.3.8.5.1 *Components,* in this context, refers to modular elements such as transmitters, receivers, modems, power supplies, switching devices, multiplexers, and service channels/orderwire equipment.

A.17.3.8.5.4 Examples of alarms are input power failure, transmitter RF output, radio off frequency, and excessive bit error rate.

A.17.4.2.1 Paging systems not under the direct control of the AHJ are permitted to be used for administrative and secondary alerting purposes but are not considered acceptable for use as a required primary dispatch system. Third-party paging systems not under the control of the AHJ often do not have the redundant design architecture to comply with 17.1.1.4. 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.17.4.2.7 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.17.4.2.11 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.17.4.2.12 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.17.4.3 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.

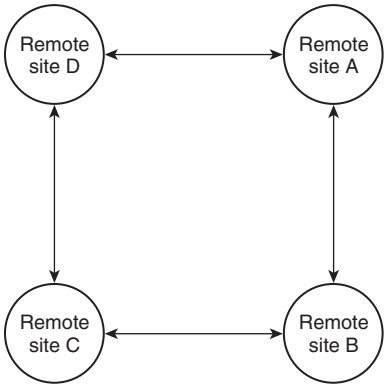


FIGURE A.17.3.8.1(2)(b) Ring Microwave System.

A.18.2.1 In many countries, the frequency license holder(s) is legally responsible for retransmission on the frequencies to which the licensee is licensed by the licensing authority of the country of jurisdiction. Therefore, the frequency license holder(s) must be able to review and approve every ERCES design prior to the commencement of any ERCES installation. The purpose of the initial review is to determine if the design, equipment selection, and overall solution will properly operate and not cause interference on the public safety land mobile radio system. For example, in the United States, this is covered in 47 CFR, *Federal Communications Commission.*

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

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

A.18.3 There are multiple system solutions that might solve the problem of in-building RF coverage for ERUs. The choice depends on many factors, including the proximity and number of buildings with such systems, the RF noise floor in the area, the costs to agencies and building owners, and the accessibility to various agencies, such as fire, emergency medical services (EMS), and law enforcement. Ideally, the RF design professional should provide frequency license holder(s) and AHJs with an analysis of the pros and cons of the options that are most useful in the particular building, so that the AHJ and frequency license holder(s) can choose a solution. This review should be made each time a new solution is proposed for another building in the vicinity, because multiple devices can have an increasing impact on noise floor and other system parameters.

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

Table A.18.3 Possible In-Building Technical Solutions

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

(continues)

Table A.18.3 *Continued*

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

(continues)

Table A.18.3 *Continued*

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

NA: Not applicable.

A.18.3.2 Mandating oscillation detection and control does not ensure the equipment will maintain operation to the best extent possible during an emergency. If a signal booster shuts down during oscillation that could leave emergency personnel stranded without communications coverage during an emergency. Oscillation is caused by the reduction in isolation between the inside and outdoor donor antennas. An event such as fire or earth movement can cause damage to the building, thereby reducing the isolation between the inside antennas and the outside donor antenna. If the signal booster were to reduce gain until oscillation is no longer present, there would be some level of communications coverage.

A.18.3.4.1 Near-far problems arise when a distributed antenna system (DAS) is not designed correctly. These problems are caused by a transmission from a portable that is near a DAS antenna, overpowering the uplink amplifier. When this occurs, the strong signal forces the amplifier into a reduced gain situation. Other portables transmitting simultaneously on a different channel(s), far away from the antenna system, will not be provided the gain necessary to achieve adequate uplink communications.

A.18.4 US Army Technical Manual TM 5-811-3, *Electrical Design: Lightning and Static Electricity Protection*, provides additional guidance.

A.18.6.1 Frequencies and modulation technologies utilized by emergency services are assigned by the licensing authority of the country of jurisdiction. In the US, for example, the FCC assigns frequencies that may be utilized by emergency services. Typically, these are thought of in the VHF, UHF, and 700/800 MHz bands. More recently, the US government created a nationwide public safety broadband network for use by emergency services. As more jurisdictions utilize non-traditional broadband networks for emergency service operations the need to have those capabilities as a part of the in-building emergency responder communications enhancement system will be important for incident operations. It is important to understand that to enhance coverage of any commercial carrier broadband signal, prior coordination and approval must be obtained from the frequency license holder of those frequencies.

A.18.6.3 Use of shared commercial and public safety systems on the same in-building communications enhancement system infrastructure should be evaluated to ensure that systems and technology provide optimized operational capabilities. Multiple DAS systems, whether combined or not, need to be designed and configured to avoid interference with each other and with other building RF systems.

