Emergency Operations Center Facility and Technology Maintenance Guide

December 2016

FEMA

Prepared Under

Contract: HFE20-14-A-0250
Task Order: HSFE20-16-J-0233.

Abstract

This document was created to assist Chemical Stockpile Emergency Preparedness Program (CSEPP) jurisdictions in cost effectively maintaining their facility and technological assets through their useful life.

This document also lists maintenance frequencies commonly used in facility management as well as provides benchmark costs.

This page intentionally left blank.

Table of Contents

1. Introduction 1

2. Scope 1

3. Background 2

3.1. Maintenance Program 2

3.2. Operating Procedures 2

3.3. Utility Contracts 3

3.4. Maintenance Contracts 3

3.5. Service Providers 4

3.6. Responsibilities 4

3.7. Summary 5

4. Program Guidance 5

5. Maintenance Program 6

6. Utilities 8

6.1. Public Utilities Commission 8

6.2. Federal Communications Commission 9

7. Facility Systems 10

7.1. Structural Systems 10
7.1.1. Foundation 10
7.1.2. Substructure 11
7.1.3. Superstructure 11

7.2. Exterior Building Systems (Building Envelope) 11
7.2.1. Exterior Walls 11
7.2.2. Roof 12
7.2.3. Roof Drainage 13

7.3. Flooring Systems 13

7.4. Electrical Systems 13
7.4.1. Grounding System 15
7.4.2. Lightning Protection System 15
7.4.3. Surge Protection Devices 15
7.4.4. Uninterruptible Power Supplies 16
7.4.5. Generators 16
7.4.6. Stored Emergency Power Supply System 17

7.5. Mechanical Systems 17

7.6. Conveying Systems **18**
7.7. Plumbing Systems **18**
7.8. Fire Protection Systems **19**
7.9. Interior Finishes **20**
7.10. Furniture, Fixtures, and Equipment **21**
7.10.1. Furniture 21
7.10.2. Fixtures 21
7.10.3. Equipment 22
7.11. Site and Landscaping Systems (Grounds) **22**
7.11.1. Hardscape 22
7.11.2. Landscaping 23
7.11.3. Planter Ground Covers 23
7.11.4. Driveways, Roads, and Parking Areas 24

8. Technology Systems **24**
8.1. Customer Premise Equipment **25**
8.1.1. Telephony 25
8.1.2. 9-1-1 Communications Systems 25
8.1.3. Cable Television 26
8.1.4. Internet 27
8.2. Local Area Network **27**
8.3. Security Systems **27**
8.3.1. Door Access Controls 28
8.3.2. Closed-circuit Television 28
8.4. Audiovisual **29**
8.5. Facility Management Computer Programs **30**
8.5.1. Computer-aided Facility Management 30
8.5.2. Computerized Maintenance Management Systems 30
8.5.3. Building Automation Systems 30
8.6. Public Safety Radio Communications **30**
8.7. Amateur Radio (HAM) **31**

9. Maintenance Frequencies **32**

10. Maintenance Budgeting and Expenditures **33**
10.1. Budgeting **33**
10.1.1. Benchmarking 33
10.1.2. Incremental 33
10.1.3. Asset-based 34
10.2. Expenditures **34**

Appendix A: Frequency **A-1**

Appendix B: National Fire Protection Association 1221 Overview **B-1**

11. NFPA 1221 ..... **B-1**

11.1. Chapter 1 – Administration **B-1**

11.2. Chapter 2 – Referenced Publications **B-1**

11.3. Chapter 3 – Definitions **B-1**

11.4. Chapter 4 – Communications Centers **B-2**
11.4.1. General B-2
11.4.2. Exposure Hazards B-2
11.4.3. Construction B-2
11.4.4. Climate Control B-3
11.4.5. Fire Protection B-4
11.4.6. Security B-4
11.4.7. Power B-5
11.4.8. Lighting B-5
11.4.9. Lightning B-6
11.4.10. Remote Communications Facilities B-6

11.5. Chapter 5 – Communication and Signal Wiring **B-6**
11.5.1. Circuit Construction and Arrangement B-6
11.5.2. Circuit Conductors B-6
11.5.3. Underground Cables B-7
11.5.4. Aerial Cable and Wire Construction B-7
11.5.5. Wiring Inside Buildings B-7
11.5.6. Circuit Protection B-8
11.5.7. Fuses B-8
11.5.8. Grounding B-9
11.5.9. Access B-9
11.5.10. Pathway Survivability B-9

11.6. Chapter 6 – Emergency Response Facilities **B-9**
11.6.1. General B-9
11.6.2. Commercial Telephone B-10
11.6.3. Fire Protection B-10
11.6.4. Power and Lighting B-10
11.6.5. Communications Conductors B-10

11.7. Chapter 7 – Operations **B-10**
11.7.1. Management B-10
11.7.2. Telecommunicator Qualifications and Training B-11
11.7.3. Staffing B-11
11.7.4. Operating Procedures B-12
11.7.5. Time B-13
11.7.6. Recording B-13
11.7.7. Quality Assurance B-14

11.8. Chapter 8 – Telephones B-14
11.8.1. Universal Emergency Number 9-1-1 Service B-14
11.8.2. Published Emergency Number Alternative Routing B-15
11.8.3. Multiple Line Telephone Systems (MLTS) B-15

11.9. Chapter 9 – Dispatching Systems B-15

11.10. Chapter 10 – Computer-Aided Dispatching (CAD) Systems B-16

11.11. Chapter 11 – Testing B-18
11.11.1. Acceptance Testing B-18
11.11.2. Operational Testing B-18
11.11.3. Power B-20

11.12. Chapter 12 – Records B-20
11.12.1. Installation B-20
11.12.2. Training Records B-20
11.12.3. Operational Records B-20
11.12.4. Maintenance Records B-21
11.12.5. Retention of Records B-21

11.13. Chapter 13 – Data Security B-21

11.14. Chapter 14 – Public Alerting Systems B-22

11.15. Annexes B-23

1. Introduction

The Chemical Stockpile Emergency Preparedness Program (CSEPP) was initiated in 1985 when the United States Congress passed a law directing the Army to dispose of its aging chemical weapons inventory. The disposal process was to be completed with the public's safety being paramount.

CSEPP has funded the construction, renovation, or relocation of Emergency Operations Centers (EOCs) in participating states and local jurisdictions. Facility upgrades were made to better equip participating jurisdictions with the ability to serve their citizens during a time of disaster, thus providing increased levels of public safety and awareness.

With the addition of more building square footage, property, and facility systems comes increasing costs and labor to manage each. The CSEPP jurisdictions are tasked to oversee the execution of the proper management of the new assets.

The Federal Emergency Management Agency (FEMA) developed this guide to identify and support the maintenance requirements for the newly installed technologies of these critical emergency facilities.

Proper maintenance of the facility and its systems will add years to their usable lives. Neglecting system maintenance will result in shortening a system's life, increasing overall operational costs, and causing unwanted downtime. Each system should be ready for use when its function is required. If a system fails to function correctly, it can affect other systems and may ultimately cause disaster.

Primary facility systems and their maintenance, frequency, and costs will be discussed in this document.

The primary purpose of facility and site maintenance for each EOC is to enable the respective site owner to identify and correct deficiencies in the early stages so that unnecessary system downtime is not experienced.

2. Scope

This document addresses the maintenance of existing facilities, building systems, and associated technological equipment through the close-out process of CSEPP.

The technological systems installed in each facility are complex state-of-the-art systems. Additionally, the hardware for these systems varies in manufacturer from one entity to the next, making maintenance even more difficult.

A facility and technology maintenance plan will greatly enhance an asset's reliability and life and help control maintenance costs.

- Maintenance personnel would focus on individual scheduled tasks and not be overwhelmed by the total maintenance plan.

- The cost of maintaining spare pieces of equipment and replacement parts would be reduced.

3. Background

3.1. Maintenance Program

A maintenance program should be developed and executed that will ensure, on a scheduled basis, every facility, facility system, and piece of technological equipment is maintained in a state of readiness.

A maintenance program should, at a minimum, address the following:

- Defined preventive maintenance schedule
- Defined checks and tests that will be conducted during the scheduled preventive maintenance visit
  - Written check/testing procedures for all fixed, mobile, and portable technological equipment to include facility systems; that is, back-up power sources, electrical systems, lightning protection, grounding, other facility systems
- Defined outage reporting and responses
  - Critical outage and failures requiring an immediate response in a defined response time
  - Routine outage requiring a less than immediate response also in a defined time
  - Defined time to place equipment back in service after a routine or critical outage
- Ensures technical manuals are available for each piece of equipment in service
  - Master disk and copies on file at the respective EOC
  - Multiple work copies for EOC in each location
- Routine inspection and maintenance of all remote EOC facilities, to include, but not be limited to, back-up EOCs, storage facilities, and others that are controlled or owned by the jurisdiction(s)

Where financially viable, contracts should be considered for maintenance of the building systems, to include, but not be limited to, radio systems, telephones, televisions, lawn and grounds care, and others. Contracts should be procured from utility service providers, to include, but not be limited to, telephones, electrical, sewer, water, and others.

3.2. Operating Procedures

Operating procedures are a large portion of a facilities maintenance program, providing detail on how a system shall function and how to deal with a system deficiency. International Organization of Standards (ISO) 9001, *Quality Management Systems – Requirements*, is one example.

Operating procedures should be developed as guidance for personnel to have knowledge of the facility systems. Operation and maintenance manuals for each facility system and technological equipment should be properly catalogued and stored for ready use by qualified personnel. Standard operating procedures (SOPs) should be developed stating each system's routine procedures and steps to correct deficiencies.

Each jurisdiction should have written procedures and radio system programming that will allow seamless interoperability with adjacent jurisdictions and higher levels of government.

Testing of all interoperability channels should take place each month and be witnessed by a technology-qualified observer. All test results should be documented and reviewed by the jurisdiction with a sign-off signature by the responsible party. The testing will ensure that fixed communication, mobile, and portable equipment is tested and/or exercised.

3.3. Utility Contracts

Utility contracts should be, when possible, negotiated for best quality at the best price. Utilities include, but are not limited to, the following:

- Electric
- Gas
- Petroleum-based fuels
- Telephone
- Customer premise equipment (CPE)
- Television/Cable

3.4. Maintenance Contracts

Maintenance contracts are contracts that should be put out for bid, unless a sole source provider is required, or at least be properly negotiated. Specific requirements of service quality, reaction times, and frequency of maintenance should be stated. Typical maintenance contracts include, but are not limited to, the following:

- Heating, ventilation, and air conditioning (HVAC)
- Custodial
- Pest control
- Waste disposal
- Grounds
- Roofing
- Uninterruptible power supply (UPS)
- Generator
- Security access system

- Closed-circuit television (CCTV)
- Fire suppression system for main building
- Fire suppression system for information technology (IT) areas
- Fire extinguisher recertification
- Telephone
- CPE
- Network

3.5. Service Providers

It is important to know who is working in your facility and on your equipment. Service providers for facility and technology systems are often, but not necessarily, the same as the system maintenance providers. Some attributes that should be required of service and maintenance providers are listed below.

- Maintenance providers should have good working knowledge and preferably history on the type of system.
- Maintenance providers should perform all work by governing standards and those imposed by the owner.
- Worksite safety must be adhered to.
- Maintenance providers should attend a safety training class, as proposed by the owner.
- Response for service should be timely, as defined by the owner.
- Labor and part pricing and billing should be consistent and within the area's average rates.
- Maintenance providers must have security clearances, as proposed by the owner.
- Work must be performed neatly in a workman-like manner.
- Debris and waste should be properly removed from the site and disposed of per federal, state, and local regulations.
- Damaged parts or equipment should be verified by the owner and disposed or stored per the owner's request.
- Inspections, maintenance, replacement, repair, etc. of the system or equipment should be recorded, dated, verified for accuracy, and signed-off by the owner or owner's representative.

3.6. Responsibilities

The respective EOC facility owner/operator is responsible for providing staff to operate the EOC and provide daily maintenance such as cleaning and operating buildings, cutting grass, removing building waste, and all other day-to-day basic requirements.

- The owner may have taken on new responsibilities with the appointment as the facility manager or at least overseeing facility management.
- The facility manager should walk the property daily and be observant of any changes.
- The facility manager has some inherent tools to accomplish their task. They are the five senses: seeing, hearing, smelling, tasting, and touching. These senses give the owner the powerful tool of observance. Generally, the owner is familiar with the day-to-day tasks and functionality of the facility and its systems and will notice changes. For example, a mild burning odor of plastic or tar is smelled; this may be an indicator that a light's ballast is malfunctioning.
- The facility manager will procure and oversee the systems, equipment, and maintenance contracts and service.
- The facility manager will oversee training on the systems and equipment.
- The facility manager will manage and oversee or at least be a steward of the facility and equipment budgets.

At the end of the facility and technology systems' respective life cycles, upgrades to the systems are anticipated. With proper maintenance, the systems should provide quality service throughout their life.

3.7. Summary

The above is an attempt to define the minimum level of support required to continue to maintain the systems as reliable and available systems plus meet what is anticipated as additional need that is yet to be defined.

