The National 911 Program

Next Generation 911 (NG911) Standards Identification and Review

A compilation of existing and planned standards for NG911 systems

Washington, DC
August 2020

DOCUMENT CHANGE HISTORY

The table below details the change history of this Standards Identification and Review document.

Version	Publication Date	Description
1.0	September 21, 2011	Initial Release
2.0	September 7, 2012	Updated Standards
3.0	January 8, 2014	Routine Revision / Updated Standards
4.0	March 4, 2015	Routine Revision / Updated Standards
5.0	March 2016	Routine Revision / Updated Standards
6.0	March 2017	Routine Revision / Updated Standards
7.0	April 2018	Routine Revision / Updated Standards
8.0	October 2019	Routine Revision / Updated Standards
9.0	August 2020	Routine Revision / Updated Standards

Table of Contents

Introduction

One of the most critical aspects of transforming the nation's 911 public safety answering points (PSAPs) from today's legacy 911 technology to Next Generation 911 (NG911) is adherence to a common set of standards. Development and adoption of international standards are key to achieving 911 interoperability across multiple local, regional, state, and national public safety jurisdictions, and beyond into the global emergency communications environment. Based on conceptual definitions dating from 2000, development began on NG911 standards in 2003 when the National Emergency Number Association (NENA) initiated technical requirements and definition work on core Internet Protocol (IP) functionality and architecture.

Beyond the walls of the 911 PSAPs, the consistent observance of standards is essential in accomplishing seamless transmission of data from the caller to 911, and on to emergency responders. As PSAPs expand the forms of data they receive and transmit to each other, and as emergency responders migrate to a broadband network (e.g., FirstNet), it is essential that standards are established and consistently adopted.

A variety of standards already exist, and many are actively under development. However, there is limited coordination across the broad NG911 community regarding what completed standards are available, what standards overlap, and what standards still need to be established. The National 911 Program, led by the United States (U.S.) Department of Transportation (USDOT), National Highway Traffic Safety Administration (NHTSA), has compiled this list of standards activities related to NG911. The standards development organizations (SDOs) mentioned herein were given the opportunity to vet the contents of this document, to assess the status of specific standards. This s a living document, and the National 911 Program will monitor and publish[1] the activities of SDOs in establishing a comprehensive set of standards for NG911.

The hyperlinks to the standards identified in this document, unless otherwise noted, were verified in August 2020.

Input from the standards community and NG911 stakeholders at large is encouraged and appreciated. The National 911 Program can be reached at (202) 366-3485 or via email at: nhtsa.national911@dot.gov.

[1] Available through the National 911 Program at: http://www.911.gov

What Is a Standard?

The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Guide 2:2004, definition 3.2, defines a standard as a[2]—

> ***document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context***

Standards affect the daily lives of everyone across the nation. From the most mundane aspects of life (e.g., electrical cords and wall sockets) to potentially life and death situations (e.g., the concentration of ingredients in generic medications), standards guide the quality, safety, and security of products or processes. Standards are widely used throughout the U.S. government and public and private sectors.

Standards can be *voluntary*—by themselves imposing no requirement regarding use—or *mandatory*. Generally, a mandatory standard is published as part of a code, rule, or regulation by a regulatory government body and imposes an obligation on specified parties to conform to it. However, the distinction between these two categories may be lost when voluntary consensus standards are referenced in government regulations, effectively making them mandatory standards.[3] Most standards are ***voluntary, consensus-based***, and ***open***: [4]

- Voluntary—Use of the standard is not mandated by law
- Consensus-based—Published standards have attained general agreement through cooperation and compromise in a process that is inclusive of all interested parties
- Open—Standards are not proprietary and are available for anyone to use

A standard may be or contain intellectual property such as patents, and the intellectual property rights (IPR) may still be held by a company. The American National Standards Institute (ANSI) essential elements state this about patents in ANSI standards:

[2] International Organization for Standardization (ISO), *ISO/IEC Directives, Part 2:2016, Principles and rules for the structure and drafting of ISO and EIC documents.* Available at: http://www.iec.ch/members_experts/refdocs/iec/isoiecdir-2%7Bed7.0%7Den.pdf

[3] National Institute of Standards and Technology, *The ABC's of Standards Activities.* Available at: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=903219

[4] Research and Innovation Technology Administration (RITA) Intelligent Transport Systems (ITS), *What Are Standards?* Available at: http://www.standards.its.dot.gov/LearnAboutStandards/ITSStandardsBackground

The ASD shall receive from the patent holder or a party authorized to make assurances on its behalf, in written or electronic form, either:
a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of implementing the standard either:
i) under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
ii) without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.[5]

What Are Best Practices?

Typically, less formal than standards, best practices are methods or techniques that have been identified as the most effective, efficient, and practical means to achieve an objective. Based on a repeatable process, best practices often emerge as the result of generally accepted principles followed by many individuals, groups, or organizations, which have been established over time. Best practices often supplement the standards process and act as common guidelines for policies and operations.

Stakeholders

Stakeholders in standardization encompass all groups that have an interest in a particular standard because those groups are likely to be most affected by changes and, therefore, want to contribute to the development process. NG911 stakeholders are members of a broad and diverse community of users who generally can be categorized as follows:

- 911 and public safety agencies and authorities
- Vendor community (including hardware and software) and related industries
- Technology, services, and consulting industries
- SDOs and standards setting organizations (SSOs)
- Consumer, research, academic, and consortia communities
- Telematics, third-party call centers, Internet, infrastructure, wireline, and wireless service providers
- Transportation agencies
- Local, state, and federal governments

[5] American National Standards Institute (ANSI), *ANSI Essential Requirements: Due process requirements for American National Standards*, January 2020. Available at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2020_ANSI_Essential_Requirements.pdf

- Regulatory agencies and public utility commissions
- Professional and trade associations
- The public at large[6]