A.18.7.2 Written consent from the radio frequency licensing authority could be required in some areas. An example of where the radio frequency licensing authority could require express written consent is through the FCC in the United States. The FCC rule Title 47, CFR, Part 90.219(b) states, in part, the following:

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

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

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

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

A.18.8 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 wired 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 "firefighter 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.18.9 Many radio systems are in use by public safety agencies in the United States. A number of them have different operational characteristics. A prescribed signal strength measurement might not produce usable voice communications for all systems [e.g., VHF, UHF, 700/800 MHz, analog, P-25, 4 slot time division multiple access (TDMA), 2 slot TDMA, etc.]. Requiring the AHJ to provide operational parameters required for usable voice communications for the systems in use eliminates possible confusion regarding the specified value, as determined by the AHJ. A better indicator of proper system performance and coverage is to use the DAQ audio quality measurement system whether the signals are either analog or digital.

A.18.9.1 *Downlink* refers to the signal from the base station to the portable. Although DAQ 3.0 is required as a minimum, it is recommended that systems be designed for DAQ 3.4 to provide a safety factor.

A.18.9.2 *Uplink* refers to the signal from the portable to the base station.

A.18.9.3 Receiver noise floor testing can be accomplished by first noting the idle noise on all channels involved within the public safety communications system at the public safety communications site closest to the ERCES with the signal booster system off. This can be done by using a spectrum analyzer with the resolution bandwidth set to be equal or less than the noise bandwidth of the receiver used at the site. Note: Use 10 kHz for 12.5 kHz narrowband systems, and use 10 kHz for 25 kHz systems at 800 MHz in the US.

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

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

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

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

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

A.18.11 Newer transmission technologies, such as LTE and 5G, will dramatically change the capability of public safety communications systems.

A.18.11.2 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. In-building emergency responder communication enhancement systems that are used to comply with the requirements of Chapter 18 should be tested in accordance with 20.3.10. Also note that this is not easily done at VHF because of filters and nonstandard Tx and Rx spacings.

A.18.12.1 Radio licensing authorities in some countries have distinctions between consumer-grade and industrial-grade in-building emergency responder communications enhancement system. 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 cannot 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 (i.e., channelized) and type B signal boosters (i.e., 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.18.12.3.4 The intent of the fire-resistance rating requirements in 18.12.3.4 is to provide for survival of the radio system backbone components correlating to the design basis for structural integrity of the building in which the system is installed. The fire-resistance rating for the primary structural frame under *NFPA 5000* is established by the required rating for structural columns. Other building codes established the fire resistance requirements for the primary structural frame using the term *primary structural frame*.

A.18.14.1.2(2)(a) The signal source for an in-building emergency responder communications enhancement system is critical to keep the system operational. Loss or reduction of the RF signal from the public safety radio communications system to the in-building communications enhancement system can take multiple forms, depending on the nature of the signal source. In systems that use a RF link between the two sites, the disconnection of the antenna coax, a short in the coax, a damaged coax, or a misdirected donor antenna can cause a degradation of RF signals such that the in-building system will not work correctly. If the source of the signal is a fiber optic cable between the sites, then damage to that cable can cause loss of signal as well.

A.19.1.1 The AHJ should consider the performance requirements of this standard, particularly the time requirements of Section 15.4, in their decision making regarding the use of CAD. CAD systems can be deployed on premise, hosted, or in the cloud.

A.19.1.2 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 15.4 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.19.1.2.1 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.19.2 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.19.3.5 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.19.4.1.2 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.19.4.4 Other systems could include intelligent transportation systems, SMART building management systems, pre-fire/pre-incident software systems, and so forth.

A.19.5.3.2 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.19.5.6 Resources can include but are not limited to ERUs, individuals, equipment, or other assets.

A.19.5.6.1 Examples of safeguards include placing source code, documentation, and flow charts into escrow.

A.19.5.7.2 The requirements for audible notification for all text message activations regarding events apply even if there are other methods of notification installed and used at the ERF.

A.19.6.1 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.19.6.4 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.19.6.6 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.19.7 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.

Sufficient testing should occur on the backup systems to verify the completeness and accuracy of the backup and recovery data and process, including switching back to the primary system.

A.19.8.1.4 The AHJ should evaluate trends in the industry towards virtual environments. There are pros and cons to this approach that bear investigation. The CAD system can be designed to allow for the deployment of virtual servers, workstations, and storage at the discretion of the AHJ.

A.19.8.1.6 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.19.8.3 The AHJ should determine the data required to be logged for use by the operations room.