4. Program Guidance

The following guidance is relevant to the operations and maintenance of EOCs and other emergency facilities:

- *NIOSH Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks*
- *American Society for Testing Materials E2668 – 10 Standard Guide for Emergency Operations Center (EOC) Development*
- *FEMA Emergency Operations Center Assessment Checklist –* https://www.fema.gov/emergency-operations-center-assessment-checklist
- *FEMA 361– Design and Construction Guidance for Community Shelters*
- *FEMA 452 – A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings*, January 2005
- *IAEM Response Capability Multi-Agency Coordination (EOC Management) Guide* (Draft, 2009)
- *Motorola R56 – Standards and Guidelines for Communication Sites*

- *NFPA 90A – Standard for the Installation of Air Conditioning and Ventilating Systems*
- *NFPA 90B – Standard for the Installation of Warm Air Heating and Air Conditioning Systems*
- *NFPA 110 – Standard for Emergency and Standby Power Systems*
- *NFPA 220 – Standard on Types of Building Construction*
- *NFPA 1221 – Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*
- *NFPA 1561 – Standard on Emergency Services Incident Management System*
- *NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs*
- *NFPA 5000 – Building Construction and Safety Code*
- *National Response Framework State and Local Partner Guides*
- *Unified Facilities Criteria (UFC) 4-141-04 – Department of Defense Emergency Operations Center Planning and Design*
- *Unified Facilities Criteria (UFC) 4-010-01– Department of Defense Minimum Antiterrorism Standards for Buildings*[1]

The standards listed above reference other standards to support their publication. Throughout this document other standards may be mentioned or quoted. These standards work hand-in-hand to accomplish the common goal of providing best practices for the EOCs and communications centers.

5. Maintenance Program

Maintenance and inspections are necessary to ensure that EOC facilities and associated systems and technological systems will operate properly throughout their design lifetime. The amount of maintenance that is likely to be required over the system design life is an important factor in determining system life-cycle costs and should be an important consideration. To minimize the total life-cycle cost, a suitable preventive maintenance program must be developed, and the program and its associated costs (e.g., training and required spare parts) included as an integral part of the maintenance and inspection evaluation process. Thus, such items as guaranteed minimum time for availability of spare parts, specification of backward compatible components and software design, initial and follow-up training, and operating and maintenance experiences with similar systems should be included in the maintenance and inspection process so that life-cycle costs can be determined and appropriate long-term resource requirements understood and budgeted.

[1] http://www.fema.gov/media-library-data/20130726-1903-25045-3905/csepp_program_guidance_december_2012.pdf

A regularly scheduled preventative maintenance program will provide the owner a historical facility and equipment performance baseline that can be referenced on an ongoing basis.

Maintenance should address all components in the EOC and associated systems and reflect the system testing methods described herein. The maintenance program should encompass minor adjustments, and the repair and replacement of components based on predetermined performance criteria, which are based on the relevant component design requirements.

Suitable EOC maintenance also needs to be provided for testing, activation, and control components to ensure that EOC facilities and associated systems will perform reliably when needed. Electronic components need to operate within tight limits to ensure that the integrity of all associated electronic systems is maintained. As an example, relatively minor degradation in complex communications and power systems can have significant negative effects on EOC reliability and area coverage.

There are typically three types of maintenance: corrective (reactive), preventative, and predictive. Other subpart maintenance groups may be zero-hour and periodic (time-based).

- **Corrective maintenance** is due to a system failure. It has not been planned and becomes the greatest cost maintenance.
    - In EOCs, relying on this type of maintenance can cause a chain-reaction of multiple system failures. These failures can cause downtime in communications systems that could result in loss of life, structure, or equipment. These results can negatively impact an agency's budget, personnel, reputation, regulatory compliance, and safety.
- **Preventative maintenance** is when systems are maintained at periodic intervals per manufacturer's or owner's specifications. This has been determined to be the least costly for critical systems.
    - Some preventative maintenance tasks can be as simple as observing a system for proper functionality.
    - Preventative maintenance at an EOC will increase system and equipment runtime and help to eliminate unscheduled downtime. It will assist the owner in scheduling needed system outages for repairs and/or upgrades.
- **Predictive maintenance** is when monitoring of the degradation of equipment and historic analysis are used to determine proper maintenance of a system.
    - Predictive and preventative maintenance work hand-in-hand. The results from predictive maintenance can be used to intelligently determine a system's preventative maintenance frequency. Many times frequencies can be lessened; therefore, saving costs with no degradation of the system's life cycle. Performing regularly scheduled preventative maintenance ultimately adds system

functionality historical data. This data should be reviewed to see if maintenance frequencies are accurate.

- Preventative system maintenance should be used to regularly schedule monitoring the systems with technology; thus predictive maintenance. Examples of predictive maintenance include, but are not limited to, vibration and oil analysis, infrared scanning, leak detection, power quality metering, and using a building management database system.

- **Zero-hour maintenance** is determining the time in which a system should be completely overhauled. This overhaul is complete, making the system or equipment like-new.
  - Realistically zero-hour maintenance in an EOC may be impractical. The cost for a complete overhaul may be greater than retiring the old and purchasing new.
- **Periodic** or time-based **maintenance** is when preventative maintenance is performed by the operator of the system or equipment. Typically, there is no system downtime.
  - Preventative maintenance tasks generally are elementary or operator task-driven. For example, within an emergency services communications facility, National Fire Protection Association (NFPA) 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, states that all primary and secondary radio and voice amplification circuits shall be voice tested twice daily. This is a typical preventative maintenance inspection performed by the operator.

6. Utilities

Public utilities include, but are not limited to, electric, gas, water, sewage, waste, telephone, television, and internet. Utility companies may be privately owned or run by the local municipalities. Electric, gas, telephone, television, and internet are normally privately owned companies. Water, sewage, and waste may be privately owned or owned by the municipality.

6.1. Public Utilities Commission

Utility companies may be allowed some monopoly rights due to the areas and coverage needed for public welfare. State Public Utility Commissions (PUCs) regulate the rates and services of some utility providers.

The following are some of the areas for which PUCs typically have regulatory responsibility:

1. Rate increase or reduction
2. Expansion or reduction of utility service boundaries
3. Construction and operation of utility facilities
4. Meter accuracy
5. Operating conditions of a utility

6. Management audits
7. Valuation of utility property
8. Natural gas and coal purchasing practices
9. Issuance or assumption of securities by a utility
10. Consumer complaints
11. Compliance with service and safety regulations

6.2. Federal Communications Commission

The Federal Communications Commission (FCC) regulates radio, television, wire, satellite, and cable.

The Federal Communications Commission regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation. In its work facing economic opportunities and challenges associated with rapidly evolving advances in global communications, the agency capitalizes on its competencies in:

- *Promoting competition, innovation and investment in broadband services and facilities*
- *Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution*
- *Encouraging the highest and best use of spectrum domestically and internationally*
- *Revising media regulations so that new technologies flourish alongside diversity and localism*
- *Providing leadership in strengthening the defense of the nation's communications infrastructure*[2]

In most cases, the owner has no choice on what utility will provide service for those utilities regulated by their state PUC. Some states allow the consumer to shop for electric and gas. Those utilities regulated by the FCC are generally shop-able by the consumer; although somewhat restrictive by region.

When possible, utilities that can be run to the facility through fiber should be pursued. This will assist prohibiting entrance of unwanted anomalies, like lightning, from entering the facility.

[2] https://www.fcc.gov/about-fcc/what-we-do

7. Facility Systems

There are numerous systems within a facility. Each must have maintenance performed in order to remain a quality system. Major facility systems are discussed below.

7.1. Structural Systems

The building's structural system consists of the foundation, substructure, and superstructure.

A list of construction requirements per NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* is noted below.[3]

- Communications center shall be located in buildings of Type 1 or Type 2 construction as defined by NFPA 220, *Standard on Types of Building Construction.*
- The lowest floor elevation of a communications center shall be above the 100-year flood plan.
- When the building that houses the communications center is located within 150 feet of the potential collapse zone of a taller structure, the roof shall be designed to resist damage from collapse of the exposing structure.
- Communications centers shall not be constructed below grade unless the lowest floor in the facility is above the 500-year flood plan. Communications centers constructed below grade shall comply with NFPA 101, *Life Safety Code*®, Section 11.7.3 and be specifically designed for the location.
- When the communications centers are housed within buildings with others that have non-emergency communication functions, they shall be divided by fire barriers having a 2-hour fire resistance rating.
- Fire barriers shall comply with NFPA 101, Section 8.2.

7.1.1. Foundation

The foundation is the building system installed to attach the building to the earth and distribute the building load from the structure to the ground. The foundation may consist of pad stones, piers, or poured concrete footers and walls.

Two major concerns for foundation design are soil settlement and load-bearing capacity. The soil beneath the foundation must be conditioned to accept the foundation. This may be achieved by replacement, compaction, and going deeper into the soil.

Foundations are the primary and first system of which a building is constructed. Proper maintenance should be conducted to provide longevity of the foundation. The maintenance should consist of pest control, removal of unwanted vegetation, and proper drainage.

[3] http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=1221

7.1.2. Substructure

The substructure is basically the areas beneath the earth resting on top of the foundation. Typically, these are basements and crawl spaces.

Substructure walls need to be properly sealed to prevent moisture from entering the below-grade space. Unwanted moisture is a breeding ground for mold, mildew, and other unhealthy environmental issues.

Maintenance of the substructure starts with proper installation. Substructures should be regularly examined for signs of moisture and deterioration.

7.1.3. Superstructure

The superstructure is the part of the building projecting above the earth. It consists of the building envelope and flooring, and houses systems within the facility.

7.2. Exterior Building Systems (Building Envelope)

The building envelope consists of two primary systems: exterior walls and roof. Their main functions are to keep the weather out, the cooling and heating in, support and house other building systems, control noise, and transfer environmental wind loads to the building infrastructure.

7.2.1. Exterior Walls

Exterior wall functions are for aesthetics, to keep the weather out, and control the climate in the interior. The exterior walls consist of decorative weather-resistant exterior material, sealants, insulation, and interior wall material. The exterior wall may be structurally supporting or a curtain wall.

Structural supporting walls are load-bearing walls that function as support for the roofing system. These include, but are not limited to, cement block, decorative block, and insulated concrete form (ICF) walls. Cement block and ICF walls are often covered with a decorative wall cladding of stone, stucco, brick, steel, cement board, vinyl, timber, or aluminum. These types of structural supporting walls can be rated building construction Type 1 or Type 2 fire-resistant and will withstand high winds. ICF walls need the proper wall cladding applied to be rated Type 1 and Type 2. As noted above, NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, states that communication centers shall be located in buildings constructed Type 1 or Type 2 as defined by NFPA 220, *Standard on Types of Building Construction*.

Curtain walls are wall sections of glass and manufactured fire-resistant Type 1 or Type 2 wall panels inserted between structurally supporting steel or masonry columns and beams. Per NFPA 1221, in communication centers, direct exterior glass windows, exposing personnel, shall be rated Level 4 bullet-resistant.

Proper maintenance should be performed to the exterior wall surfaces so they can maintain their aesthetics and perform their function of resisting the elements and providing safety for personnel and equipment.

7.2.2. Roof

The roof is supported by the infrastructure: exterior and interior supporting walls, columns, beams, and trusses.

The roof horizontal surface is generally made up of three major elements: decking, insulation, and waterproofing membrane. The roof waterproofing membrane in commercial buildings, due to their gently sloping nature, is usually either bituminous or single-ply.

In order to drain properly, the industry standard for the flat, gently sloped roof is between 0.25-inch and 2-inches per foot. In some special cases, 0.125-inch per foot is allowed on aggregate-surfaced coal-tar roofs.

Build-up roofing (BUR) and polymer-modified bitumen sheet membrane (MB) are two types of bitumen roofing often used in the industry today. The roof surface resists hail and light foot traffic. Well-maintained BUR will last approximately 20–30 years. If local codes allow, they may be re-covered with a second bituminous roof. Top coatings may be applied to lengthen the life and provide reflectance and ultraviolet (UV) protection.

Single-ply roofing typically has two classes: thermoset and thermoplastic membranes.

Thermoset roofing consists of ethylene propylene diene monomer (EPDM) and Hypalon membranes. EPDM uses carbon black to block-out UV and is a rubber-like material. The warrantied life of EPDM material is 40 years, although the expected life is 22–35 years due to seam failure. EPDM recoating has not been perfected. Hypalon can be recoated and should be between 15–20 years.

Thermoplastic membrane roofing is generally thermoplastic polyolefin (TPO) or polyvinyl chloride (PVC) materials. The commercial roof material warranty for both is 25 years. TPO's expected life is between 22–30 years and PVC is 30 plus years. Neither material is easy to topcoat.

The most critical component for single-ply roofing is the installation method. Proper overlapping of the seams is very important. Delamination of the seams and roofing material loosening from the substrate are two of the biggest contributors to roof leaks. Single-ply roofing can be mechanically attached or fully adhered. Mechanical attachment is the best method to hold-up during high winds and requires no extra ballast weight. Fully adhered, glued to substrate is susceptible to delamination due to condensation beneath the membrane.