Standards Organizations

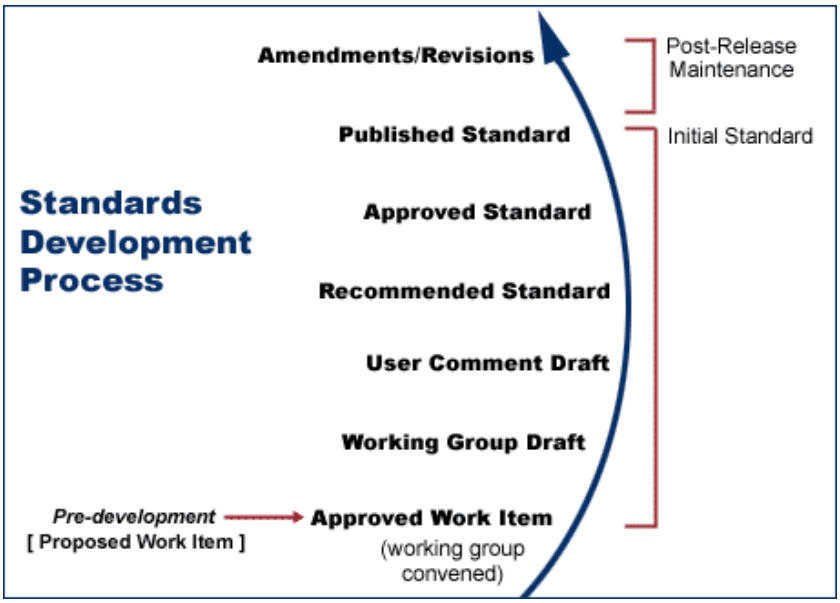
Standards organizations are bodies, organizations, and institutions whose focus is developing and maintaining standards in the interest of a user community. These organizations can be governmental, quasi-governmental, and non-governmental.[7] Typically, their mandate is geographically oriented—international, regional, or national. Organizations that establish, review, and maintain standards are considered to be SDOs,[8] although consortia are sometimes differentiated as SSOs. Generally speaking, SDOs and SSOs consistently adhere to a set of requirements or procedures that govern the standards development process.

How Are Standards Developed?

At the heart of the U.S. standards system are voluntary standards that arise from a formal, coordinated, consensus-based, and open process. Developed by subject matter experts from both the public and private sectors, the voluntary process is open to all affected parties and relies on cooperation and compromise among a diverse range of stakeholders. Organizations also work together to develop joint standards, which forge relationships and allow for a collaborative and cooperative effort. Joint standards will be especially important with respect to the synergistic environment of emergency communications, such as the environment shared by the Nationwide Public Safety Broadband Network (NPSBN) and NG911.

Although the development process may vary to some extent from organization to organization, fundamentally each organization has an established set of formally documented procedures for initiating, developing, reviewing, approving, and maintaining standards. As an example, the following diagram illustrates the USDOT Research and Innovative Technology Administration (RITA) Intelligent Transportation Systems (ITS) standards development process:[9]

[6] Although it is generally accepted that the public is an NG911 stakeholder (as the primary 911 call originator), typically, any involvement with the standards process occurs only when they participate as part of another stakeholder group.
[7] Quasi- and non-governmental standards organizations are often non-profit organizations.
[8] Standards Development Organization or Standard Developing Organization.
[9] Intelligent Transportation Systems Joint Program Office, *Standards Development Process.* http://www.standards.its.dot.gov/LearnAboutStandards/StandardsDevelopment



The Institute of Electrical and Electronics Engineers (IEEE) emphasizes that standards "are 'living documents', which may initially be published and iteratively modified, corrected, adjusted and/or updated based on market conditions and other factors."[10] Given that standards development is an iterative process, often there are procedures for publishing draft and/or interim documents at different stages in the process prior to formal approval. Once approved, various factors can render standards outdated, including technological advancements and new or revised requirements. ANSI advises periodic maintenance "by review of the entire document and action to revise or reaffirm it on a schedule not to exceed five years from the date of its approval as an American National Standard."[11]

What Is Standards Accreditation?

Typically, process accreditation bodies do not develop standards but instead provide accreditation services for the purpose of assessing and certifying the standards development process of other SDOs. For example, ANSI facilitates development of American National Standards (ANS) by accrediting the procedures of SDOs. Accreditation by ANSI signifies that the procedures used by the standards body, in connection with the development of ANS, meet the Institute's essential requirements for openness, balance, consensus, and due process.[12] Given the voluntary nature of standards, SDOs are not mandated to attain accreditation. However, accreditation does demonstrate adherence and conformity with a formal and recognized standards development

[10] Institute of Electrical and Electronics Engineers (IEEE) Volunteer Training Program, *How are Standards Made?* Available at: http://standards.ieee.org/develop/process.html

[11] ANSI, *ANSI Essential Requirements: Due process requirements for American National Standards*, January 2020. Available at: https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2020_ANSI_Essential_Requirements.pdf

[12] ANSI Standards Activities, *Domestic Programs (American National Standards) Overview.* Available at: http://www.ansi.org/standards_activities/domestic_programs/overview.aspx

process. Given the expense and time involved, not all SDOs pursue accreditation, although they are still likely to adhere to a similarly rigorous standards development process.

Types of Standards

The standards referenced within this document, generally are within one of the one of the six categories shown below:

- **Product Standard—**Describes the expectations and minimum requirements for a particular product, typically in the context of a specific use. Product standards would most often be reflected in descriptions of hardware, software, and other technology solutions.
- **Interface Standard—**Describes the requirements for connecting two or more systems, or technologies, to one another. User interface standards would describe the interconnection between a human and a machine.
- **Data Standard—**Describes the definition, format, layout, and other characteristics of data stored within a system or shared across systems. Data standards help to ensure the seamless exchange of data between disparate systems and permit a common understanding to interpret and use data consistently.
- **Test Standard—**Describes the test methodologies, processes, and other requirements associated with determining the performance or fitness of a particular product.
- **Performance Standard—**Describes how a product or service should function, often in terms of quality, quantity, or timeliness.
- **Operational Standard—**Describes how a function or business process should occur, setting minimum requirements for performance or delivery. Operational standards could include standard operating procedures (SOPs), training guidelines, and policies.

The first three categories (product, interface, and data) are primarily design standards that describe how a product should be developed and define the particular attributes or characteristics associated with its construction. Alternately, performance standards describe how a product should function and how testing should be used to determine that it meets all affirmed requirements.

How to use this Standards Document

This document is intended to be a comprehensive list of standards that are relative to NG911. Older standards are included if they are still relevant through the transition phase from legacy to NG911. Readers are advised that if more information on a standard is needed, then they should consult the standards development organization itself.

The language describing the purpose of the SDOs and their relevant standards has come from the organization's descriptions and standards websites themselves. This document does not serve to promote or endorse any SDO or resource.