A.19.8.5 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.19.9.1 The capability should exist to move data to alternate, long-term storage for retrieval. Access to the data should be restricted through security measures enabled by the AHJ.

A.19.11.1 MDCs can include any IP-enabled device (e.g., smartphones, tablets, laptops).

A.19.11.2.2 Store and forward technology can provide this functionality.

A.19.11.5.4 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 22. The MDC should have the ability to present appropriate displays of daytime and nighttime for the protection of the user.

A.19.12.1 Integrated mapping can be a function available to the MDC with similar functionality as a CAD workstation.

A.20.3.10 Test Procedures. The test plan should ensure testing throughout the building. Test procedures should be as directed by the AHJ or the frequency license holder(s). The following information is provided to guide the AHJ or the frequency license holder(s) on several types of testing methods that can be used when testing an in-building emergency responder communications enhancement system.

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

Testing procedures typically are performed on a grid system. A grid is overlaid onto a floor area to provide 20 grid cells. Grid cells are provided with definite minimum and maximum dimensions. For most buildings, using a minimum grid dimension of 20 ft (6.1 m) and a maximum grid dimension of 80 ft (24.4 m) will suffice to encompass the entire floor area. Where a floor exceeds 128,000 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). It is also recommended that each sector be tested individually with 20 grid cells in each sector.

Signal strength measurements should be taken at the center of each grid, where required.

The DAQ scale is 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 3.4: Speech understandable with repetition only rarely required. Some noise/distortion.
(5) DAQ 4: Speech easily understood. Occasional noise/distortion.
(6) DAQ 4.5: Speech easily understood. Infrequent noise/distortion.
(7) DAQ 5: Speech easily understood.

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

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

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

The minimum allowable DAQ for each grid square is 3.0. Not more than two nonadjacent grid squares should be allowed to fail the test. In the event that three of the areas fail the test, or if two adjacent areas fail the test, then consideration should be given to redesigning and reinstalling the public safety radio enhancement system to meet the minimum system design requirements.

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 with an identification of the location on the floor. In addition, the gain values of all RF-emitting devices and system components should be measured and the test measurement results should be kept on file with the building owner and with the AHJ and licensee so that the measurements can be verified each year during annual tests.

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

Table A.1 of the TSB-88 standard provides several land mobile radio (LMR) technologies and variants that map SINR and BER to expected DAQ values. Determining DAQ for narrowband, analog, or P25 digital systems is conducted by

quantitatively measuring a minimum SINR value of 18 dB and a maximum BER value of 2.5 percent or by measuring to other values, as provided by the frequency license holder(s) and the AHJ.

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

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

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

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

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

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

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

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

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

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

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

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

To test the emergency responder communications enhancement system with two portable radios, the following procedure can be used: One portable radio should be positioned no greater than 10 ft (3 m) from an indoor distribution antenna or leaky coaxial cable. The second portable radio should be positioned at a distance that represents the farthest distance possible in that location of the building from an indoor distribution antenna or radiating cable. Both portables should be simultaneously keyed up on different frequencies or talkgroups within the same radio band, and listeners or POLQA test equipment on the two different frequencies or talkgroups should verify that the voice messages received were intelligible to DAQ 3.0. Testing should be performed on each floor; once per band, if multiple bands are supported; and once per each powered unit, if multiple units are used. These tests should use two frequencies specified by the AHJ. If the technology uses TDMA, the test should use two time slots on the same frequency.

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

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

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

For example, if a signal booster has been designed to enhance the communications signal within the building, one approach is to set up a test signal on an unused frequency through the in-building ERCES via keying a portable inside the building on the test frequency. Then, a walk test should be performed around the outside perimeter of the building at ground level, not less than 3 ft (1 m) away from the building walls, to measure the test signal's power level. The test process

should verify that the leaked signal at 3 ft (1 m) from the building walls is at least 15 dB below the average signal level from the public safety communications network on one or more channels of the public safety communications network, or not greater than a level determined by the frequency license holder(s).

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

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

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

Typically, acceptance tests are required by the AHJ and frequency license holder(s) prior to building occupancy. As-built drawings should be provided including all system design parameters, other information required from the DAQ level and commissioning tests, including a full report with grid locations, DAQ measurements, and RF-emitting device or system component gain values. The acceptance test typically entails a random test by the AHJ of radio communication in various portions of the building, especially including the critical areas. The AHJ and frequency license holder(s) can review any test documentation and ensure that the findings of the commissioning test with respect to DAQ levels and gain values are supported by the acceptance test.

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

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

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

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 RF system designer in possession of a current general radio operator's license or an equivalent license issued by the frequency licensing authority of the country of jurisdiction and other certifications, as required by the AHJ.