EPDM is the least expensive single-ply roof. No special tooling is required to install the roof. It is susceptible to damage from various chemical products. Petroleum-based sealants must not be used on EPDM roofs.

The facility manager should perform regular roof maintenance to assure damage to persons and property located internally is avoided. Proper roof maintenance will help to maintain roof warranties.

7.2.3. Roof Drainage

Generally, on larger flat or slightly sloped roofs, the roof drainage is sloped to roof drains centralized on the roof and channeled to vertical piping within the building framework.

Most codes require two means of roof drainage: normal roof drains and emergency overflow drainage. The overflow drainage can be day-lighted at the roof level with through-wall scupper drains. This drainage may also be installed as parallel higher-mounted roof top drains that attach to the same down pipe at a lower level within the interior structure.

Regular maintenance is needed to remove debris or obstructions from the roof drain inlets. The inlet covers (strainers) must be checked for proper placement and attachment. If drainage is blocked, it will cause stress and undo load to the roof and substructure. The likelihood of roof leakage will increase.

Maintenance of the roof drainage does not stop at the top; it must be maintained until it discharges. Gutters, downspouts, property storm drains, French drains, retention ponds, and others must be cleared of unwanted debris to prohibit blockages.

7.3. Flooring Systems

The flooring system is the horizontal surface attached to the exterior walls or resting upon them. The flooring provides support for exterior and interior walls, personnel, furnishings, and other building systems. The flooring system provides safety for personnel and equipment, as a ceiling, to the floor below.

Precast concrete panels, cast-in-place concrete, steel deck and concrete, wood beam and planking, and concrete slab on-grade are types of flooring systems. The flooring system is considered one-way when the floor load is distributed on two opposite sides (e.g., precast concrete panel and joist slab). A two-way floor system is supported by all four sides (e.g., slabs and waffle slabs).

Flooring systems need to be maintained to keep their integrity. Penetration through flooring shall be per manufacturer’s specifications. Fire stopping around a penetration shall be installed per NFPA standards and building codes.

7.4. Electrical Systems

Electricity is supplied to the facility through a process of generation, transmission, and distribution on what we know as the power grid. The power grid is a network of electrical

power generation suppliers putting power onto a network of high-voltage transmission lines, which are distributed to the consumer by their local utility provider.

The facility electrical system is a complex system with many components; thus, numerous connections that are each susceptible to failure. Component failure comes from, but are not limited to, moisture, chemical corrosion, dirt, improper installation, use of dissimilar metals, loose connections, lightning strikes, not being properly exercised, and age.

Major components that will require maintenance include the following:

- Service entrance wiring
- Transformers
- Main panel board
- Grounding
- Lightning protection system (LPS)
- Subpanels
- Raceways
- Devices
- Surge protection devices (SPDs)
- Breakers
- Disconnects
- Fuses
- UPS
- Generators
- Transfer switches
- Lighting systems
- Motor control centers
- Ground fault circuit interrupters
- Contactors and relays

One of the best and evasive maintenance tools for electrical components is thermal imaging. Using a thermal imager to check for loose and corroded connections within electrical components will help in planning a timely repair of the affected equipment.

Major electrical subsystems are discussed in the subsections that follow.

7.4.1. Grounding System

A single-point grounding system is required by NFPA 70, *National Electrical Code®*. NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* requires that the communications center critical equipment be bonded to the single-point facility ground system in accordance with NFPA 70, Article 647.

Motorola R56®, *Standards and Guidelines for Communication Sites*, dated September 1, 2005, has been used heavily as the grounding guide for CSEPP projects.

7.4.2. Lightning Protection System

The LPS is an insurance policy for the safety of the building and personnel and equipment housed within. Lightning protection has a one-time initial cost and a low maintenance cost throughout its life.

The LPS shall ground properly to the facility grounding system.

The LPS is to be inspected and certified after installation and re-certified after addition or removal of components and every three years by a certified designer inspector for LPS. Interim annual inspections by a facility manager or designated personnel shall be performed to assure system component integrity.

For every thunderstorm or electrical disturbance, a qualified technical person must inspect every surge protector in the system for damage and/or blown fuses.

7.4.3. Surge Protection Devices

SPDs shall be installed on alternating current (AC) power distribution panels. Communications centers' critical equipment panels shall have a Motorola type 1 SPD, a hybrid SPD using silicon avalanche diode (SAD) and metallic oxide varistor (MOV) technology. Only normal mode SPDs shall be used on AC panels and equipment.

SPDs shall be installed on all AC power, telephone, data, and communication cabling entry points after entering the building. The SPDs shall be properly grounded to the facility's single-point grounding system.

Motorola R56® type 3 SPDs shall be installed at all AC power, and secondary SPDs on the telephone, data, and communication cabling at every communications center operator's station. The SPDs shall be properly grounded to the building single-point ground system.

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* requires SPDs to be installed per NFPA 70, *National Electrical Code®,* Article 280 and SPDs on critical equipment per Article 285.

7.4.4. Uninterruptible Power Supplies

A UPS will provide almost instantaneous power to critical equipment during a main utility power outage. The UPS provides stored power to the loads through batteries. The battery's direct current (DC) is converted to AC through a power inverter.

The runtime for a UPS, until battery depletion, is relatively short; normally 15–30 minutes. This is enough time for the standby generator to supply emergency power to the building's critical systems and others.

The UPS is a critical electrical component and requires specific maintenance. The area where a UPS is located must maintain manufacturer-specific ambient temperature settings; typically, 68–77 degrees (°) Fahrenheit (F). Temperatures greater will diminish the life of the batteries. A rule-of-thumb is for every 15° above 77° F, the battery life will be reduced by 50 percent.

Another factor that affects battery life is cycling frequency. Each discharge and length of discharge, then recharge of the battery is a cycle. The more the battery cycles, the less capacity is left in the battery. A UPS battery normally lasts 3–5 years.

Maintenance to be performed on a UPS includes, but is not limited to, the following:

- Keeping the UPS free of dust; change or clean filters
- Keeping the UPS in a conditioned environment
- Keeping all connections tight; a thermal image camera can help detect loose connections
- Retightening electrical connections annually
- Checking battery voltage for bad cells
- Visually checking battery casings for bulging

Good records should be kept of all service and maintenance performed.

7.4.5. Generators

Generators are backup power when the utility power is lost. The size of the generator is determined by the kilowatt load of the equipment determined critical to function during a utility power outage.

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* requires two independent power sources be installed at the communications center. The utility is the primary source and a permanently mounted generator (standby) is the secondary. With the loss of utility power, the generator shall automatically pick up the load within 10 seconds. A hook-up for a trailer-mounted mobile unit should be installed as a redundant backup plan.

Generators shall be operated, tested, and inspected per specifications stated in NFPA 110, *Emergency and Standby Power Systems*.

7.4.6. Stored Emergency Power Supply System

NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*, is the governing standard for a stored emergency power supply system (SEPSS). A SEPSS may consist of either a rectifier plant, UPS, generator powered by a stored electrical energy source, or a combination thereof, up to and including conductors, terminations, supervisory equipment, and load transfer equipment.

The type of SEPSS to be used is determined by the maximum time, in seconds, that the load may be without power.

7.5. Mechanical Systems

HVAC systems consist of heating, ventilation, cooling, humidification, dehumidification, air filtration, and life-safety smoke isolating or removal systems. HVAC systems are complex and have many moveable parts, which creates maintenance issues.

HVAC systems are environmental systems for the safety, good indoor air quality (IAQ), and comfort of personnel and critical equipment within a facility. The system design is based on the building size, purpose, personnel, equipment, initial cost, continual finance availability, and expected equipment life.

HVAC components that require maintenance include, but are not limited to, the following:

- Evaporator
- Condenser
- Fan
- Pumps
- Filters
- Belts
- Controls
- Valves
- Boilers
- Chillers
- Ductwork
- Piping
- Refrigerant
- Insulating materials
- Grilles and vents
- Pumps
- Heat exchangers

- Variable air volume (VAV) boxes

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, requires HVAC systems designed to maintain temperature and relative humidity within limits specified by the equipment manufacturers. It also requires backup systems for operation rooms and other spaces housing electronic equipment determined to be essential to the operation of the communications center.

7.6. Conveying Systems

Conveying systems are used to transport personnel and equipment in a facility, and include elevators and escalators. Elevators especially assist handicapped individuals in moving throughout multi-story facilities.

These systems must meet code requirements for their performance. It is recommended that testing be performed per American Society of Mechanical Engineers (ASME) A17.1, *Safety Code for Elevators and Escalators*, Sections 8.10 and 8.11. A one-year inspection and test and five-year (full load) inspection and test shall be minimally performed.

Elevator interiors and shafts are an extension of multiple systems that require regular maintenance. These systems include, but are not limited to, electrical, mechanical, interior, and fire. Elevator interiors need to be properly cleaned and sanitized, lighted, alarmed, ventilated, and have communications to the exterior.

7.7. Plumbing Systems

Plumbing systems consist of, but are not limited to, cold and hot potable water lines, non-potable process water lines, fire systems, fuel supplies, waste water disposal, and storm water disposal. Like the HVAC system, the plumbing system is a complex network of equipment closely linked in process to complete its function.

The functionality of the plumbing systems directly relates to proper maintenance. Leaks or clogs in plumbing systems can cause destruction to property and health issues to personnel. The cost of not fixing a leak or clog is generally greater than the repair.

Plumbing components that require maintenance include, but are not limited to, the following:

- Valves
- Backflow preventers
- Check valves
- Piping
- Metering devices (gauges)
- Controls
- Appliances (fixtures)

- Vents
- Heaters
- Insulation
- Pumps
- Traps
- Waste treatment equipment
- Water treatment equipment

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, requires a toilet facility and lunch area that are directly accessible for personnel in the communications center. Backup sanitation facilities and drinkable water supply shall be provided for personnel during extended periods of failure to public water or sewage systems.

7.8. Fire Protection Systems

A fire protection system involves the mechanical, plumbing, electrical, door access, and security systems of a facility. The purpose of a fire protection system is to protect the building, personnel, and equipment housed within the facility. A fire protection system includes the fire alarm system, suppressing the fire, and providing evacuation for personnel.

A fire alarm system's major components are detectors, annunciators, controllers, and wiring. These components need to be tested and maintained.

Fire suppression system components that require maintenance include, but are not limited to, the following:

- Piping
- Controls
- Pumps
- Air compressors
- Fire extinguishers
- Chemical systems
- Valves
- Mechanical water flow alarm
- Sprinklers
- Backflow preventers
- Check valves
- Metering devices (gauges)

- Strainers
- Hoses
- Flapper valves
- Status indicators

An evacuation plan shall be provided for the facility. NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* states that there shall be a management approved, written, dated, and annually tested emergency fire plan that is part of the Comprehensive Emergency Management Plan (CEMP).

Proper evacuation would involve door access controls, smoke- or fire-activated self-closing door hardware, and panic hardware. Fire exit routes shall be properly lighted and clear of obstructions. This involves the proper removal of snow and ice at fire exits.

NFPA 1221 states fire extinguishers are required as per NFPA 10, *Standard for Portable Fire Extinguishers*. An automatic fire detection, alarm, and notification system is required per NFPA 72, *National Fire Alarm and Signaling Code*. The building that houses a communications center shall be protected by an approved, supervised automatic sprinkler system that complies with NFPA 13, *Standard for the Installation of Sprinkler Systems*.

Fire protection systems need to be inspected and require maintenance by certified personnel. The facility manager should consult the NFPA standards for the type(s) of fire suppression systems in the facility. The standards will state the frequency of testing and inspections required. For example, NFPA 10 states fire extinguishers shall be manually inspected at least every 31 days by the facility manager or designated personnel and, for most types of extinguishers, annual external and internal maintenance, by certified personnel.

7.9. Interior Finishes

Interior finishes include, but are not limited to, wall, ceiling, floor, door, and window treatments. The quality, style, and physical abuse of the finish will determine its expected life. Never-the-less, maintenance must be performed regularly to keep the finishes clean and properly attached to their substrates.

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems,* states that the exposed walls and ceilings shall have a flame-resistance index of 25 or less and a smoke development index of 50 or less. Interior floors shall comply with the requirements of NFPA 101, *Life Safety Code*®; they shall be Class 1 as established by NFPA 101.

Communications centers, data rooms, and other critical areas require specific electrostatic dissipative (ESD) flooring. The flooring used in these areas shall meet a resistance value between 1x10e6 and 1x10e9 ohm. The flooring must be properly grounded to the facility

single-point ground system. This type of flooring system was established to dissipate static electrical charges that could harm personnel and critical equipment.

7.10. Furniture, Fixtures, and Equipment

Furniture, fixtures, and equipment (FF&E) used within facilities widely depends on the organization's budget, function, and style. FF&E are movable or removable parts with no permanent attachment to the structure and depreciate quickly; they play a large role when it comes to budgeting and maintenance.