The Need for Standards in NG911

It is imperative that the essential NG911-related standards and technology are established and available for 911 Authorities and PSAPs to support transitioning to an open, non-proprietary NG911 system. Without standards and technologies in place, service and equipment providers may develop new, vendor-specific solutions. This unstandardized, unplanned approach can and will affect the ability of PSAPs and emergency response entities to effectively share information and be interoperable. Further, without critical processes and protocols (e.g., certification and authentication, routing business rules, and best practices), the benefits of the NG911 system, including routing based on criteria beyond location, and connection of service providers beyond common service providers to the 911 system, may not be realized. The appropriate use of standards will ensure the compatibility and interoperability required to realize the full potential of NG911.

Standards Affecting NG911

It is important to identify, understand, and actively monitor those standards that are most likely to have a significant impact on the implementation of NG911. This is consistent with the National Technology Transfer and Advancement Act of 1995[13], which directs government agencies to use "voluntary consensus standards" created by SDOs. Specifically, it instructs federal agencies, such as USDOT, to participate in the standards development process so that these organizations remain aware of USDOT's position on relevant standards. This involvement is expected to influence overall development, thus ensuring that the resulting standard is appropriate for use by federal agencies.

The specific standards identified in this document are limited to those most directly germane to NG911. For example, numerous technical standards are associated with the existing access and originating networks. However, this document undertakes to highlight only those relating to the changes required to support the enhanced capability, such as emergency call support provisioning, between the assortment of client devices and Emergency Services IP networks (ESInets). Standards involving network interfaces, including Voice over Packet (VoP), Voice over Internet Protocol (VoIP), or Voice over Digital Subscriber Line (VoDSL), although critical to the end-to-end architecture, are too detailed and non-specific to NG911 for inclusion.

What's New in Standards

Standards and best practices are ever changing to adapt to the evolving environment. This section is not all inclusive; so it is recommended that users review any document listed before using it and should review each document already in use for updates.

The following SDOs have released and/or revised standards since this publication was released on July 1, 2019. The new/revised standards are identified in the table (gray boxes) contained in each SDO description.

- 3rd Generation Partnership Project (3GPP)

[13] National Technology Transfer and Advancement Act of 1995, P.L. 104-113. Available at: http://www.nist.gov/standardsgov/nttaa-act.cfm.

- Alliance for Telecommunications Industry Solutions (ATIS)
- Association of Public-Safety Communication Officials (APCO)
- Building Industries Consulting Service International (BICSI)
- Department of Commerce (DOC)
- European Telecommunications Standards Institute (ETSI)
- Information Security Forum (ISF)
- Information Sharing and Analysis Organizations (ISAO)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization of Standardization (ISO)
- International Telecommunications Union (ITU)
- Internet Engineering Task Force (IETF)
- ISACA®
- National Information Exchange Model (NIEM)
- North American Electric Reliability Corporation (NERC)
- Open Geospatial Consortium (OGC®)
- Society of Cable Telecommunications and Engineers (SCTE)
- Telecommunications Industry Association (TIA)

Standards and Best Practices Organizations

This section identifies the work performed and currently underway by professional organizations and SDOs involved with the requirements and specifications pertaining to the implementation of NG911. For each, the purpose of the organization and pertinent standards and/or best practices are provided. This information provides perspective on the involvement of 911 within the broader world of emergency response and public safety.

For a more detailed look at individual standards, see below.

3rd Generation Partnership Project (3GPP)

Name 3rd Generation Partnership Project (3GPP)

Type International Standards Organization—Industry (Mobile Broadband/Universal Mobile Telecommunications System [UMTS])

Purpose 3GPP brings seven telecommunications SDOs together—Association of Radio Industries and Businesses (ARIB); Alliance for Telecommunications Industry Solutions (ATIS); China Communications Standards Association (CCSA); European Telecommunications Standards Institute (ETSI); Telecommunications Standards Development Society, India (TSDSI); Telecommunications Technology Association, Korea (TTA); and Telecommunication Technology Committee, Japan (TTC) —referred to as "organizational partners." 3GPP provides its members with an environment to produce the reports and specifications that define 3GPP technologies.

Website http://www.3gpp.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
3GPP TSG SA Release 16	*Release 16*	Provides information on 5G phase 2 and prepares the groundwork for IMT-2020	Version 0.4.0 (2020-03)
3GPP TS 23.228	*IP Multimedia Subsystem (IMS); Stage 2*	Describes the stage-2 service for the IP Multimedia Core Network Subsystem (IMS), which includes the elements necessary to support IP Multimedia (IM) services.	Version 16.4.0 (2020-03)
3GPP TS 24.229	*IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*	Describes the call control protocol for use in the IM Core Network (CN) subsystem based on the SIP and the associated SDP.	Version 16.5.0 (2020-03)

Document ID	Document Title	Document Description	Latest Revision/ Release Date
3GPP TS 29.010	*Information element mapping between Mobile Station - Base Station System (MS - BSS) and Base Station System - Mobile-services Switching Centre (BSS - MSC); Signaling Procedures and the Mobile Application Part (MAP)*	Provides specifications for the interworking between information elements contained in layer 3 messages sent on the MS-MSC interface where the MSC acts as a transparent relay of information; provides specifications for the interworking between information elements contained in BSSMAP messages sent on the BSC-MSC interface and parameters contained in MAP services sent over the MSC-VLR interface where the MSC acts as a transparent relay of information.	Version 15.1.0 (2018-12)
3GPP TSG SA Release 12	Release 12	Focuses on the use of LTE technology for emergency and security services, with technical specifications for mission-critical application layer functional elements and interfaces.	March 2015
3GPP TSG SA Release 13	Release 13	Provides specifications for public safety and mission critical communications, explores Wi-Fi integration and system capacity and stability.	January 2016
3GPP TSG SA Release 14	Release 14	Describes LTE support for V2x services, eLAA, 4 band carrier aggregation, and inter-band carrier aggregation.	March 2017
3GPP TSG SA Release 15	Release 15	Provides information on 5G-Phase 1 as well as LTE-Advanced Pro specifications.	December 2018

Document ID	Document Title	Document Description	Latest Revision/ Release Date
3GPP TS 23.167	*IP Multimedia Subsystem (IMS) emergency sessions*	Describes the stage 2 service for emergency services in the IP Multimedia Core Network Subsystem (IMS), including the elements necessary to support IP Multimedia (IM) emergency services and IM emergency services for eCall.	Version 16.1 (2019-12)
3GPP TS 23.517	*TISPAN; IP Multimedia Subsystem (IMS); Functional architecture*	Describes the IMS core component of the TISPAN NGN functional architecture and its relationships to other subsystems and components.	Version 8.0.0 (2007-12)

Alliance for Telecommunications Industry Solutions (ATIS)

Name Alliance for Telecommunications Industry Solutions (ATIS)

Type Standards-Setting Organization—Industry (Telecommunications) (ANSI)

Purpose ATIS develops technical and operational standards for the information and communications technology (ICT) industry.