Local adopting jurisdictions could require the installing contractors to have an in-building emergency response communications enhancement system training certificate issued by a nationally recognized organization or school and a certificate issued by the manufacturer of the equipment being installed.

A.20.3.10.2.3.2(2) If, during testing, it is found that the link budget, system design parameters, internal construction conditions, or nearby development have changed, the system should be modified to maintain the optimum performance of the system.

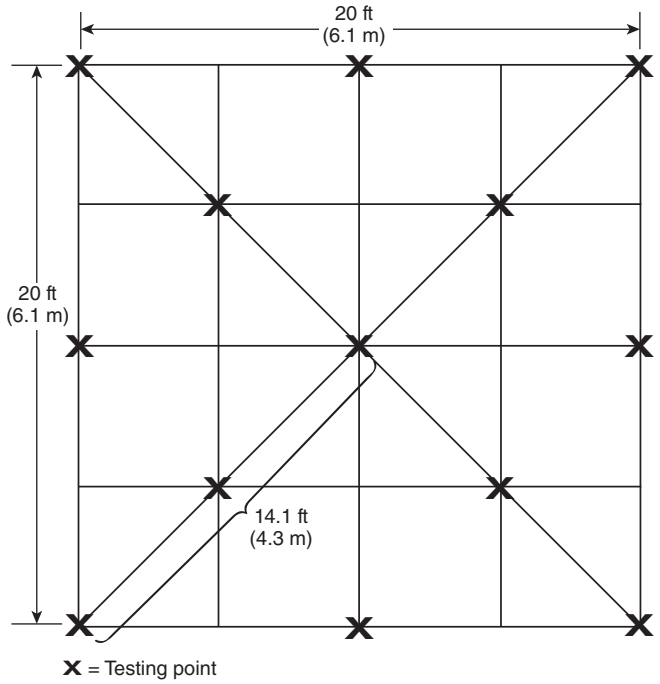


FIGURE A.20.3.10 POLQA Testing "X."

A.21.5.1 The CAD system should record a history (audit trail) of the following actions taken with the items:

(1) Creation
(2) Change, including modification, deletion, or supplementation
(3) Disposition, including close-out, archiving, and transfer
(4) Inquiry to external data sources

Each entry in the history should include the following:

(1) Coordinated universal time (UTC) of action
(2) Identification of the individual performing the action
(3) Identification of the device on which the action was performed
(4) Effects of action on the characteristics of the items

A.21.7.4.1 The AHJ needs to look at federal and state guidelines for records retention and be cognizant of the balance between the cost of long-term records retention and the need for records to be available for possible future legal purposes.

A.22.1 With the increasing numbers of people working from home, and the increase in ransomware attacks, the need for a comprehensive ICT security plan has never been greater.

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

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

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

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

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

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

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

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

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

A.22.1.4 All employees are responsible for maintaining security. Employment contracts, collective bargaining agreements, personnel manuals, and departmental directives should

Table A.22.1 Defense-in-Depth Strategies

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

enforce this responsibility. 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 or automatic monitoring for security compliance
(3) Routine auditing
(4) Archiving of security events or incidents for auditing or study

A.22.1.5 Recent events have revealed a common thread in many — attacks the adversary gains the credentials (i.e., 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." (dhs.gov/stopthinkconnect), which can be used as a foundation for such user training.

A.22.1.6 The goal of any information system is to only allow access by the following persons:

(1) Those who are authorized to use the system and are current employees
(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 (i.e., 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 (e.g., promotion, demotion, discharge)
(3) Password security rules (e.g., 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 (e.g., paper shredding, hard disk destruction)
(7) Implementation of two-factor authentication where feasible

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. End-end encryption can be available in future systems such as those that use LTE technology.

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 (i.e., something they know), and the token ID (i.e., 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 (i.e., 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 (i.e., lack of availability), false information is being placed on a trusted network (i.e., lack of integrity), and data are being stolen remotely (i.e., 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 or interoperability.

With the increased use of public and private cellular networks, first responders often use software applications that can provide the same information to a user of a cellular phone as if the person had an authorized subscriber unit on a public safety network. AHJs have to consider the operational consequences of this potential use.

A.22.1.7 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 DoS 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 17.3.4.1.18. 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.22.1.8 Computer systems have become not only the primary resource for storing information but also the primary workhorse for users to perform their jobs; therefore they have also become a primary objective for intruders for either data gathering or destruction. This makes a computer system the end point for security, and it requires layers to be built around it to minimize the risks associated with intruders accessing the information contained within the computer or with the trusted capability placed at their disposal.