7.10.1. Furniture

When purchasing furniture, the owner must consider quality, functionality, and cost. Quality may come with a higher price tag, although the owner should especially consider the warranty. Some furniture manufacturers offer a lifetime warranty on the mechanical functions of the furniture. The facility manager must be aware of the warranties. A great deal of money can be spent on new furniture when the old could be repaired, as new, for just the labor cost.

Today furniture is made with ergonomics in mind. Attention to the style of furniture for the proper workplace ergonomics is a must. A great deal of lost downtime and personnel absence can be avoided by procuring the correct furnishing for the tasked work.

Per Motorola R56®, *Standards and Guidelines for Communication Sites*, communications centers, data rooms, and other critical areas require metallic furniture to be properly grounded to the building single-point ground system. This excludes chairs, although the chairs should be ESD protective and have a resistance to ground between 1x10e5 and 1x10e9 ohm. The chairs are designed to work in conjunction with the ESD flooring. The purpose of the grounding is to eliminate the effects of electrical disturbances from external and internal sources such as lightning, AC power disturbances, or electrostatic discharge.

7.10.2. Fixtures

Fixtures are those items that may need utilities to function or are attached to the building after construction. Bathroom appliances and partitioning, towel dispensers, enclosed automatic teller machines (ATMs), kitchen appliances and cabinetry, and window treatments are considered fixtures.

Fixtures require maintenance and constant upkeep. For example, towel dispensers need to be cleaned, refilled, batteries changed, and fixed.

Per Motorola R56®, *Standards and Guidelines for Communication Sites*, communications centers, data rooms, and other critical areas require metallic fixtures to be properly grounded to the building single-point ground system. The purpose for grounding is as mentioned previously.

7.10.3. Equipment

The equipment in FF&E refers to equipment needed by personnel to perform their tasked work. Phones, faxes, computers, radio equipment, monitors, and smart boards are some examples.

The equipment, like fixtures, requires maintenance and upkeep. In a communications center, a large quantity of the equipment is specialized. The equipment will need to be maintained and serviced by qualified personnel. The facility manager will need to procure agreements, leases, or contracts from vendors for the equipment maintenance; cost is a consideration. The facility manager should ensure care is taken when procuring equipment to determine if the manufacturer requires a specified service provider. This could increase maintenance costs.

Per Motorola R56®, *Standards and Guidelines for Communication Sites*, communications centers, data rooms, and other critical areas require metallic equipment chassis to be properly grounded to the building single-point ground system. The purpose of the grounding is as previously mentioned.

7.11. Site and Landscaping Systems (Grounds)

7.11.1. Hardscape

Hardscape areas include walkways, stairways, retaining walls, patio areas, and other areas made up of hard building materials for exterior use.

Hardscape areas must be regularly cleaned or cleared from debris, spills, and unwanted plant life. Debris will abrade the surfaces from foot traffic. Unwanted vegetation on the surface or between surfaces not only is unsightly but can be a trip or slip hazard. Mold growing on surfaces is a slip and health hazard.

Uneven surfaces are trip hazards. Most hardscape walkways, over time, will begin to settle, and not all sections at the same rate. Tree roots may grow beneath the surface. These situations will cause unleveled walking surfaces. The surfaces should be made level within 0.25-inch vertical rise.

Grout and mortar joints between hardscape, over time, will need to be replenished or repaired. Vegetation should be removed.

Handrails or handholds shall be verified for proper attachment. Their surfaces should be free from dirt, debris, and wildlife droppings. The entire system will require proper maintenance to retain its appearance and functionality.

Stairways shall be cleared of debris and other obstructions that may be a trip or slip hazard. The proper riser (vertical height between treads) and run (tread depth) shall be maintained. Typically, no greater than 7¾ inches on the riser and no less than 10 inches on the tread. This is especially a concern when the stairway was fabricated from landscape timbers or pavers.

7.11.2. Landscaping

Lawns shall be mowed at regular frequencies to maintain the lawn type recommended length. This length will vary during seasons and precipitation.

Watering of lawn and planting areas in drought seasons, as permitted by local jurisdictions, should be performed. Lawn and plantings with good root growth help to control erosion of topsoil during rainy seasons.

Weeds promote wildlife and insect infestation, tarnish appearance, and choke-out preferred plantings. Left uncontrolled, weeds can destroy a building's parking area, hardscape, fences, wall finishes, foundations, and other systems. A planned maintenance for weed control should be scheduled.

Proper drainage of the hardscape and landscape is paramount. Water should be channeled away from building foundations, walkways, and driveways. Standing water is a slip hazard, especially in winter months; it promotes insect infestation, growth of molds and algae, and suffocates plant life. Storm sewers and their grates should be periodically checked for debris and functionality.

The softscape, plants, trees, shrubs, flowers, and color schemes, are a costly investment. It's an investment that makes the workplace more attractive to the general public as well as the employees. With proper initial selection and continued maintenance, the softscape can remain healthy and aesthetically appealing. Pruning, extraction, and replacement of softscape is an ongoing maintenance cost.

7.11.3. Planter Ground Covers

Ground coverings, mulches, for planters typically are wood chips, pine straw, or stone. The covering is used to help control weeds, retain heat, control erosion, and retain moisture.

Organic mulches, wood chips, and pine straw are initially less expensive. They will breakdown over time and fertilize the soil beneath. The moist fertile soil makes a prime habitat for earthworms. Earthworms will aerate and vermicompost the soils, promoting good plant health.

Organic mulches will need replenishing each year. While the mulches may not have totally broken down, their appearance will be lacking. One alternative to replenishing the mulches is to have the mulch bed re-stained.

Inorganic mulches, pebble, rock, rubber, or pumice, typically, are greater in initial cost. Over the long-term, they may be less costly. They will not need to be replenished every one to two years like organic, they keep their appearance, and do not require as much maintenance. Inorganic mulches are better insulators and heat retainers than organic. Keeping the soil beneath heated promotes healthy bacterial growth, thus increasing the length of the growing season. They do not mold or promote insect infestation like organic.

The choice of organic or inorganic mulch is a matter of preference, although the inorganic is the less maintenance-intense choice.

7.11.4. Driveways, Roads, and Parking Areas

Driveways, roads, and parking areas need to be maintained. Over time with weathering, application of anti-skids or salts, and normal use, they will begin to breakdown. Concrete and asphalt will divot and need to be repaired. Sealing of asphalt surfaces will prolong its life. Cleaning of surfaces from debris, which causes abrading of the surfaces, is highly recommended. Spills and foreign fluids should be properly cleaned from the surfaces. Vehicle, walkway, and handicap linings will need to be replenished.

Vehicle barriers over time will deteriorate and be misaligned. They will need to be replaced, realigned, or refurbished.

Signage will tend to fade, oxidize, and get distorted due to weather. Sign posts and signage gets destroyed due to wildlife, vandalism, and accidental vehicular traffic.

Property fences tend to deteriorate faster when vegetation is allowed to grow around and on it. Gate posts, hinges, latching mechanisms, and locks will need to be maintained for ease of access. Bare copper materials and others that may cause galvanic corrosion to galvanized fencing shall be prohibited. Repairs to fencing may be needed due to unwanted destruction from vandalism, wildlife, or vehicles.

8. Technology Systems

Facility technology systems are systems that use an information system to accomplish their regular and specific tasks. Information systems are ever-changing. The information system of today is generally a computer-based system, whose basic components are hardware, software, databases, networks, and procedures.

In larger facilities, an information technology (IT) department oversees the maintenance and service of the information systems in a facility. The facility manager may assume responsibility for the installation and maintenance of the system’s hard-wiring and utilities.

Maintenance and service for technology systems is usually manufacturer-specific; at least until the warranty period has expired. The initial pricing and ongoing upkeep can be costly. Choosing the proper system in the beginning is very important. The costs for initial system installation, warranty, and future maintenance should be considered during the selection process of a technology system.

The system provider should offer and submit an ongoing service contract or service level agreement (SLA), unless the owner agrees to pay per visit or take on the service themselves. The SLA will document the services the vendor will provide and should outline performance standards and benchmarks they are to meet. Some benchmarks that the vendor should meet are time-of-day of service, response time, cost of emergency

service, software upgrades, system performance notifications, availability of historical data and generation of statistics, cost of helpdesk, telephone support, penalties, and exclusions. SLAs should be rolled into the initial system cost when available.

Major facility technology systems are discussed below.

8.1. Customer Premise Equipment

CPE includes equipment that is being housed at the facility owner's site, after the demarcation point (demarc). The utility provider will install their service to the demarc. After the demarc, it is the owner's responsibility to provide the equipment and service. The equipment and service may be purchased, leased, or rented from the service provider or other entity.

Today each of these systems are computer-based. Computer-based systems require hardware and software maintenance, updates, and replacement. Inter-facility hardwire and wireless networking systems need to be installed and maintained as well.

8.1.1. Telephony

Telephony is the process of transmission of voice and other sounds through telephones and their systems by use of wire, fiber optics, or wireless media.

There are many subparts to the telephone system:

- Plain old telephone service (POTS) lines
- Trunk lines
- Private branch exchange (PBX)
- Voice over Internet Protocol (VoIP)

These subparts are generally procured through different vendors. This means several contracts with vendors who need to marriage their equipment with those provided by others. The facility manager or designated person should be aware of how the entire system interacts. Monies can be wasted by having a vendor troubleshoot a problem that was not caused by their equipment.

8.1.2. 9-1-1 Communications Systems

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, Chapters 6–10 discuss the primary telephony and radio requirements for telecommunications in a communications center. Chapters 11–13, respectively, deal with the requirements for testing, record keeping, and data storage for the communications system.

9-1-1 CPE is a robust extension to the facility's telephone system. National Emergency Number Association (NENA) document NENA-04-001, *NENA Recommended Generic Standards for E9-1-1 PSAP Equipment*, provides information on features and interfaces to be considered when purchasing CPE.

- Enhanced 9-1-1 (E9-1-1) System Features
  - Selective routing
  - Default routing
  - Alternate routing
  - Central office transfer (selective, fixed, manual)
  - Automatic number identification (ANI)
  - Automatic location identification (ALI)
  - Forced disconnect
  - Night service – allowing a public safety answering point (PSAP) the ability to transfer their function to another directory number
  - Automatic call distribution (ACD) by central office or CPE
- PSAP Interfaces
  - Trunk
  - Central office-based E9-1-1
  - ALI database
  - Computer aided dispatch (CAD)
  - Recorders and teleprinters
  - ANI display
  - ALI display
  - PSAP time synchronization
  - Remote data transfer
  - 1A2 key telephone system
  - Telephone analog audio
  - Radio/telephone headset
  - Off-hook signal contact pairs
  - Handset/headset
  - PBX/ACD
  - PSAP alarms
  - Telecommunications Device for the Deaf/Teletypewriter (TDD/TTY)

8.1.3. Cable Television

Television may be provided by radio waves through the air, called broadcast television, or by coaxial cables, fiber-optic cables, and direct broadcast satellite.

Television is a vital part of a communications center. With today's technology, the real-time visual broadcasts of weather and news help arm the communications center with foreknowledge of upcoming or live events. The television helps to provide employee awareness, during downtime, and maintain employee morale.

8.1.4. Internet

The Internet is a global network of computer systems working together, much like the electrical grid, sharing and storing information.

The Internet has grown since its origin in the 1960s. It began as a commissioning by the United States Federal Government to build a robust, fault-tolerant computer network. Today, it is the medium to provide the World Wide Web (WWW), electronic mail (email), communications, VoIP telephony, streaming media, webcams, video conferencing, and file sharing.

Internet access is purchased by the facility for their required speed of data transmission and the quantity of projected users. The Internet may be provided through telephone POTS lines, coaxial cable, fiber-optic, or radio waves.

8.2. Local Area Network

The local area network (LAN) is the interfacility network that provides the working platform for multiple building systems. It allows users to access and input data from facility systems such as security, door access, CCTV, audiovisual (A/V), and others.

The LAN is generally supported and maintained by the facility's IT department or an on-call vendor. Different vendors may be needed to support their individual systems.

8.3. Security Systems

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, section 4.6 gives the primary detail on security needed at a communications center. Paragraph 4.6.2 states, "Entry to the communications center and other buildings and structures that contain equipment essential to the operation of the communications systems shall be restricted to authorized persons."[4] It goes on to state that potential areas of entry by unauthorized personnel "shall be protected by an electronic intrusion detection system. … The intrusion system shall be annunciated in the operations room and another location designated by the AHJ."[5]

Components of a security system include, but are not limited to, the following:

- Door access controls
- CCTV

[4] http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=1221
[5] Ibid.

- Security vestibules
- Self-closing fire doors rated not less than one-hour fire rating
- Self-closing fire doors rated bullet-resistant to Level 4 as defined by American National Standards Institute (ANSI)/Underwriters Laboratories (UL) 752, *Standard for Bullet-Resisting Equipment*
- Window sills on a direct exterior wall at a height of four feet or higher above finished grade or finished floor, whichever is higher
- Direct exterior windows rated Level 4 bullet-resistant as defined by ANSI/UL 752
- Perimeter walls meeting the same ballistic protection as windows
- Unauthorized vehicles prevented to a distance no less than 82 feet, unless the building is rated for blast-resistance

8.3.1. Door Access Controls

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communication Systems*, requires restricted access to authorized areas at a communications center. NFPA 72, *National Fire Alarm and Signaling Code*; NFPA 80, *Standard for Fire Doors and Other Openings Protectives*; NFPA 101, *Life Safety Code*®; and federal, state, and local building codes must be used to meet the requirements for installation of the door access control system.