Website http://www.atis.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0700025.v002	*Wireless Emergency Alert (WEA) International Roaming Specification*	Provides the requirements for presentation of emergency alerts when U.S. and Canadian users are roaming throughout the U.S. and Canada, when U.S. and Canadian users roam elsewhere in the world where 3GPP PWS-based alerting is supported, and when international roamers from beyond North America roam into North America with a 3GPP PWS-capable mobile device.	February 2020
ATIS 0700015.V004	*ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*	Identifies and adapts 3GPP common IMS emergency procedures for applicability in North America to support emergency communications originating from an IMS subscriber.	July 2018
ATIS-0100022.2008(S2018)	*Priority Classification Levels for Next Generation Networks*	Formalizes a set of priority classification levels for admission control and service restoration in NGNs; highest priority classifications are reserved for ETS.	December 2008

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0300104(2019-10)	*Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document - NGN Basics, Emergency Services, NGN Testing, and Network Survivability*	Provides basic information regarding NGNs, as applicable to the NGIIF.	October 2019
ATIS-0300116(2019-10)	*Interoperability Standards between Next Generation Networks (NGN) for Signature-based Handling of Asserted information using ToKENs (SHAKEN)*	Provides NGN telephone service providers (SPs) with a framework and guidance for interoperability as calls process through their networks implementing Signature-based Handling of Asserted information using ToKENs (SHAKEN) technologies to ensure the validation as well as the completion of legitimate calls and the mitigation of illegitimate spoofing of telephone identities.	October 2019
ATIS-0500001	*High Level Requirements for Accuracy Testing Methodologies*	Provides a common frame of reference that stakeholders can use to validate the accuracy methodology of 911 location technologies and whether test equipment meets requirements.	November 2011
ATIS-0500003	*Routing Number Authority (RNA) for pseudo Automatic Number Identification Codes (pANIs) Used for Routing Emergency Calls: pANI Assignment Guidelines and Procedures*	Contains the guidelines and procedures for the assignment and use of pANIs used to route emergency calls, such as E911 calls or other types of emergency calls that need to become native E911 calls throughout the North American E911 systems (U.S. and Canada).	July 2005
ATIS-0500004	*Recommendation for the Use of Confidence and Uncertainty for Wireless Phase II*	Contains ESIF recommendation for managing location confidence and uncertainty for wireless Phase 2 calls.	August 2005

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0500005	*Standard Wireless Text Message Case Matrix*	Addresses the need for standard wireless text messages; some PSAP screen formats provide space ALI text messages and the text messages are used to alert the call taker of a unique condition.	September 2005
ATIS-0500008	*Emergency Services Network Interfaces (ESNI) Framework*	Defines the framework and structure of the ESNI suite of standards; includes the ESMI that provides interconnections between next generation PSAPs and the ESNet.	October 2008
ATIS-0500009	*High Level Requirements for End-to-End Functional Testing*	Establishes procedures/standards to test that delivery of wireless 911 data remains constant through the network and is delivered with integrity to the PSAP.	April 2006
ATIS-0500013	*Approaches to Wireless E9-1-1 Indoor Location Performance Testing*	Provides recommendations for indoor wireless testing methodologies and validation.	February 2010
ATIS-0500017	*Considerations for an Emergency Services Next Generation Network (ES-NGN)*	Defines an emergency services architecture based upon the ATIS definition of an ES-NGN; identifies potential standards gaps and focuses on the interconnection between the ES-NGN and networks that originate emergency calls.	June 2009
ATIS-0500018	*p-ANI Allocation Tables for ESQKs, ESRKs, and ESRDs*	Contains ESQK, ESRK, and ESRD allocation tables and capacities; assists Wireless Service Providers (WSPs) and Mobile Positioning Centers (MPCs) in improving the efficacy of p-ANI number use and administration, and complement preservation and utilization of limited p-ANI number resources.	August 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0500019.2010(R2015)	*Request for Assistance Interface (RFAI) Specification*	Defines/describes the RFAI between the ES-NGN and a PSAP.	September 2010
ATIS-0500021	*Supplemental Location Data*	Contains standards for including supplemental location data to the ALI database from technologies providing indoor radio frequency (RF) coverage requiring a small signal footprint.	October 2012
ATIS-0500022	*Test Plan Input for a Location Technology Test Bed*	Leverages earlier standards and methods to provide a broad baseline test plan document for wireless indoor location accuracy testing.	October 2012
ATIS-0500023	*Applying Common IMS to NG9-1-1 Networks*	Provides the stage 1 definition for an IMS-based next generation emergency services architecture based on the 3GPP IMS standards.	April 2013
ATIS-0500024	*Comparison of SIP Profiles*	Compares SIP profiles defined by ATIS, 3GPP, and NENA as they relate to emergency services.	April 2013
ATIS-0500025	*Class of Service Support for Semi-Static Wireless*	Addresses E911 Class of Service associated with a small cell that has a less than 100 meter coverage in an indoor environment.	July 2013
ATIS-0500026	*Operational Impacts on Public Safety of ATIS-0700015, Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*	Explains the IP to NG911 interfaces, without overdependence on technical terms and acronyms, to assist public safety in understanding the operational impact from future IMS-originated emergency calls.	September 2014
ATIS-0500027	*Recommendations for Establishing Wide Scale Indoor Location Performance*	Provides the methodology to characterize wide-scale indoor location accuracy performance by creating regional test beds and extrapolating their test results.	May 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0500028	*Analysis of Unwanted User Service Interactions with NG9-1-1 Capabilities*	Illustrates use cases that convey the need for a broader analysis of standardized user service definitions for possible interactions with NG911 capabilities and identification of which interactions could lead to unwanted behavior.	February 2015
ATIS-0500030	*Guidelines for Testing Barometric Pressure-Based Z-Axis Solutions*	Provides broad guidelines for testing barometric pressure-based altitude (z-axis) measurement systems, which are being proposed to enable more accurate and more actionable indoor wireless 911 location.	May 2016
ATIS-0500031.v002	*Test Bed and Monitoring Regions Definition and Methodology*	Describes and provides the technical details of the approach of characterizing wide scale indoor wireless location performance, for the purposes of E911, through representative testing in a test bed and subsequently applying its results to live wireless network emergency call statistics gathered from a number of diverse monitoring regions.	February 2017
ATIS-0500032	*ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture*	Defines the Stage 2 (architecture) and Stage 3 (protocol) specifications for an IMS-based NG911 Service Architecture. This Standard includes the architecture, functional elements, call flows, protocols, and interfaces which were derived from the Stage 1 requirements in ATIS-0500023, "Applying Common IMS to NG9-1-1 Networks."	November 2016