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

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

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

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

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

(1) Worms
(2) Trojans
(3) Backdoor attacks
(4) Spyware
(5) Port scans
(6) VoIP attacks
(7) Internet protocol version 6 (IPv6) attacks
(8) DoS attacks
(9) Buffer overflows
(10) Statistical anomalies
(11) Protocol anomalies
(12) Application anomalies
(13) Malformed traffic
(14) Invalid headers
(15) Blended threats
(16) Rate-based attacks
(17) Zero-day threats
(18) TCP segmentation and IP fragmentation
(19) Unauthorized use of computational resources

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

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

Additional sources of information on cloud computing include the following:

(1) NIST SP 500-292, *NIST Cloud Computing Security Reference Architecture*, nist.gov/publications/nist-cloud-computing-reference-architecture
(2) NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, csrc.nist.gov/publications/detail/sp/800-144/final
(3) APCO, *Mitigating Risks in the Application of Cloud Computing in Law Enforcement*, psc.apcointl.org/2013/01/07/mitigating-risks-in-the-application-of-cloud-computing-in-law-enforcement-2

A.22.1.8.4.1 Videos, pictures, text messages, and emails received from the public could contain viruses or have other malware embedded within them.

A.22.1.8.5 AHJs are encouraged to adopt two-factor authentication for access to public safety networks and computers. Two-factor authentication means that a person must have something they know (i.e., a password) plus something that they possess. Many entities are using as the second factor a one-time security code sent to the employee's personal cell phone, or using a token device with a random number key generator. Two-factor authentication materially improves the defense of the networks and computer systems.

A.22.1.8.6 A DoS attack can take place in multiple ways, including a threat actor having robots make numerous simultaneous 9-1-1 calls, or numerous simultaneous text messages, or numerous simultaneous emails with videos or pictures. Another attack is a false message of emergency, which ties up ESUs on nonexistent emergencies. "Swatting" attacks where a person claims a SWAT team is needed because of a hostage or similar situation. AHJs should make plans for how to deal with these attacks and train employees on the plan.

A.22.1.9 A common approach to gaining unauthorized access to systems is to leverage a known vulnerability within a software system, which is why it becomes important to ensure that the system is properly maintained throughout its life cycle with up-to-date software versions and patches that close vulnerabilities and bugs. To help prevent existing vulnerabilities from being exploited, it is important to regularly patch an IT infrastructure. Because patch application can sometimes negatively affect the performance of critical communications land mobile radio systems, security patches should be tested in a controlled environment prior to production rollout. Common software attacks can be divided into several categories:

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

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

A.22.1.10 To ensure continuity of services when the system data are corrupted or destroyed, or the center must relocate because of fire, explosion, or natural disaster, disaster recovery provisions need to be in place. System configuration, temporary data, and static data (such as voice traffic stored in a voice logging recorder) need to be retained. Data retention is needed for several purposes: for legal records (voice logging recorders), for training and maintenance purposes, and to allow system recovery if the primary databases are corrupted or destroyed. Data retention should be guaranteed even during catastrophic failures such as network errors, hard-drive crashes, component failure, and server room obliteration. Database backups should be stored at a physically separate location. Because much of the information might contain legal, criminal, or medical information, the backups must be physically locked and secured to prevent copying, reading, or tampering. For first responder mission-critical communications systems, the importance of quickly recovering systems to bring the users and the system functionality back to full operational status is a matter of life and death. It is therefore important to find an enterprise backup solution that has been tested against the information system.

Backup and disaster recovery can be an expensive and time-consuming process. It is not just a matter of making regular backups and taking them offsite. Having the equipment and space to restore the off-site backups is often overlooked.

Disaster recovery procedures include fire service building preplans, incident response run cards, EMS preplans for certain high-risk individuals in the served community, and local law enforcement records.

A.22.1.10.2 Offsite storage of mission-critical information is highly encouraged. Loss of data can occur from malicious cyber attacks that aim to erase or modify data. Ransomware attacks have become more frequent. When a ransomware attack occurs, all data is encrypted and the agency must pay a ransom, sometimes in the thousands or millions of dollars, to regain the information. In some cases, despite a ransom being paid, the data is not returned. Data loss can occur when catastrophic physical site failure is caused by a storm, flood, fire, earthquake, etc. Cloud-based storage of such information is off-site, but this adds additional risks that need to be assessed.

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

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

Such backup data should be stored on media that is not connected to any network, which provides an "air gap".

A.22.1.10.4 Ransomware attacks on public safety agencies are becoming more common. In some cases the request is for a ransom payment in exchange for the key to unlock the data. On some occasions, the actor threatens to expose the data publicly if the ransom is not paid.