A door access control system has a number of components, which require maintenance and provide opportunities for failure. Major components are as follows:

- Computer
- Software
- Door interface
- Interfacility cabling
- Pushbuttons
- Card readers
- Intercom
- Video intercom
- Electronic latches and strikes
- Door hardware (hinges, panic hardware, closures, etc.)

8.3.2. Closed-circuit Television

CCTV is the facility's audio surveillance system. The CCTV system is primarily comprised of a camera, recorder, and monitor. The components are networked together on the LAN. This may be by hardwire or wireless interfaces.

Maintaining a CCTV system includes, but is not limited to, the following:

- Ensuring the camera and housing are clean and dry
- Ensuring the camera's focus and auto iris are adjusted
- Checking operations of pan, tilt, and zoom
- Inspecting wiring and cabling for wear and proper support
- Ensuring coaxial cable signals are free from distortion
- Ensuring monitors maintain a quality image
- Ensuring video recorders are functioning properly
- Ensuring power connections are secure
- Verifying SPDs for functionality and grounding

Maintenance, other than trouble calls, should be scheduled at least once annually.

8.4. Audiovisual

An A/V system provides real-time situational awareness for communications center personnel, providing the opportunity for quick reaction and decision-making. The A/V system should be simple to operate through a graphical user interface developed by the vendor in coordination with communications center personnel.

Some A/V components include, but are not limited to, the following:

- Projector, to interface with automated projector screen
- Touch-screen interactive monitor
- Video matrix system and controllers
- Audio system (program audio and local voice reinforcement)
- A/V control system
- Monitors in the communications center

A/V systems should have biannual preventative maintenance, which includes the following:

- Cleaning and dusting of racks, cable connections, and equipment
- Cleaning the projector filter
- Checking projector lamp hours
- Calibrating the focus, screen fit, and picture quality of the video system
- Tuning the audio system
- Updating software
- Conducting a complete system functionality test

8.5. Facility Management Computer Programs

Facility computer programs, such as Computer-aided Facilities Management (CAFM), Computerized Maintenance Management Systems (CMMS), and building automation system software, are key programs for a facility manager to manage their assets.

Facility manager computer software and hardware will require updates, upgrades, and periodic replacement. The hardware that interfaces with the software will require calibration, adjustment, and replacement.

8.5.1. Computer-aided Facility Management

CAFM uses IT support for planning facility operations. It assists the facility manager in tracking, planning, managing, reporting, and updating facility layouts, and moving assets in drawing and word files.

The CAFM system is used as a tool for budgeting, asset management, space management, scheduling, and other customer services. Computer-aided design can be integrated with most CAFM systems to assist the facility manager with facility space management and asset moving management.

8.5.2. Computerized Maintenance Management Systems

CMMS are IT-based programs that the facility manager can use to manage the day-to-day functions of the facility. Work orders, trouble calls, asset maintenance, labor hours spent, and materials purchased are some of the common functions of a CMMS. With data collected from daily operations, the facility manager can analyze the facility systems and make adjustments in maintenance to help control asset cost and maintain a healthy life cycle.

8.5.3. Building Automation Systems

A facility controlled by a building automation system is generally referred to as a smart building. Sensors interface with the building automation program to allow monitoring and adjustment of alarms and set points for building systems. Building systems such as HVAC, security, fire prevention, electrical, plumbing, and others may be supervised by a building automation system.

The sensing devices will require adjustment, calibration, and periodic maintenance or replacement.

8.6. Public Safety Radio Communications

The FCC requires very strict adherence to their issuance of licenses to operate equipment that provides communications via the air waves. FCC inspections and fines can be levied for non-compliance to rules and regulations. Some FCC requirements address the following:

- Licensing/renewal of licenses
- Frequencies

- Radiated output power of transmitters
  - Distortion
- Bandwidth requirements
- Effective radiated power (ERP) from antennas
- Harmonic suppression of transmitters

In addition, the Federal Aviation Administration (FAA) regulates FCC communications tower lighting. Rules are as follows:

- Towers over 200 feet in height must have tower lighting that meets FAA requirements.
- When a light on a tower fails for any reason, it must be reported to the FAA immediately and must be replaced as soon as possible.
  - Lighting power failures for a given tower must also be reported immediately.

Note: ANSI/Telecommunications Industry Association (TIA)–222-G, *Structural Standard for Antenna Supporting Structures and Antennas* was updated effective January 1, 2017 to TIA-222-H. The revisions added specific comments on metal fatigue in tower materials because an upgrade for metal fatigue will be required.

8.7. Amateur Radio (HAM)

The United States Federal Government began licensing amateur radio operators in 1912. In May 1914, after thousands of amateur radio operators—HAMs—in the United States were licensed, Hiram Percy Maxim saw the need for an organization to band together amateur radio operators. Maxim founded the American Radio Relay League (ARRL).

Pursuant to law, the FCC has issued detailed regulations for the amateur service, which are addressed in 47 Code of Federal Regulations, Title 47: Telecommunication, Part 97–Amateur Radio Service.[6] All FCC requirements must be closely monitored to ensure FCC regulations are met.

HAM radio operators have provided communications in times of disasters at no cost to anyone. HAM radio is often referred as the last effort for communications during a disaster or communications outage or problem with commercial entities. If a disaster or an emergency arises, volunteer teams of amateur radio operators will operate the amateur radio equipment in the EOCs. Amateur operators provide this service at no cost; the "biggest bang for the buck" in communications services. In addition, amateur radio operators supplement the equipment provided in the EOCs with personal equipment, such as a fixed station, mobile station, emergency generators, etc. Therefore, it is critical that amateur wireless communications equipment be installed and maintained in EOCs.

[6] http://www.arrl.org/part-97-amateur-radio

HAMs can also help fill the gap between agencies whose radio systems are incompatible with one another.

Amateur radio disaster response activities usually are provided under the umbrella of the Amateur Radio Emergency Service® (ARES), sponsored by the ARRL, and the Radio Amateur Civil Emergency Services (RACES), administered by FEMA. RACES works with government agencies to maintain civil preparedness and provide communications in times of civil emergencies. RACES is activated at the request of a local, state or federal official.

Amateur radio equipment that will require maintenance includes, but is not limited to, the following:

- Receivers
- Transmitters
- Antenna feed cables
- Transmitter – power output
- Power supply voltages
- Grounding
- AC power voltage/regulation
- Remote control equipment
- Computer/fiber optic interface

The following must also be accomplished when necessary:

- Transmitter intermodulation distortion (IMD) test
- Transmitter audio output calibration
- Antennas sweep testing
- Standing wave ratio (SWR) measurement
- Testing for FCC requirements
- FCC license renewal (station/operator)
- Equipment repair and upgrades

9. Maintenance Frequencies

Facility systems shall be inspected for integrity after service, additions, replacement, and at regularly scheduled maintenance intervals.

Maintenance frequencies largely depend upon the facility's geographic location. Negative geographic location attributes include seasonal climate changes, rural or urban environments, supply availability restraints, and others; for example, the HVAC filters

and condenser coils will need to be changed and cleaned more frequently in dusty environments.

Maintenance frequencies are dependent upon non-typical weather patterns; for example, drought will cause a decline in the lawn mowing frequency.

Software upgrades to facility systems is almost inevitable. The frequency of software upgrades is dependent upon system hardware upgrades, replacement, or obsolescence.

Data acquired from historical and experience-based insight and published industry standards for the frequency of facility system maintenance is illustrated in Appendix A – Frequency.

10. Maintenance Budgeting and Expenditures

Facility and technology maintenance is the owner's or designated person's responsibility. There are various budgeting methods that the owner can use, such as the benchmarking, incremental, and asset-based methods that are discussed below.

10.1. Budgeting

10.1.1. Benchmarking

Benchmarking is where the facility and system maintenance costs are calculated on a standard increment. Using the cost per square foot of building space is a good starting point. If maintained throughout the years, it can be a great estimating tool for future projects and a gauge to see current variances.

Benchmarking using industry square foot costing for facility systems is essential when a facility is new or there is no recent historical data.

10.1.2. Incremental

Incremental budgeting is based on the preceding period's budgeted or actual results as a baseline, with incremental amounts added for the new budget period. There are advantages and disadvantages to this method.

- Advantages
  - Incremental budgeting is fairly stable and changes are gradual.
  - The impact of budget variances can be detected in a timely manner.
  - The method is relatively simple to understand and manage.
  - It is a reasonable method for smaller facilities.
  - Incremental budgeting makes maximum use of historical expenditure and capital cost data.

- Disadvantages
  - Incremental budgeting assumes that the activities and maintenance remain the same.
  - It encourages the spend it or lose it mentality.
  - A budget could become out-of-date and not correspond to the required level of maintenance if not properly altered.
  - There are no incentives to reduce cost or generate new ideas.

10.1.3. Asset-based

Asset-based budgeting is a more accurate way to budget as each asset is examined individually to determine expected costs for the various work to be performed, such as inspections or preventative maintenance.

Asset maintenance costs are built from the bottom up, planning for defined maintenance windows and inspections, for example. This method tracks costs for maintaining an individual system or, even finer, each specific component. When used properly, this method is useful in determining an asset's life cycle, and when it will be necessary to plan for replacement.

Asset-based budgeting can promote cost-savings and generate different maintenance strategies. Larger entities would likely find this method advantageous.

10.2. Expenditures

Maintenance and repair expenses are costs to restore a system or equipment to its original or working condition, and are generally smaller cost items. These expenses should be accounted for in the yearly maintenance operations cost. Adjustments should be made each year in the budget to reflect the system's or equipment's increased cost due to age.

Capital expenses are costs to purchase an asset, extend its life, or improve its efficiency or capacity, and are generally large cost items. Capital expenses should be separate line items on the maintenance budget.

Appendix A: Frequency

The Facility and Technology System Maintenance Frequency spreadsheet can be found on the following pages.

Facility and Technology Systems	Sub-system	Task	Frequency
Site and Landscaping Systems (Grounds)			
	Hardscape	Cleaning	Monthly
	Landscape	Cut lawn	Weekly
		Water lawn and/or plantings	Weekly
		Weed removal	2x/Month
		Prune trees and shrubs	Semi-annually
		Check and clear drainage	Semi-annually
	Planter	Replenish or stain organic mulch	Annually
		Refurbish embedded inorganic mulch	Every 3–5 years
	Driveway Roads and Parking Areas	Sweeping	Semi-annually
		Anti-skid application and snow plowing	As needed
		Sealing and re-lining	Every 3 years
	Waste Disposal	Trash removal	2x/Week
Structural Systems			
	Foundation	Inspect for deterioration	Annually
	Substructure	Inspect for deterioration	Annually
Exterior Building Systems (Building Envelope)			
	Roof	Inspect	Quarterly
	Roof Drainage	Inspect	Quarterly
	Exterior Walls	Clean and inspect sealants	Annually
Flooring Systems			
	Fire Barriers	Inspect for deterioration	Annually
	Integrity	Inspect for deterioration	Annually
Mechanical Systems / HVAC Systems			
	HVAC	Filter cleaning or replacement	Quarterly
		Inspect fans, bearings, and belts	Semi-annually
		Clean evaporator and condenser	Annually

Facility and Technology Systems	Sub-system	Task	Frequency
		Inspect duct work and plenum	Every 2 years
Plumbing Systems			
	Potable Water System	Pressure pump system maintenance	Semi-annually
		Inspect water component functionality	Annually
		Inspect backflow preventer	Annually
	Sewer System	Lift station maintenance	Monthly
Electrical Systems			
	Grounding	Inspect connections	Quarterly
	Lightning Protection System	Verify connections	Quarterly
		Recertification and system testing	Every 3 years
	Surge Protection Devices	Visual inspection	Monthly
		Physical inspection	Annually
	Uninterruptible Power Supply	Inspect equipment for loose connections, burned insulation on conductors, any signs of wear	Quarterly
		Visually check batteries	Semi-annually
		Test UPS transfer switches, maintenance bypass, and circuit breakers.	Semi-annually
		Thermal scan	Annually
		Battery Replacement	Every 5 years
	Generator	30-minute run test	Weekly
		Operation w/load switching test	Monthly
		Oil Service	Semiannually
		Fuel	Annually
	Emergency Lighting and Exit Signs	30-second functionality test	Monthly
		1.5-hour functionality test	Annually
	Lighting	Control testing and inspection	Annually
		Bulb replacement	Every 2 years