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0700028.V002	*Location Accuracy Improvements for Emergency Calls*	This Standard specifies the requirements, architecture, and interfaces required to support the commitments defined in the roadmap described above as well as the rules as outlined within the FCC CFR.	January 2019
ATIS-1000010.2006(S2016)	*Support of Emergency Telecommunications Service (ETS) in IP Network*	Defines the procedures and capabilities required to support ETS within and between IP-based service provider networks.	June 2006
ATIS-1000012.2006 (S2016)	*Signaling System No. 7 (SS7) – SS7 Network and NNI Interconnection Security Requirements and Guidelines*	Provides security requirements and guidelines for SS7 network and its network interconnections.	November 2006
ATIS-1000019.2007 (S2017)	*Network to Network Interface (NNI) Standard for Signaling and Control Security for Evolving VoP Multimedia Networks*	Specifies VoP and multimedia signaling and control plane security requirements for evolving networks.	March 2007
ATIS-1000026.2008 (S2018)	*Session Border Controller Functions and Requirements*	Provides information on the Session Border Controller (SBC) functions and requirements that reside within a service provider's network.	April 2008
ATIS-1000029.2008 (S2018)	*Security Requirements for NGN*	Provides security requirements for the NGN against security threats, and to mitigate the effects of security attacks.	November 2008
ATIS-1000034.2010(S2020)	*Next Generation Network (NGN): Security Mechanisms and Procedures*	Describes some security mechanisms that can be used to fulfill the requirements described in ATIS-1000029.2008 and specifies the suite of options for each selected mechanism.	November 2010

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-1000038	*Technical Parameters for IP Network to Network Interconnection Release 1.0*	Explains the "Interconnection Technical Parameters" that need to be collected and eventually exchanged between two service providers so that they can successfully interconnect IP-based facilities and VoIP services at an NNI.	August 2010
ATIS-1000040	*Protocol Suite Profile for IP Network to Network Interconnection Release 1.0*	Identifies a set of protocols and specifies their profile so that signaling, media, and network related parameters can be uniformly and consistently utilized across the interconnection interface; supports a service seamlessly across an IP network to network interconnection as identified by the test scenarios defined in ATIS-1000041.	August 2010
ATIS-1000041	*Test Suites for IP Network to Network Interconnection Release 1.0*	Specifies a set of call test scenarios involving SIP and other signaling messages which for various situations may be required to provide an expected reaction to an event or a sequence of events appropriate to the previously signaled message; "expected reaction" is based upon the protocol profile established in the messages that flow across the NNI.	August 2010
ATIS-1000049	*End-to-End NGN GETS Call Flows*	Describes end-to-end call/session flows for various wireline and wireless access technologies, in addition to the IMS Core Network call/session flows in support of NGN Government Emergency Telecommunications Service (GETS).	August 2011

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-1000055.2013 (R2018)	*Emergency Telecommunications Service (ETS): Core Network Security Requirements*	Provides a set of common (i.e., independent of network type or technology) and core network security requirements for the protection of ETS in a multi-provider NGN environment.	August 2013
ATIS 1000060.2014 (R2019)	*Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services*	Provides a set of requirements for the security protection of NS/EP NGN-PS in LTE access networks.	October 2014
ATIS-1000061.2015(R2020)	*LTE Access Class 14 for National Security and Emergency Preparedness (NS/EP) Communications*	Provides operational guidance regarding the assignment and use of the 3GPP LTE specifications for Access Class Barring to support NS/EP NGN-PS.	February 2015
ATIS-1000065.2015(R2020)	*Emergency Telecommunications Service (ETS) Evolved Packet Core (EPC) Network Element Requirements*	Specifies ETS requirements for an EPS consisting of the E-UTRAN and EPC for support of NGN GETS voice, NGN GETS video, NGN GETS Guaranteed Bit Rate (GBR) data, and NGN GETS data transport.	February 2015
ATIS-1000066.2016	*Emergency Telecommunications Service (ETS) Network Element Requirements for IMS-based Next Generation Network (NGN) Phase 2*	Specifies ETS requirements for an IP Multimedia Subsystem (IMS) Core Network for support of NGN GETS Voice and NGN GETS Video.	October 2016
ATIS-1000067.2015(R2020)	*IP NGN Enhanced Calling Name (eCNAM)*	Defines a Calling Name Delivery service in the IP-based NGN.	August 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-1000678.v3.2015(R2020)	*Lawfully Authorized Electronic Surveillance (LAES) for Voice over Internet Protocol in Wireline Telecommunications Networks, Version 3*	This document provides the mechanisms and the interfaces between a Telecommunication Service Provider (TSP) and a Law Enforcement Agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance for VoIP in Wireline Telecommunications Networks.	July 2015
ATIS-1000679.2015(R2020)	*Interworking between Session Initiation Protocol (SIP) and ISDN User Part*	Provides information on the signaling interworking between the ISDN User Part (ISUP) protocol and SIP in order to support services that can be commonly supported by ISUP and SIP based network domains.	April 2015
ATIS-1000068	*Support of TTY Service over IP Using Global Text Telephony*	Describes the means that the TTY service can be provided over IP between operator's networks through the use of the Global Text Telephony (GTT) capability which enables simultaneous audio and/or video with text media stream.	August 2017
ATIS-1000071	*Technical Report on a Nationwide Number Portability Study*	Outlines the characteristics of the current U.S. local number portability implementation based on use of the Location Routing Number (LRN) method and explores different approaches for implementing Nationwide Number Portability (NNP) and their impacts.	July 2016
ATIS-1000072	*Analysis of Mitigation Techniques for Calling Party Spoofing*	Provides a Technical Report on Originating Party Spoofing in Internet Protocol (IP) Communication Networks.	September 2016