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

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

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

returned, and paying such a ransom will only encourage threat actors to continue and expand the practice.

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

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

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

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

A.22.1.11 Many computer security references and standards suggest implementing logging and auditing functions on computer networks. Without logs, investigating security breaches and incidents is a frustrating experience because there are very few data with which to reconstruct the incident. Additionally, legal action is impossible without the necessary proof. But functions implementing logging thoughtlessly can cause its own problems. For instance, logs can overrun a computer, making it run slower and eventually stopping all processes. This can occur when the logs are allowed to get too large. The larger the underlying log file, the longer it takes to append data to the file; eventually, the delay can become noticeable. This can happen when the logs have taken all the available local hard drive space.

There are four approaches to prevent these self-inflicted DoS attacks. First, separate disk partitions can be established for the system and application logs. This will not prevent the logs from growing but will prevent them from interfering with the operating system. Although the solution seems obvious, interestingly enough, logs default to writing to the operating system partition.

Second, logs can be set up to overwrite on a regular basis, effectively reducing the amount of log data available. This approach sounds reasonable, except that it does not take into consideration the effect of a security attack or network failure. Generally, when hardware is failing and applications are not running properly, more logging is generated. So, right when logs are the most valuable, they will contain the least span of time because of the additional logging traffic being generated.

Third, logs can be manually removed from machines on a regular basis. This works well if implemented meticulously, but the weak link is the human interaction required. What happens when resources change, other tasks become a higher priority, or someone takes a vacation? Log removal needs to be automated.

Fourth, and finally, implementing automated log removal is the best — and the most expensive — approach. Basically, a system logging server that receives all the logs is added to the network. Then, each device (e.g., server, workstation, router, and switch) is set up to push logs to the new syslog server. In addition to centralizing the log data, this approach allows for reporting across log sources and correlating log data. It also prevents the logs from potentially compromised machines from being easily "doctored" by the attacker.

A.22.1.12 A key element of ensuring that the system maintains a proper security posture is the periodic auditing of the vulnerabilities inherent in the system to ensure that new vulnerabilities are being addressed and that previously closed vulnerabilities have not resurfaced as a result of changes made to systems during normal business operations. Auditing can be done by individually scanning every asset on the system with a vulnerability management tool, or it can be done automatically by a centralized appliance that is capable of scheduled scans. Both are available from industry leaders in the field. All vulnerability management tools should be used consistently to ensure baseline security compliance.

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

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

A.22.1.13 Environmental and physical security is a keystone to any security plan, and it is critical that agencies have tools integrated into every system. The physical security system requires capabilities for alarm monitoring and reporting of critical network functions, and it is designed to handle a multitude of voltage and control alarms. The system should be used to monitor alarms or perform auxiliary voltage control functionality. The information collected should be forwarded for centralized monitoring and alarm notification with the capability of forwarding alerts to notify the appropriate personnel of the issue. The centralized system should be capable of monitoring basic alarms for dispatchers and supervisors to keep them aware of important information, which would including the following:

(1) Power failure
(2) Excessive base station transmitter voltage standing wave ratio (VSWR)
(3) Shelter door alarms
(4) Cabinet door alarms
(5) Line power failure
(6) UPS failure
(7) Generator failure
(8) Smoke detector
(9) Humidity detector
(10) HVAC failure
(11) Low generator fuel
(12) Low battery

A.22.2 The 9-1-1 centers and the communications systems that support them are critical infrastructure (CI). Therefore, it is recommended that emergency services agencies conduct annual security audits, following the guidelines of one of the references listed in Annex C. Such audits are, however, reactive in nature.

It is also recommended that emergency services agencies contract with a reputable outside expert service to conduct penetration testing. Such testing is best done annually or every 18 months. The purpose of such testing is to determine whether security procedures and controls are working against common types of cyberattacks. Without this information it is impossible to know if the preventive measures are working. A confidential report should be made and kept for senior

management of the emergency services agency to assist in long-term improvements.

A.22.4 Security-by-design is a concept in data security wherein software and hardware components and systems have been designed to inherently have security built in from the beginning, as opposed to depending upon security through add-on software, devices, or modifications to the original design.

A.23.1 Chapter 23 focuses on emergency notification systems that use cellular networks or landline telephone systems to alert the public via outdoor notification or siren alerting systems for events like tornadoes or hurricanes.

A.23.1.4 The education of the public and distribution of PASAAs need to be considered when planning or making a system improvement. The PAS should take into consideration the special needs of individuals in the community.