Facility and Technology Systems	Sub-system	Task	Frequency
Conveying Systems			
	Elevator	Recertification and system testing	Annually
Fire Protection Systems (FPS)			
	Fire Extinguishers	Pressure and physical condition	Monthly
		Recertification and system testing	Annually
	Fire Suppression System Main Building	Recertification and system testing	Annually
	Fire Suppression System Equipment Area	Recertification and system testing	Annually
	Smoke and Fire Detection System	Recertification and system testing	Annually
Interior Finishes			
	Custodial	Carpet shampooing	Semi-annually
		Flooring hard surface deep cleaning and sealing	Semi-annually
		Window and window covering cleaning	Semi-annually
Furniture, Fixtures, and Equipment			
	Custodial	Facility general cleaning, bathroom and kitchen sanitizing, carpet spot removal and trash removal	2x/Week
		Door glass cleaning and handle sanitization	2x/Week
		High dusting of vents, lights, wall hangings, etc.	Monthly
		Chair and equipment dusting/vacuuming	Monthly
Customer Premise Equipment (CPE)			
	Telephony	Vendor-specific	Contract response time
	9-1-1 Communications Systems	Vendor-specific	Contract response time
		Operator functionality testing per NFPA 1221	Daily

Facility and Technology Systems	Sub-system	Task	Frequency
		Primary and secondary radio and voice amplification circuits	2x/Daily
		Wired dispatch circuits	Daily
		Power supply for wired dispatch	Daily
		PSAP emergency telephone circuits	Daily
		TDD/TTY	Daily
		Outside alert systems	AHJ Requirements
	Cable Television	Vendor-specific	Contract response time
	Internet	Vendor-specific	Contract response time
Local Area Network (LAN)			
	LAN	Vendor- or internal IT department-specific	Response time generated
Security Systems			
	Door Access Controls	Visual inspection and adjusting	Monthly
	Closed-circuit television (CCTV)	Camera service and system checks	Annually
Audiovisual (A/V)			
	A/V Components	Service and functionality checks	Semi-annually
Facility Management Computer Programs			
	Computer-Aided Facility Management (CAFM)	Vendor-specific	Contract response time
	Computerized Maintenance Management Systems (CMMS)	Vendor-specific	Contract response time
	Building Automation System (BAS)	Vendor-specific	Contract response time
Public Safety Radio Communications			
	Two-way Radio Equipment	Functionality test	Annually

Facility and Technology Systems	Sub-system	Task	Frequency
	Tower Sites	Required maintenance tasks	See tower site maintenance document for detail
Amateur Radio (HAM)			
	Radio Equipment	Exercise test	Monthly
	Two-way Radio Equipment	Functionality test	Annually

Appendix B: National Fire Protection Association 1221 Overview

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, 2016 Edition, addresses "the installation, performance, operation, and maintenance of public emergency services communications systems and facilities."[7] The standard is updated every three years.

A brief overview of the standard is provided below. The majority of information has been taken directly from the standard. Free access to the standard may be found at the following website: http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=1221.

For ease of reference, this appendix is numbered as Section 11.

11. NFPA 1221

11.1. Chapter 1 – Administration

Chapter 1 reviews the standard's updates, alerts, future editions, scope, purpose, applications, retroactivity, and equivalency.

Not all updates made to the past 2013 standard edition will be retroactive for preexisting facilities, equipment, structures, or installations. Table 1.4 in Chapter 1 lists those chapters that are retroactive.

11.2. Chapter 2 – Referenced Publications

Chapter 2 lists other documents that are referenced in NFPA 1221. The referenced documents or portions thereof are to be considered part of the requirements of the document. Examples of, but not limited to, listed publications are the American Society for Testing and Materials (ASTM), Institute of Electrical and Electronics Engineers (IEEE), Telecommunications Industry Association/Electronic Industries Alliance (TIA/EIA), and Underwriters Laboratories (UL).[8]

11.3. Chapter 3 – Definitions

Chapter 3 provides explanatory definitions that are relevant to this particular standard. Words not defined within this chapter will assume the ordinarily accepted definition as found in *Merriam-Webster's Collegiate Dictionary*.

For example, AHJ is the authority having jurisdiction and is defined as "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." As another example,

[7] NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, 2016 Edition. Section 1.1.1.
[8] Ibid., Chapter 2.

an alarm is "A signal or message from a person or device indicating the existence of an emergency or other situation that requires action by an emergency response agency."

11.4. Chapter 4 – Communications Centers

The requirements for construction and system installations for communications centers, alternate communications centers, and remote communications centers are discussed in Chapter 4.

11.4.1. General[9]

At all times, communications equipment is to be kept in working condition.

A center's primary means of communications is to be compatible with Emergency Response Facilities' (ERF) primary means of communications.

A center's alternate means of communications is to be compatible with an ERF's alternate means of communications.

An alternate communications center, geographically separated from the primary center to ensure survivability of the alternate center, is to be maintained.

An operations and maintenance plan for the alternate center is to be developed and included in a CEMP.

When the alternate facility is operational, it is not to rely on equipment at the primary center for any functions.

11.4.2. Exposure Hazards[10]

When the building that houses the center is adjacent to another structure, the exposed walls are to be protected in accordance with NFPA 5000, *Building Construction and Safety Code*®, or the legal building code in effect. The more stringent of the two is to apply.

When the building that houses a communications center is within 150 feet of a taller structure, the roof is to be designed to resist damage if the taller structure were to collapse.

The lowest floor of the communications center is to be above the 100-year flood plain.

11.4.3. Construction[11]

Communications centers are to be located in buildings that comply with NFPA 220, *Standard on Types of Building Construction*, type T1 or T2 construction.

[9] Ibid., Section 4.1.
[10] Ibid., Section 4.2.
[11] Ibid., Section 4.3.

The roof covering is to be Class A.

Communications centers that occupy the same building as non-emergency entities are to be separated by fire barriers rated as 2-hour fire resistant in compliance with NFPA 101, *Life Safety Code®*.

Communications centers are not to be located below grade unless they are above the 500-year flood plain and designed specifically in compliance with NFPA 101.

Interior walls and ceilings are to have a flame resistance index of 25 and a smoke index of 50 as tested in accordance with ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials*.

The floor material is to comply with the requirements of NFPA 101.

The operations room is to have a toilet facility and lunch area directly accessible by staff within the secure area.

Backup drinking water and sanitary facilities are to be provided for staff during extended downtimes of public utilities.

The building is to comply with seismic protection requirements of NFPA 5000, *Building Construction and Safety Code®*, or the legal building code in effect.

11.4.4. Climate Control[12]

HVAC units are to be installed in accordance with NFPA 90A, Standard for the Installation of Air-Conditioning and Ventilating Systems, and 90B, Standard for the Installation of Warm Air Heating and Air-Conditioning Systems.

A communications center is to have its own climate control; non-dependent of adjoining facilities.

The equipment room, operations, and office areas are to have their own controls for temperature and humidity.

Fresh air intakes are to be designed to restrict smoke from external area fires and to resist intentional introduction of hazardous gaseous substances.

Emergency controls are to be installed within the operations area to close outside air intake dampers.

The operations and electronic equipment areas are to have redundant HVAC units. The units are to be capable of receiving power from all utility and backup generator sources. HVAC units are to be located so as to inhibit tampering, vehicle impact, or introduction of hazardous gaseous substances.

[12] Ibid., Section 4.4.

11.4.5. Fire Protection[13]

This section of NFPA 1221 references NFPA 10, *Standard for Portable Fire Extinguishers*; NFPA 72, *National Fire Alarm and Signaling Code*; NFPA 13, *Standard for the Installation of Sprinkler Systems*; supervision in accordance with NFPA 101, *Life Safety Code®*; and NFPA 75, *Standard for the Fire Protection of Information Technology Equipment*.

11.4.6. Security[14]

Security requirements for a communications center are briefly described below.

11.4.6.1. Doors

Access is to be restricted to authorized personnel only.

Doors are to be protected by an electronic intrusion detection system. The system is to be annunciated within the operations room and another area as designated by the authority having jurisdiction (AHJ).

A security vestibule is to be installed at the main entrance to the communications center.

Door openings are to be protected by 1-hour rated self-closing fire doors.

Door openings are to be protected by listed, self-closing doors rated for Level 4 bullet resistance.

11.4.6.2. Windows

Window sills are to be four feet above the floor or finished grade, whichever is higher.

Direct exterior windows are to be rated for Level 4 bullet resistance.

If an exterior window faces a secured area and is not able to be viewed or accessed from outside the secured area, bullet proof glass is not required.

Bullet proof glass windows are to be fixed non-operable glass.

11.4.6.3. Walls

Walls are to have the same bullet proof characteristics as the windows.

11.4.6.4. Restricted Entrance

Unauthorized vehicles are to be restricted within 82 feet of the facility, unless the facility is blast-resistant as approved by the AHJ.

[13] Ibid., Section 4.5.
[14] Ibid., Section 4.6.

11.4.7. Power[15]

Critical operations power systems (COPS) are to supply power to the designated critical operations areas (DCOAs).

DCOAs include the operations room; Information Technology (IT) areas; telephone rooms; electrical and mechanical equipment rooms; fire protection equipment rooms; sanitary facilities; and others areas designated by the AHJ.

At least two independent power systems are to be installed:

- Primary – utility power
- Standby (Generator) – energizes within 10 seconds; reference NFPA 70, *National Electrical Code*®, Article 700.12

A backup mobile generator hook-up is to be provided.

Power systems are to be monitored for operation and alarms; annunciation is to be within the operations room.

The utility power disconnecting means is only to be accessible to authorized personnel.

SPDs are to be installed.

A single-point grounding system is to be installed.

A UPS is necessary to:

- Supply load to the critical IT, telephone, radio, and other sensitive electronic equipment
- Supply load to equipment during the transfer time from utility to back-up generator power; in no case less than 15 minutes

The UPS status is to be annunciated within the operations room

The UPS is to have a by-pass switch for maintenance without any interruption of service.

11.4.8. Lighting[16]

Adequate artificial lighting is to be provided for staff to perform their assigned tasks.

Emergency lightning is to be provided. Emergency lighting is to energize to full capacity within 10 seconds of power loss.

Illumination levels are to be adequate for staff to perform essential tasks.

[15] Ibid., Section 4.7.
[16] Ibid., Section 4.8.

11.4.9. Lightning[17]

Buildings that house communications centers are to have an LPS that complies with NFPA 780, *Standard for the Installation of Lightning Protection Systems*.

11.4.10. Remote Communications Facilities[18]

Essentially, the same specifications noted for a primary communications center apply to a remote facility.

11.5. Chapter 5 – Communication and Signal Wiring

Chapter 5 discusses conductors, cables, and fiber-optic cables installed for audio and visual signaling and transmission of voice, television, and data to and within the communications center.

11.5.1. Circuit Construction and Arrangement[19]

Installation of the communication and signal wiring circuits is to comply with NFPA 70, *National Electrical Code*®.

Record drawings of the communication and signal wiring are to show diagrams of office wiring.

Communication and signal wiring from other than the municipality must be given permission by the AHJ to run in the same cable.

11.5.2. Circuit Conductors[20]

Circuit conductors are to be secured to prevent vibration and breakage.

Conductors terminated and collocated on equipment racks with other systems are to be identified, whenever possible.

Metallic shielded or sheathed fiber-optic cabling is to be grounded per NFPA 70, *National Electrical Code*®.

Wiring for control equipment shall be No. 24 American wire gauge (AWG) or greater.

Wiring that is unsupported or subject to vibration shall be No. 18 AWG or larger.

Exterior wiring shall meet International Municipal Signal Association (IMSA) specifications, unless they are provided by a public utility on lease.

[17] Ibid., Section 4.9.
[18] Ibid., Section 4.10.
[19] Ibid., Section 5.1.
[20] Ibid., Section 5.2.

11.5.3. Underground Cables[21]

Underground cables installed in ducts, manholes, or vaults are to be protected from damage and heat from fire in adjacent buildings. The cables are to be identified within the enclosures. The cables may be collocated with communication and signaling cabling 600 volts, nominal or less. The underground cables are to be separated, as far as physically possible, with a non-combustible barrier from other circuits 250 volt to ground or greater.

Conduits or ducts are to be sealed upon entering the building to prevent entrance of moisture or hazardous gases.

Direct-burial cables are to be buried 24 inches or greater, and are to be run in areas that are not intended for future excavation, such as under sidewalks. A detectable warning tape is to be installed 12 inches below grade directly above the buried cables.

Cable splices are to be accessible for maintenance and inspection. The splices are to be made providing functionality and protection as the cable would have afforded. The ends are to be sealed from moisture.

11.5.4. Aerial Cable and Wire Construction[22]

Aerial communication and signaling cables are to be run beneath power wires. These cables are to be protected from damage within trees, beneath bridges, and other areas that may be subject to damage the cables.

Cables are to be supported by messenger wire or be rated as a self-supporting cable assembly. The span length is to be within the cable manufacturer's specifications.

Single wire runs are to be No. 12 AWG for copper-covered steel; No. 10 AWG for galvanized iron, steel, or hard-drawn copper; or No. 6 AWG for aluminum.

Aerial communication and signaling wiring is to enter structures and raceways through an approved downward sloped weather-head preceded by a drip loop.

Cables that traverse downward on a pole are to be protected from damage. Metallic covering is to be bonded to the earth grounding electrode system. The installation is to be made watertight. The cable insulation is to be rated for 600-volt and approved for wet locations.