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0700039	*Guidelines for Emergency Call Location Selection and Reporting by Originating Networks*	Provides a roadmap for technology changes that was submitted to the FCC in response to an FCC initiative (proceeding 07-114) to provide a number of improvements to emergency location capabilities including providing a dispatchable location for emergency calls to PSAPs.	May 2018
ATIS-0500036	*ATIS Standard for IMS-based Next Generation Emergency Services Network Interconnection*	Defines the Stage 2 (architecture) and Stage 3 (protocol) specifications for the interconnection of an IMS-based NG911 Emergency Services Network with legacy and other NG911 Emergency Services Networks for initial emergency call origination and call transfers (bridging).	July 2018
ATIS-0500037	*Overview of how an IMS Originating Network interfaces to an E9-1-1 or NG9-1-1 System*	Provides an overview of ATIS-0700015.v003, Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination, that may aid Public Safety in understanding the application of this standard as it relates to the migration to NG911.	June 2018
ATIS-0500033	*Overview and Operational Considerations for an IMS-based Next Generation 9-1-1 (NG9-1-1) Service Architecture based on ATIS-0500032*	Provides an overview and operational consideration for an IMS-based NG911 Service Architecture based upon ATIS-0500032, *ATIS Standard for Implementation of an IMS-based NG9-1-1 Service Architecture*.	February 2017

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ATIS-0500034.v002	*Comparison of Enhanced 9-1-1 (E9-1-1) and Next Generation 9-1-1 (NG9-1-1) Focused on Reportable Outage Data Points*	Compares the ability to detect failures/outages associated with emergency calls in an E911 environment versus a transitional and end-state NG911 environment.	August 2019
ATIS J-STD-036-C-2	*Addendum to J-STD-036-C, Enhanced Wireless 9-1-1 Phase II*	Enables an MPC and PDE to assign appropriate COS when delivering data to a PSAP.	June 2017
J-STD-110.01.v002	*Joint ATIS/TIA Implementation Guideline for J-STD-110, Joint ATIS/TIA Native SMS/MMS to 9-1-1 Requirements and Architecture Specification, Release 2*	Addresses CMSP and TCC provider deployment considerations of J-STD-110.v002.	May 2015

Association of Public-Safety Communications Officials (APCO)

Name Association of Public-Safety Communications Officials-International (APCO)

Type National Standards Organization (ANSI-accredited)

Purpose APCO develops standards and disseminates information about public safety communication issues—such as wireless 911, staffing and retention, and the impact of emerging technologies—and participates in committees, partnerships, and government initiatives.

Website http://www.apcointl.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO 1.120.1-20xx	*Crisis Intervention Techniques and Call Handling Procedures for Public Safety Telecommunicators*	Identifies requirements for handling calls involving emotionally distressed individuals.	In Development
APCO 1.121.1-20xx	*Managing Operational Overload in the Public Safety Communications Center*	Document will provide best practices for planning, mitigating and handling operational overload.	In Development
APCO 3.112.1-20xx	*Detecting Early Warning Symptoms of Stress in Public Safety Telecommunicators*	Details key performance indicators (KPIs) as they relate to personnel performance measurements, accuracy and quality of information logged or provided by communications center personnel.	In Development
APCO 1.119.1-20xx	*Public Safety Telecommunicator Critical Incident Stress Debriefing (CISD) Program*	Provides the requirements for a Critical Incident Stress Debriefing (CISD) program specifically geared towards identifying and assisting Public Safety Telecommunicators.	In Development

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO 1.108.1-2018	*Minimum Operational Standards for the Use of TTY/TDD devices in the Public Safety Communications Center*	Defines the minimum operational standards for the use of TTY/TDD devices in a PSAP.	Version 1 August 13, 2018
APCO 1.113.1-2019	*Public Safety Communications Incident Handling Process*	Provides best practices for call handling in the PSAP.	Version 1 January 9, 2019 (Version 2 in Development)
APCO 1.117.1-2019	*Public Safety Communications Center Key Performance Indicators*	Provides KPI inherent in all ECC work, regardless of size, services, or location; provides a list of conditions that allow agencies to further refine performance analysis and management.	Version 1 October 10, 2019
APCO 1.118.1-201x	*Key Performance Indicators for Public Safety Communications Personnel*	Provides KPIs as they relate to personnel performance measurements, accuracy and quality of information.	In Development
APCO 2.102.1.201x	*Advanced Automatic Collision Notification (AACN) Data Set*	Describes and outlines the AACN data set.	In Development
APCO 3.110.1-2019	*Cybersecurity Training for Public Safety Communications Personnel*	Provides guidance and direction in developing cyber security training programs.	Version 1 December 27, 2019
APCO ANS 1.101.3-2015	*Standard for Public Safety Telecommunicators When Responding to Calls of Missing, Abducted and Sexually Exploited Children*	Details the response process for missing, abducted, and/or sexually exploited children.	Version 3 January 8, 2015 (Version 4 in Development)
APCO ANS 1.110.1-2015	*Multi-Functional Multi-Discipline Computer Aided Dispatch (CAD) Minimum Functional Requirements*	Provides functional requirements that a CAD system shall include.	Version 1 January 9, 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO ANS 1.111.2-2018	*Public Safety Communications Common Disposition Codes for Data Exchange*	Provides a standardized list of disposition codes to facilitate effective incident exchange between NG911 PSAPs and other authorized agencies.	Version 2 March 20, 2018
APCO ANS 1.112.1-2014	*Best Practices for The Use of Social Media in Public Safety Communications*	Provides a consistent foundation for agencies to develop specific operational procedures and competencies when using social media.	Version 1 2014 (Version 2 in Development)
APCO ANS 1.114.1-2017	*APCO Recommended Best Practices for PSAPs When Processing Vehicle Telematics Calls from Telematics Service Providers*	Provides best practices to guide the interactions between Telematics Call Center Operators and PSAP Telecommunicators.	January 29, 2017
APCO ANS 1.115.1-2018	*Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications*	Identifies competencies, operational factors and training requirements relating to next generation technologies.	Version 1 July 3, 2018
APCO ANS 1.116.1-2015	*Public Safety Communications Common Status Codes for Data Exchange*	Provides a standardized list of status codes that can be used by emergency communications and public safety stakeholders when sharing incident related information.	Version 1 April 7, 2015
APCO ANS 2.103.2-2019	*Public Safety Communications Common Incident Types for Data Exchange*	Identifies public safety communications common incident types for data exchange.	Version 2 10/18/2019
APCO ANS 2.106.1-2019	*Public Safety Grade Site Hardening*	Addresses the requirements for public-safety-grade site hardening of wireless communications sites and facilities.	Version 1 June 21, 2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO ANS 3.101.3-2017	*Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO)*	Identifies the competencies and training requirements for CTOs.	Version 3 September 12, 2017
APCO ANS 3.102.2-2017	*Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor*	Identifies the competencies and training requirements for public safety communications supervisors.	Version 2 September 12, 2017
APCO ANS 3.103.2.2015	*Minimum Training Standards for Public Safety Telecommunicators*	Identifies the training requirements for public safety telecommunicators.	Version 2 July 14, 2015
APCO ANS 3.103.2-2013	*Wireless 9-1-1 Deployment and Management Effective Practices Guide*	Provides an overview of the technology applications and management of wireless calls, as well as public and responder expectations.	Version 2 September 27, 2013 (Version 3 In Development)
APCO ANS 3.104.2-2017	*Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator*	Identifies the competencies and training requirements for PSAP training coordinators.	Version 2 September 19, 2017
APCO ANS 3.106.2-2017	*Core Competencies and Minimum Training Standards for Public Safety Communications Quality Assurance Evaluators (QAE)*	Identifies the competencies and training requirements for PSAP QA evaluators.	Version 2 September 12, 2017
APCO ANS 3.107.1.2015	*Core Competencies and Minimum Training Requirements for Public Safety Communications Technician*	Identifies the competencies and training requirements for PSAP communications technicians.	Version 1 February 24, 2015 In Revision