A.23.3 Alert systems are used to warn the public of dangers and to provide information and recommended actions to the public regarding events that can be expected to result in loss of life, endanger public health, or destroy property. These events could include, but are not limited to, tornadoes, hurricanes, floods, fire, and chemical releases.

A.23.4.1(3) Radio broadcast systems include systems identified as using public radio, private radio, television, cable, cellular, and pager technologies.

A.23.5 Reporting is an issue that varies greatly depending on the PAS solution used. A simple broadcast system could offer little to report, and a telecommunications-based system could offer the opportunity to identify specific locations or telephone lines to which a recorded message or an alert data message (ADM) was sent, as well as information that a PASAA, a telephone answering device, or a person has received the voice message or ADM.

Annex B Explanation of the Professional Qualifications Standards and Concepts of JPRs

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

B.1 Explanation of the Professional Qualifications Standards and Concepts of Job Performance Requirements (JPRs). The primary benefit of establishing national professional qualifications standards is to provide both public and private sectors with a framework of the job requirements for emergency services personnel. Other benefits include enhancement of the profession, individual as well as organizational growth and development, and standardization of practices.

NFPA professional qualifications standards identify the minimum job performance requirements (JPRs) for specific emergency services levels and positions. The standards can be used for training design and evaluation, certification, measuring and critiquing on-the-job performance, defining hiring practices, job descriptions, and setting organizational policies, procedures, and goals.

Professional qualifications standards for specific jobs are organized by major areas of responsibility defined as *duties*. For example, the firefighter's duties might include fire department communications, fireground operations, and preparedness and maintenance, whereas the fire and life safety educator's duties might include education and implementation, planning and development, and evaluation. Duties are major functional areas of responsibility within a specific job.

The professional qualifications standards are written as JPRs. JPRs describe the performance required for a specific job and are grouped according to the duties of the job. The complete list of JPRs for each duty defines what an individual must be able to do to perform and achieve that duty.

B.2 The Parts of a JPR.

B.2.1 Critical Components. The JPR comprises three critical components, which are as follows:

(1) Task to be performed, partial description using an action verb *(See Figure B.2.1 for examples of action verbs used in the creation of JPRs.)*
(2) Tools, equipment, or materials that are to be provided to complete the task
(3) Evaluation parameters and performance outcomes

Table B.2.1 gives an example of the critical components of a JPR.

B.2.1.1 The Task to Be Performed. The first component is a concise statement of what the person is required to do. A significant aspect of that phrase is the use of an action verb, which sets the expectation for what is to be accomplished.

B.2.1.2 Tools, Equipment, or Materials That Should Be Provided for Successful Completion of the Task. This component ensures that all the individuals completing the task are given the same tools, equipment, or materials when they are being evaluated. Both the individual and the evaluator should know what will be provided in order for the individual to complete the task.

B.2.1.3 Evaluation Parameters and Performance Outcomes. This component defines — for both the performer and the evaluator — how well the individual should perform each task. The JPR guides performance toward successful completion by identifying evaluation parameters and performance outcomes. This portion of the JPR promotes consistency in evaluation by reducing the variables used to gauge performance.

B.2.2 Requisite Knowledge and Skills. In addition to these three components, a JPR describes requisite knowledge and skills. As the term *requisite* suggests, these are the necessary knowledge and skills the individual should have prior to being able to perform the task. Requisite knowledge and skills are the foundation for task performance.

Table B.2.1 Example of a JPR

Component	Example
(1) Task to be performed	(1) Perform overhaul at a fire scene,
(2) Tools, equipment, or materials	(2) given PPE, attack line, hand tools, flashlight, and an assignment,
(3) Evaluation parameters and performance outcomes	(3) so that structural integrity is not compromised, all hidden fires are discovered, fire cause evidence is preserved, and the fire is extinguished.