11.5.5. Wiring Inside Buildings[23]

Within a communications center, communication and signaling wire, cables, and fiber-optic cables are to run to the operations area by means of conduits, ducts, shafts, raceway, and overhead cable trays or troughs. The systems are to be identified and listed as suitable to provide protection from physical damage.

[21] Ibid., Section 5.3.
[22] Ibid., Section 5.4.
[23] Ibid., Section 5.5.

The wire, cable, or cable assembly is to be fire-rated to the specification of its environment; for example, plenum-rated cables and raceways are to be used within air handling spaces.

When installed within buildings, conductors and fiber-optic cabling is to be installed in electrical metallic tubing (EMT), intermediate metallic conduit (IMC), rigid metallic tubing (RMC), metallic surface raceways, reinforced thermosetting resin conduit (RTRC), or for environmental reasons and approved by the AHJ in polyvinyl chloride (PVC).

Conductors and fiber-optic cabling is to be run free of splice as much as practical. Splices are to be made in approved enclosures or approved terminating devices. The covers and doors housing the splices are to be identified by a distinctive color labeling. The words "Emergency Communication-signal Circuit" are to be used for the required label.

When communication and signaling wiring are run in a shaft with power and light circuits, the wiring is to be separated by two inches or both are to be enclosed in non-combustible enclosures.

Cross-connecting facilities for metallic and fiber-optic cabling, like a main distribution frame (MDF) or an intermediate distribution frame (IDF) area, are to be either in or adjacent to the communications center's operations area.

Mission-critical wired devices and others whose failure would have a negative impact on the dispatching process are to be located on or within non-combustible surfaces, like pedestals, cabinets, or panels.

11.5.6. Circuit Protection[24]

Circuit protection by means of fast-acting SPDs are required on wired communication circuits at their point of entrance into the communications center.

SPDs are to be installed in a location accessible for maintenance only by qualified personnel. SPDs are to have manufacturer name and model number legible.

Buildings that house the communications centers are to have an LPS installed and compliant per NFPA 780, *Standard for the Installation of Lightning Protection Systems*.

11.5.7. Fuses[25]

Fuses are to be located at the power source and clearly marked with amperage rating. Fuses greater than 2 amps are to be enclosed.

[24] Ibid., Section 5.6.
[25] Ibid., Section 5.7.

11.5.8. Grounding[26]

SPDs and sensitive electronic equipment, like computers, telecommunications equipment, and two-way radio systems, are to be bonded to the building's single-point grounding system. This is to be in accordance with NFPA 70, *National Electrical Code*®, Article 647.

Where required by the AHJ, unused wires and cable pairs are to be grounded.

Listed isolated ground receptacles, in accordance with NFPA 70, are to be provided for all cord-and-plug connected essential and sensitive electronic equipment.

11.5.9. Access[27]

All equipment is to be accessible for maintenance.

11.5.10. Pathway Survivability[28]

Communication and signaling pathways are to comply with NFPA 70, *National Electrical Code*®, and as referenced in NFPA 72, *National Fire Alarm and Signaling Code*, Section 12.4.

NFPA 72 Section 12.4 states that pathways are to comply with NFPA 70 for critical circuits.

NFPA 70 Article 770.179(E)(1) or (E)(2) for circuit integrity of fiber-optic cable or electrical circuit protective system installation states a 2-hour fire rating for the cable or the system.

NFPA 70 Article 800.179(G)(1) or (2) for circuit integrity of communication cable or electrical circuit protective system installation states a 2-hour fire rating for the cable or the system.

11.6. Chapter 6 – Emergency Response Facilities

Emergency response facilities (ERFs) are facilities that house emergency response agencies and emergency response unit personnel that respond to fire, medical, law enforcement, rescue, and other situations that deal with the preservation of life and safety.

11.6.1. General[29]

ERFs are to have primary and secondary means of dispatch that are compatible with the communications center. The equipment is to be maintained in working order.

A public accessible means of reporting alarms to the communications center is to be provided on the ERF exterior.

[26] Ibid., Section 5.8.
[27] Ibid., Section 5.9.
[28] Ibid., Section 5.10.
[29] Ibid., Section 6.1.

11.6.2. Commercial Telephone[30]

A commercial telephone line is to be provided at each ERF. When no other means of communications between the communications center and ERF is provided, the commercial line is to be non-public. A telephone line provided and maintained by the AHJ, such as through their PBX, is not an acceptable commercial line.

11.6.3. Fire Protection[31]

Fire protection is to be provided according to NFPA 5000, *Building Construction and Safety Code*®, or local requirements; the more stringent is to apply. The sprinkler system is to comply with NFPA 13, *Standard for the Installation of Sprinkler Systems*. Fire alarm systems shall comply with NFPA 72, *National Fire Alarm and Signaling Code*.

11.6.4. Power and Lighting[32]

ERFs are to have two separate means of reliable power source. Lighting is to be provided to allow emergency response units to affectively operate communications equipment. Emergency lighting is to comply with NFPA 101, *Life Safety Code*®, Section 7.9.

11.6.5. Communications Conductors[33]

SPDs are to comply to those installed in the communications center.

An LPS is to be installed in compliance with NFPA 780, *Standard for the Installation of Lightning Protection Systems*.

11.7. Chapter 7 – Operations

11.7.1. Management[34]

The AHJ is to provide a director, manager, or supervisor to oversee the operations of the communications center. The AHJ is to provide supervisory training for the manager and others in supervisory positions.

Communications centers are to have trained and qualified technical support either in-house or contracted for the maintenance of the communications center's systems.

Maintenance and installation records are to be maintained per the requirements of the AHJ. When an outside contractor performs maintenance, they are to forward written records to the employee designated by the AHJ. Written records are required for the following: maintenance, testing, installation, and extension of the system. Equipment and systems are to be accessible to the AHJ for maintenance.

Maintenance by an outside contractor is to be by a contract that has measurable guarantees of performance.

[30] Ibid., Section 6.2.
[31] Ibid., Section 6.3.
[32] Ibid., Sections 6.4 and 6.5.
[33] Ibid., Section 6.6.
[34] Ibid., Section 7.1.

11.7.2. Telecommunicator Qualifications and Training[35]

Telecommunicators are to meet the qualifications set forth by NFPA 1061, *Professional Qualifications for Public Safety Telecommunications Personnel*. The AHJ is to establish the operational guidelines by which telecommunicators will perform. These requirements are to include education, age, background, character, medical and physical requirements that are subject to the Equal Employment Opportunities Act and American with Disabilities Act, and cognitive and psychomotor skills for areas of reading, spelling, speech, mathematics, basic language, written communications, listening, and basic computer skills.

Telecommunicators are to be certified in the position which they hold, and are to be recertified per the requirements of the certifying organization.

Telecommunicators are to be trained in general emergency service operations and have access to information regarding locations of streets, landmarks, and congested or hazardous areas.

Telecommunicators are to have operational knowledge of communications equipment, systems, and networks within the communications center. They are to know governing regulations and rules for use of the communications equipment, such as FCC rules.

Telecommunicators are to be trained in TDD/TTY procedures and provided refresher training every six months.

Telecommunicators are to receive training in the CEMP and Tactical Interoperability Communications Plan (TICP) annually.

11.7.3. Staffing[36]

Two telecommunicators are required to be on duty at all times. Others are to be added as determined by the amount emergency and non-emergency calls received during a yearly period.

A supervisor is to be on-duty when there are more than two telecommunicators on-duty. The supervisor, although generally a problem solving role, may relieve the telecommunicator for short periods of time. The telecommunicator is to remain at the communications center and be ready for immediate recall to duty.

Emergency calls are to take preference over non-emergency calls. Non-emergency calls are not to delay emergency response by a telecommunicator.

An SOP is to be drafted by the AHJ for the process when a telecommunicator is asked by an incident commander to be dedicated to the incident.

[35] Ibid., Section 7.2.
[36] Ibid., Section 7.3.

11.7.4. Operating Procedures[37]

Ninety-five percent of alarms received on emergency lines are to be answered within 15 seconds and 99 percent within 40 seconds. Compliance is to be evaluated monthly using the previous month's data.

Various emergency calls, such as, those requiring language translation and hazardous material incidents, require processing within 90 seconds 90 percent of the time and within 120 seconds 99 percent of the time.

Law enforcement alarms are to be processed within the parameters required by the AHJ.

When an alarm is transferred from the primary PSAP to a secondary answering point, the alarm transfer is to be within 30 seconds 95 percent of the time. The originating telecommunicator is to remain on the line until the transfer is confirmed by the accepting telecommunicator. This transfer procedure is to be used on emergency 9-1-1 calls.

A telecommunicator is to be aware of a dispatched unit's status at all times. Records to be recorded include the unit dispatched, time dispatched, en route time, arrival time, time of patient contact (if applicable), and time of return to service.

A distinctive audible alert tone is to precede all emergency alert alarms.

An evacuation alarm is to be a distinctive audible tone; different than that of an emergency alert alarm.

An interoperability plan, between agencies that interact, is to be established and reviewed at least annually. The plan is to include written procedures, communication links and protocols, and common terminologies.

Communications equipment involved with each alarm is to be promptly restored to service after each alarm. If the equipment is found faulty, a telecommunicator is to troubleshoot and repair or isolate the fault and report it to the proper personnel.

SOPs are to include:

- All standardized procedures that a telecommunicator is expected to perform without direct supervision
- Implementation plan for alternate communications center
- Procedures related to the CEMP
- Emergency response personnel emergencies
- Activation of an emergency distress function
- Assignment of incident radio communications plan matrix

[37] Ibid., Section 7.4.

- Time limit for acknowledgement by units that have been dispatched
- Methods for call trace
- Methods for caller location determination

An SOP is to be developed for responding to TDD/TTY calls. A telecommunicator is to treat an open line or silent call (no voice response) as a TDD/TTY call.

The CEMP is to include a comprehensive regional emergency communications plan. The plan is to have provisions for real-time communications between emergency response agencies responding to the same incident. The plan is to be exercised at least annually.

When a unit has been dispatched does not respond within the established time limit, the telecommunicator is to attempt to contact the unit by one or more methods, such as radio contact, re-dispatch via primary or secondary dispatch system, or initiate communication with the unit's supervisor. If time has elapsed per SOP requirements, the telecommunicator is to dispatch a backup unit.

11.7.5. Time[38]

All systems and their devices (computers, servers, appliances) are to synchronize via a master clock, and are to automatically update during daylight savings and standard time changes without the intervention of the AHJ.

Any timekeeping device not capable of synchronization is to be maintained within 60 seconds of the master clock system.

11.7.6. Recording[39]

Communications centers are to have a logging voice recorder, synchronized with the master clock, that has a channel for recording the following:

- Each transmitted or received radio channel or talk group
- Each voice dispatch alarm circuit
- Each telecommunicator telephone

Logging equipment connected to a Next Generation 9-1-1 Emergency Services IP network (ESInet) is to have the ability to log event data.

Telecommunicators are to have the ability to instantly recall recordings from their position.

Logged data is to be maintained and retained per the requirements of the AHJ.

[38] Ibid., Section 7.5.
[39] Ibid., Section 7.6.

11.7.7. Quality Assurance[40]

A communications center is to establish a quality assurance program to review and refine procedures, policy, and execution of their existing alarm processing methods.

11.8. Chapter 8 – Telephones

Chapter 8 deals with the telephony facilities and equipment used by the emergency response agencies.

When 9-1-1 services are available in an area, they are to be listed as such in the telephone directory. If 9-1-1 services are not available, specific numbers are to be published in the telephone directory for emergency services and non-emergency calls.

In addition, a separate non-published telephone line is to be installed and maintained for communications with other emergency services agencies and central station alarms. Another line is to be installed and maintained for non-emergency calls.

If an ERF is not continuously staffed 24 hours for emergency call answering, there is to be an answering device with a recorded message directing the caller to a staffed ERF.

Minimum required telephone lines and numbers within a communications center are listed below:

- Published emergency number with two lines for call taking; additional lines added as volume deems necessary.
- Published non-emergency number that is attended by personnel at least 40 hours per week Monday through Friday
- One outgoing line
- Separate line for ERF to ERF and central station alarms
- Separate automated unlisted voice-alert telephone line when AHJ allows
- Separate automated unlisted data alarm when AHJ allows
- Normal business (non-emergency) lines as needed

When all emergency lines are in use, the next emergency call is to hunt to other lines as predetermined by the AHJ. Non-emergency lines are not to hunt to emergency lines.

All emergency telecommunicator positions are to be equipped to answer TDD/TTY messages.

11.8.1. Universal Emergency Number 9-1-1 Service[41]

The system is to be designed so that no single point of failure prevents calls from being answered.

[40] Ibid., Section 7.7.
[41] Ibid., Section 8.4.

At least two diverse calling routes are to be established to prevent a single point failure.

When a communications center has E9-1-1 services, the equipment is to be capable of receiving ANI and ALI.

11.8.2. Published Emergency Number Alternative Routing[42]

A rerouting call plan is to be included in the CEMP. Calls unable to be answered by a communications center are to be properly rerouted.