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO ANS 3.108.2.2018	*Core Competencies and Minimum Training Standards for Public Safety Communications Instructor*	Identifies the competencies and training requirements for PSAP instructors.	Version 1 February 3, 2014 Version 2 June 7, 2018
APCO ANS 3.109.2.2014	*Core Competencies and Minimum Training Standards for Public Safety Communications Manager/Director*	Identifies the competencies and training requirements for communications managers and/or directors.	Version 2 June 9, 2014 (Version 3 In Development)
APCO/CSAA ANS 2.101.2-2014	*APCO/CSAA ANS for Alarm Monitoring Company to PSAP CAD External Alarm Interface*	Provides detailed technical data to software providers who support CAD systems or alarm monitoring applications concerning the common data elements and structure when electronically transmitting a new alarm event from an alarm monitoring company to a PSAP.	Version 2 August 5, 2014 (Version 3 In Development)
APCO/NENA 2.105.1-2017	*NG9-1-1 Emergency Incident Data Document (EIDD)*	Provides format for sharing emergency incident information.	Version 1 January 3, 2017
APCO/NENA ANS 1.102.3-2020	*Public Safety Answering Point (PSAP) Service Capability Criteria Rating Scale*	Provides an assessment tool for PSAP managers and their governing authorities to identify their current level of service capability.	Version 3 1/30/2020
APCO/NENA ANS 1.105.2-2015	*Standard for Telecommunicator Emergency Response Taskforce (TERT) Deployment*	Includes information to provide guidance and helpful material regarding the development, maintenance, and deployment of a TERT.	Version 2 July 14, 2015 (Version 3 in Development)
APCO/NENA ANS 1.107.1.2015	*Standard for the Establishment of a Quality Assurance and Quality Improvement Program for Public Safety Answering Points*	Defines components of a QA/QI program within a PSAP.	Version 1 April 2, 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
APCO/NENA ANS 3.105.1-2015	*Minimum Training Standard for TTY/TDD Use in the Public Safety Communications Center*	Defines the training standards for TTY/TDD use in communications centers.	Version 1 February 24, 2015
APCO/NPSTC ANS 1.104.2-2017	*Standard Channel Nomenclature for the Public Safety Interoperability Channels*	Provides standard nomenclature for FCC and NTIA-designated nationwide interoperability channels used for public safety voice communications.	Version 2 January 3, 2017

Building Industries Consulting Service International (BICSI)

Name Building Industries Consulting Service International (BICSI)

Type International Trade Association (Infrastructure Systems)

Purpose BICSI supports the information and communications technology (ICT) community. ICT covers the spectrum of voice, data, electronic safety and security, project management, and audio and video technologies. It encompasses the design, integration, and installation of pathways, spaces, optical fiber- and copper-based distribution systems, wireless-based systems, and infrastructure that support the transportation of information and associated signaling between and among communications and information-gathering devices.

Website www.bicsi.org

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/BICSI 006-2020	*Distributed Antenna System (DAS) Design and Implementation Best Practices*	Provides requirements and recommendations for the design and installation of a standards-compliant, vendor-neutral DAS to be used for a wide range of applications, environments and locations.	2020 Edition
Telecommunications Distribution Methods Manual (TDMM)	*Telecommunications Distribution Methods Manual*	Reference manual for telecommunications and information communications technology infrastructure design	14th Edition / 2020
BICSI 009-2019	*Data Center Operations and Maintenance Best Practices*	Provides a framework for data center operation policies and practices covering data centers from the small enterprise to the large hyperscale colocation data center.	2019 Edition
ANSI/BICSI 001-2017	*Information and Communication Technology Systems Design and Implementation Best Practices for Educational Institutions and Facilities*	Provides educational facilities ICT infrastructure design planning to support facility and technological growth.	2017 Edition