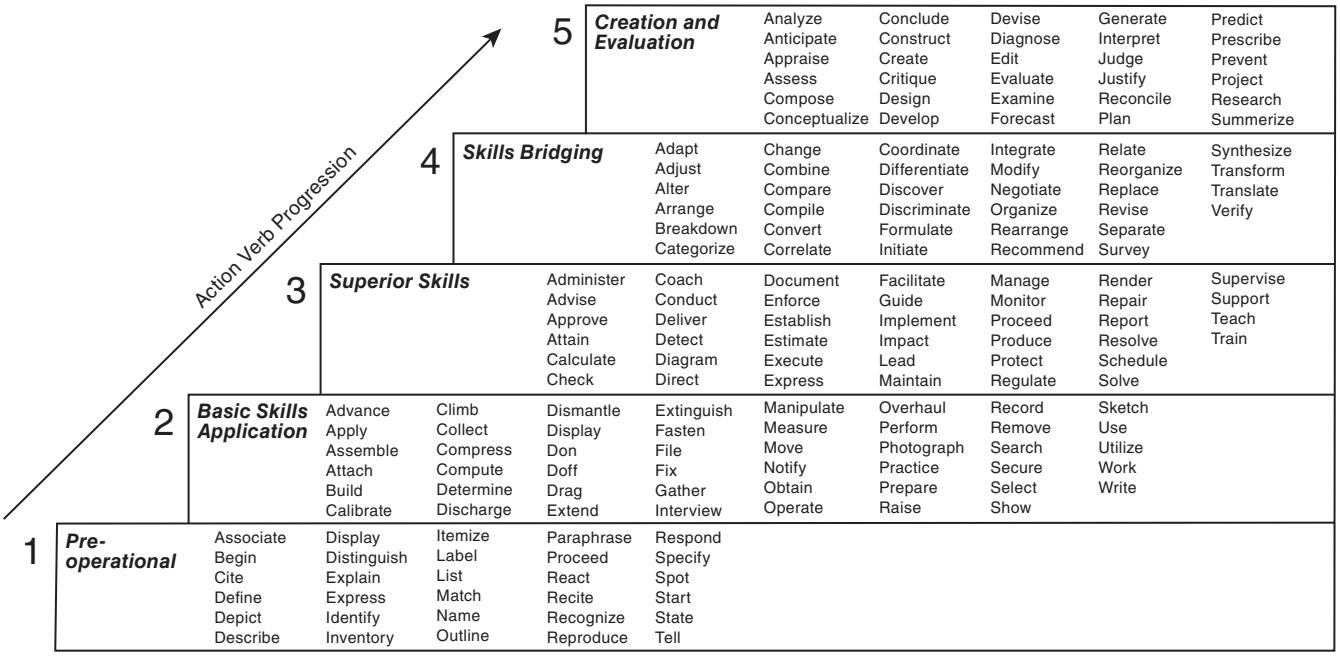


FIGURE B.2.1 Examples of Action Verbs.

B.2.3 Examples. With the components and requisites combined, a JPR might be similar to the two examples in B.2.3.1 and B.2.3.2.

B.2.3.1 Example: Firefighter I. Perform overhaul at a fire scene, given PPE, attack line, hand tools, flashlight, and an assignment, so that structural integrity is not compromised, all hidden fires are discovered, fire cause evidence is preserved, and the fire is extinguished.

(A) Requisite Knowledge. Knowledge of types of fire attack lines and water application devices for overhaul, water application methods for extinguishment that limit water damage, types of tools and methods used to expose hidden fire, dangers associated with overhaul, signs of area of origin or signs of arson, and reasons for protection of fire scene.

(B) Requisite Skills. The ability to deploy and operate an attack line; remove flooring, ceiling, and wall components to expose void spaces without compromising structural integrity; apply water for maximum effectiveness; expose and extinguish hidden fires in walls, ceilings, and subfloor spaces; recognize and preserve signs of area of origin and arson; and evaluate for complete extinguishment.

B.2.3.2 Example: Fire and Life Safety Educator II. Prepare a written budget proposal for a specific program or activity, given budgetary guidelines, program needs, and delivery expense projections, so that all guidelines are followed and the budget identifies all the program needs.

(A) Requisite Knowledge. Knowledge of budgetary process; governmental accounting procedures; federal, tribal, state, and local laws; organizational bidding process; and organization purchase requests.

(B) Requisite Skills. The ability to estimate project costs; complete budget forms; requisition/purchase orders; collect, organize, and format budgetary information; complete program budget proposal; and complete purchase requests.

B.3 Potential Uses for JPRs.

B.3.1 Certification. JPRs can be used to establish the evaluation criteria for certification at a specific job level. When used for certification, evaluation should be based on the successful completion of JPRs.

The evaluator should verify the attainment of requisite knowledge and skills prior to JPRs evaluation. Verification could be through documentation review or testing.

The individual seeking certification should be evaluated on the completion of the JPRs. The individual should perform the task and be evaluated based on the evaluation parameters and performance outcomes. This performance-based evaluation is based on practical exercises for psychomotor skills and written examinations for cognitive skills.

Psychomotor skills are those physical skills that can be demonstrated or observed. Cognitive skills cannot be observed but rather are evaluated on how an individual completes a task (process-oriented) or a task's outcome (product-oriented).

Performance evaluation requires that individuals be given the tools, equipment, or materials listed in the JPR in order to complete the task.

Table B.3.1 provides examples of how assessment methodologies can be utilized by a certifying body.