If the AHJ requires unanswered calls within a PSAP to reroute to alternative PSAP lines, the lines are to be monitored and recorded per AHJ requirements.

When a PSAP is a part-time operation, calls are to be transferred automatically. A call transfer switch may be used, but not solely relied upon as the transfer method.

If a call is not answered within 20 seconds, it is to transfer to an alternate PSAP, or be held in queue.

When held in queue, the caller is to receive a recorded message stating they have been connected to the PSAP. This is to include a TDD/TTY recorded message. The caller will be periodically reminded they are connected. There is to be a visual and audible notification within the operations room showing that unanswered calls are in queue.

11.8.3. Multiple Line Telephone Systems (MLTS)[43]

MLTS, for example PBX, must allow the caller to dial 9-1-1 without using a preceding number. MLTS are to provide information to the communications center for a return calling number. Where E9-1-1 is available, MLTS are also to provide ANI and ALI for the MLTS extension. If the facility is less than 7,000 square feet, the ALI for the extension is not required.

11.9. Chapter 9 – Dispatching Systems[44]

The dispatching system is to be designed to receive and retransmit alarms.

Transmission of trouble calls is not to interfere with receipt or transmission of alarms.

A communications center that receives less than 730 calls per year (two calls per day, average) is to have one primary dispatch circuit. When call volume is greater, the center is to have, minimally, two separate and dedicated dispatch circuits, i.e. primary and secondary. A primary dispatch circuit can be achieved through one or a combination of the methods below listed.

- Wired circuit

[42] Ibid., Section 8.5.
[43] Ibid., Section 8.6.
[44] Ibid., Chapter 9.

- Non-trunked voice radio channel
- Microwave carrier channel
- Polling or self-interrogating digital data radio channel
- Dedicated telephone circuit
- Trunked radio system

A secondary dispatch circuit path can be achieved through one or a combination of the methods below listed.

- Wired circuit
- Designated radio channel
- Approved dedicated telephone circuit

The secondary circuit path is to be received by the ERF by independent equipment than that of the primary circuit path.

11.10. Chapter 10 – Computer-Aided Dispatching (CAD) Systems[45]

When CAD systems are used, they are to contain all hardware and software to interface with the E9-1-1 system. The CAD system is to be able to interface with the CPE and receive data to populate a call-for-service data entry form.

The software is to provide data entry, resource recommendations, notification, tracking and store records for all alarms, call status, other calls of service, etc. The information is to be maintained for later analysis.

When a CAD system is used, there is to be a secondary dispatch method in the event of CAD system failure. The AHJ must put safeguards in place for preservation of operation, sustainability, and maintainability of the system.

Security for the CAD system is to be in different levels. User restrictions, by login and password, for different access capabilities dependent upon user needs are to be employed. Access to CAD hardware is to be limited to authorized personnel only, as determined by the AHJ. Network isolation to maintain bandwidth, measures to prevent denial-of-service attacks, and anti-virus software are to be employed.

CAD systems are to have the capability for alarm exchange between other CAD systems, 9-1-1 databases, and third-party systems as determined by the AHJ. When exchanging data with a third-party, an agreement is to be in place with the third-party to monitor system integrity.

The use of a CAD system does not eliminate the need for a secondary dispatch circuit.

[45] Ibid., Chapter 10.

The power for the CAD system and equipment necessary for its operations is to be supplied with electrical power through a SEPSS. The SEPSS is to maintain the critical load for 60 minutes, minimally. Both a generator and UPS are to be utilized for critical loads.

The CAD system is to be in a lighted room and legible without hindrance of glare from ambient light.

The CAD system is to support all designated printers; a spare printer is to be available. Printers used in the ERF are to be capable of printing a complete emergency message within 30 seconds.

When the CAD system is the primary or secondary dispatch means, it is to have an audible notification for alarms. A visual alarm notification is permitted as well. If a voice notification or text alert message notification is used, it is to be followed by a distinct alerting signal.

The CAD system and components are to be able to accomplish the functions listed below, minimally:

- Handle the call volume for types and sized per AHJ required parameters
- Recommend unit assignments to calls
- Ensure the optimum response units are selected
- Allow the telecommunicator the ability to override unit assignments
- Log a telecommunicator override
- Prioritize system processes making sure emergency operations take precedence
- Detect faults and failures
- Queue a notification message to a supervisor and other designated telecommunicators
- Response time no greater than 2 seconds; timed from completion of the telecommunicator message keying to a full display of system response at the position where a response is required
- Fully functional 99.95 percent of the time
- Automatic power-failure recovery capability
- Data back-up system
- Redundant capabilities where no single component failure would cause a complete system outage
- Automatic switchover upon failure of component(s) without manual intervention
- Alternate method of receiving alarms from a third-party
- Capable to continuously monitor CAD interfaces for integrity
- Spare hardware readily available; i.e. display screens, pointers, and keyboards

- On-line storage for minimally 100 days of historic data
- Wired and wireless data systems communicating at a rate of 56,000 bits per second with the ERFs and administrative sites
- Mobile units communicating with the CAD system at a rate of 9,600 bits per second
- Interface with a map display system

Mobil data computers (MDCs) and their equipment are to be manufactured for the environment in which they are intended to be used. MDCs are to maintain status of availability between the CAD and unit.

11.11. Chapter 11 – Testing

All equipment is to be restored to operating condition after each test or alarm. If the test shows system troubles, an operator is to take steps to correct the fault. If an operator cannot clear the fault, s/he is to take proper steps to isolate the fault and report it to the person responsible for maintenance.

11.11.1. Acceptance Testing[46]

New equipment and/or systems are to be supplied with operations and maintenance manuals.

New equipment is to be tested per manufacturer's specifications.

System cabling insulation is to be tested before making connections to terminals. A resistance value of 200 megohms or greater per mile between conductors and conductors and ground is to be obtained.

When radio equipment is installed or repaired, the items below are to be tested and recorded:

- Frequency
- Modulation
- Power output
- Receiver sensitivity and selectivity

11.11.2. Operational Testing[47]

Wired dispatch circuits are to be tested and recorded, minimally, once every 24 hours.

Graphic signal circuits are to be tested by sending a message transmission.

The power supply for wired dispatch circuits are to be tested and recorded, minimally, once every 24 hours. The current strength of each circuit is to be tested.

[46] Ibid., Section 11.2.
[47] Ibid., Section 11.3.

Voltage across the terminals of each circuit is to be tested as follows:

- Tested on the inside of the protective devices
- Voltage drop of greater than 10 percent is to be immediately investigated

Voltage between ground and circuits is to be tested.

Voltage tests may be supplemented by a ground current test. If the test shows a current reading greater than 5 percent of the normal line current, it is to be immediately investigated.

The voltage across the common battery terminals on the device side is to be tested. The voltage from the battery terminals to ground is to be tested. Any abnormal ground readings are to be immediately investigated.

Personnel outside alert devices (audible, telephone, radio, etc.) are to be tested as required by AHJ.

All primary and secondary radio and voice amplification circuits are to be voice tested twice daily.

PSAP emergency telephone circuits are to be tested daily.

Emergency lighting is to be tested per NFPA 101, *Life Safety Code®*, Section 7.9, which includes:

- Monthly 30 second test of the emergency and exit lighting systems
- Annual 1½ hours test of emergency and exit lighting systems

During testing, all lighting is to stay functional. Written records of the testing are to be kept.

SEPSS/UPS testing is to be per NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*.

- At least two sets of manuals are to be supplied by the manufacturer.
- Operational inspections and testing are to be performed monthly.
- Load tests are to be performed annually as well as any required monthly tests.
- Replacement of batteries is to be per manufacturer specifications, generally between three and five years.

TDD/TTY systems are to be tested daily.

Two-way radio communications equipment is to be tested, recorded, and signed once every 12 months by a person approved by AHJ.

Testing and maintenance are to be performed per NFPA 72, *National Fire Alarm and Signaling Code*.

11.11.3. Power[48]

Emergency Power Supply Systems (EPSS) and Standby Power Supply Systems (SPSS) are to be tested per NFPA 110, *Standard for Emergency and Standby Power Systems*.

A weekly discharge test, 30 minutes long, is to be performed on emergency battery power systems.

A written schedule for routine maintenance and operational testing is to be maintained.

11.12. Chapter 12 – Records

Complete records showing that dispatching systems are operational and functioning are to be maintained.

11.12.1. Installation[49]

Records for wired circuits are to include wiring schematic and/or design, office wiring diagrams, and a list of manufacturers and specifications for materials used, including the date purchased.

Records for radio channels and associated wiring are to include plans that show transmitters and receivers, interconnected office wiring diagrams, and a list of manufacturers and specifications for materials used, including the date purchased.

Changes and additions to systems are to be recorded.

Acceptance test and as-built drawings are to be maintained after installation, additions, or maintenance to the system.

Access to site-specific software systems are to be given to the AHJ, which is to maintain software records for the life of the system.

11.12.2. Training Records[50]

Training records are to be maintained for each employee, as directed by AHJ.

11.12.3. Operational Records[51]

Call and dispatch performance statistics are to be maintained.

Statistical analysis is to be completed for call and dispatch performance measurements monthly and compiled for a one-year period.

[48] Ibid., Section 11.4.
[49] Ibid., Section 12.2.
[50] Ibid., Section 12.4.
[51] Ibid., Section 12.5.

A management information system (MIS) program is to track incoming calls and dispatched alarms and provide real-time information and strategic management reports.

11.12.4. Maintenance Records[52]

Maintenance records for both routine and emergency situations are to be kept. The records are to include the date, time, nature of maintenance, repairer's name, and affiliation.

11.12.5. Retention of Records[53]

Records of installation, changes, additions, as-built drawings, acceptance testing, operational records and maintenance records are to be maintained for the life of the equipment.

Records for operating procedures, recording, operational testing, and other operational records are to be kept for two years, or as required by law or the AHJ.

When call detail reporting is used, records are to be maintained for two years or as required by law or the AHJ.

11.13. Chapter 13 – Data Security[54]

A communications center is to develop, implement, and utilize a comprehensive, defense, in-depth process and plan to ensure total data security. The plan is to include and/or accomplish the items listed below.

- A policy statement outlining the AHJ's requirements and goals of the plan is to be included in the plan.
- Responsibilities are to be assigned to personnel for completion of the plans tasks.
- The plan is to specify training and education requirements for personnel to complete tasks, and is to have a continuing education component.
- The EOC is to control access, with varying access levels, of personnel into critical operation areas.
- Network security systems are to be implemented.
- A computer security system is to be installed to prevent attacks on the EOC's computers and servers.
- Software patch management is to be implemented to ensure that all software is periodically updated.
- The AHJ is to implement a data disaster recovery procedure.
- The communications center is to implement logging and auditing provisions to allow for investigation of security or operational problems.

[52] Ibid., Section 12.6.
[53] Ibid., Section 12.7.
[54] Ibid., Chapter 13.

- A vulnerability management process is to be implemented to access periodically the ability of the public safety communications systems, including communication centers, wireless networks, and wired IT networks.
- The EOC is to implement environmental and physical security of the facility systems, such as entry, smoke or fire, power, and radio performance.

The plan is to have methods, procedures, and schedules for testing the system. The data system testing frequency will be determined by the AHJ.

11.14. Chapter 14 – Public Alerting Systems[55]

Public alerting systems (PASs) are to meet the requirements listed below.

- All components are to meet federal, state, and local rules and regulations.
- An SOP is to be developed by the AHJ.
- A PAS that is developed to work with a communications network is to be engineered to work within the network's capacity.
- PASs that are designed to give non-emergency messaging are to be designed to give priority to emergency alerts.
- An upgrade to PAS is to be backward-compatible with existing systems.
- The AHJ is to develop and enforce security procedures for use of the PAS. The procedures are to be consistent with federal, state, and local laws.
- PASs are to be used for natural and man-made events that may result in loss of life, property, or endanger public health.
- Types of permitted PASs include:
  - Automated voice dial-out
  - Automated signal dial-out, with use of PAS alerting appliances (PASAAs)
  - Radio broadcast and tone-alert, with use of PASSAs
  - Wireless, with use of PASSAs
  - Paging, with use of PASSAs
  - Siren and loud-speaker
  - Integrated Public Alert and Warning System (IPAWS)

PASAAs are to meet the following capabilities:

- Receive an alert data message (ADM) from PAS
- Provide an audible alert as defined by NFPA 72, *National Fire Alarm and Signaling Code*

[55] Ibid., Chapter 14.

- Provide a red, clear, amber, or blue flashing light visual alert signal in response to an ADM
- Provide a local trouble signal for a low-battery condition; lighting color used by other signal purposes is not to be used

11.15. Annexes

NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, includes several annexes that provide explanatory material, memorandum, guidelines, and references. A listing of the annexes in order of appearance is below.

- Annex A – Explanatory Material
- Annex B – Frequency-Sharing Memorandum of Understanding
- Annex C – Planning Guidelines for Universal Emergency Number (9-1-1) Service
- Annex D – Computer-Aided Dispatching (CAD) systems
- Annex E – Cybersecurity
- Annex F – Informational References

This page intentionally left blank.