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/BICSI 002-2019	*Data Center Design and Implementation Best Practices*	Provides requirements, guidelines and best practices applicable to any data center, including security, power, cooling, cabling, and other topics.	2019 Edition
ANSI/BICSI 003-2014	*Building Information Modeling (BIM) Practices for Information Technology Systems*	Provides detailed information about BIM content models and object parameters, setting the recommended levels and guidelines for BIM models.	2014 Edition
ANSI/BICSI 007-2020	*Information Communication Technology Design and Implementation Practices for Intelligent Building and Premises*	Provides requirements and recommendation for design and implementation of the structured cabling system and related applications for any size building or premise, regardless if it is serves commercial, government, transportation, residential, or any other functions.	2020 Edition
ANSI/BICSI 008-2018	*Wireless Local Area Network (WLAN) Systems Design and Implementation Best Practices*	Provides requirements and recommendation for design and implementation of the structured cabling system supporting a WLAN; and concepts within wireless transmission for developing WLAN deployments.	2018 Edition
ANSI/BICSI N1-2019	*Installation Practices for Telecommunications and ICT Cabling and Related Cabling Infrastructure*	Provides ICT industry installation practices.	2019 Edition
ANSI/BICSI N3-20	*Planning and Installation Methods for the Bonding and Grounding of Telecommunication and ICT Systems and Infrastructure*	Provides guidance to prevent injury and equipment damage through proper installation of an ICT bonding and grounding system.	2020 Edition

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/BICSI-004-2018	*Information Communication Technology Systems Design and Implementation Best Practices for Healthcare Institutions and Facilities*	Provides ICT design and implementation best practices for healthcare institutions and facilities.	2018 Edition
ANSI/BICSI-005-2016	*Electronic Safety and Security (ESS) System Design and Implementation Best Practices*	Provides the requirements and recommendations of a structured cabling infrastructure that would support all types of security systems.	2016 Edition
BICSI G1-17	*ICT Outside Plant Construction and Installation: General Practices*	Provides information on traditional infrastructure such as cabling and pathways, but also items not typically found within interior design work, such as right-of-way, permitting and service restoration.	2017 Edition
Telecommunications Project Management Manual (TPMM)	*Telecommunications Project Management Manual*	Provides information needed to execute telecommunications projects.	1st Edition

CableLabs

Name CableLabs

Type Standards-Setting Organization – Industry (Cable)

Purpose CableLabs works on standards and technologies for the delivery of high-speed data, video, voice, and next-generation services. CableLabs provides testing, certification facilities and technical information.

Website https://www.cablelabs.com

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CL-RQ-IP-CPE-SEC	*Common Security Requirements for IP-Based MSO-Provided CPE*	Identifies the areas where common vulnerabilities exist for such CPEs, and crafts requirements to avoid those vulnerabilities.	Version I01 March 15, 2013
DPoE-SP-IPNEv2.0	*DPoE IP Network Element Requirements*	Specifications to provide requirements for additional service capabilities and corresponding provisioning and network management capabilities.	Version I07 February 28, 2018
DPoE-SP-MEFv2.0	*DPoE Metro Ethernet Forum Specification*	Specifications on DOCSIS-based provisioning and operations of IP using DOCSIS Internet service (which is typically referred to as High Speed Data (HSD)), or IP (HSD) for short, and Metro Ethernet services as described by Metro Ethernet Forum (MEF) standards.	Version I06 February 28, 2018
PKT-SP-24.229	*PacketCable SIP and SDP Stage 3 Specification 3GPP TS 24.229*	Defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on SIP and the associated SDP.	Version C01 March 14, 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
PKT-SP-33.203	*PacketCable Access Security for IP-Based Services Specification 3GPP TS 33.203*	Specifies the security features and mechanisms for secure access to the IM subsystem (IMS) for the 3G mobile telecommunication system.	Version C01 March 14, 2014
PKT-SP-BSSF	*PacketCable Business SIP Services Feature Specification*	Specifies emergency call procedures for business (IP Centrex) phones (i.e., endpoint is not embedded in CM, and can be behind NAT).	Version C01 March 14, 2014
PKT-SP-CI	*PacketCable Cellular Integration Specification*	Addresses how to provide the user a consistent telephony feature experience on either PacketCable or circuit cellular networks (3GPP or 3GPP2) and during domain transfers between PacketCable and 3GPP or 3GPP2 circuit cellular networks.	Version C01 March 14, 2014
PKT-SP-CMSS1.5	*PacketCable 1.5 CMS to CMS Signaling Specification*	Specifies the protocols and procedures to use between call management servers (CMSs) belonging to a single service provider as well as between CMSs that belong to different service providers.	Version C01 November 20, 2019
PKT-SP-ESG	*PacketCable Enterprise SIP Gateway Specification*	Defines the requirements for the PacketCable 2.0 Enterprise SIP Gateway (ESG) device to simplify and streamline the initial deployment and ongoing management of Business Voice services to enterprise customers.	Version C01 April 5, 2017
PKT-SP-RSTF	*PacketCable Residential SIP Telephony Feature Specification*	Specifies implementation of common residential telephony features in a PacketCable network with SIP-based User Equipment (UEs).	Version C01 March 14, 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
PKT-SP-RST-UE-PROV	*PacketCable RST UE Provisioning Specification*	Specifies RST UE provisioning attributes to support emergency calls.	Version C01 March 14, 2014
PKT-SP-TGCP1.5	*PacketCable 1.5 PSTN Gateway Call Signaling Protocol Specification*	Describes an application programming interface called a Media Gateway Control Interface (MGCI) and a corresponding protocol (MGCP) for controlling VoIP PSTN gateways from external call control elements.	Version C04 November 20, 2019
PKT-TR-ARCH-FRM	*PacketCable Architecture Framework Technical Report*	Describes the architecture framework for PacketCable™ networks, including all major system components, the various functional groupings and the network interfaces necessary for delivery of services via a PacketCable network.	Version C01 March 14, 2014
PKT-TR-SIP	*PacketCable SIP Signaling Technical Report*	Extends cable's real-time IP communication service architecture and accelerates the convergence of voice, video, data, and mobility technologies.	Version C01 March 14, 2014
WR-SP-WiFi-ROAM	*Wi-Fi Roaming Architecture and Interfaces Specification*	Specifies architecture requirements for best effort data roaming among cable operator Wi-Fi networks.	Version I04 December 1, 2014

Department of Commerce (DOC)

Name Department of Commerce (DOC)

Type Government Agency

Purpose The DOC promotes job creation and economic growth by providing data to support commerce and fostering innovation through standards setting and conducting research.

Website http://www.commerce.gov/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
SP800-171 Rev. 2	*Protecting Controlled, Unclassified Information in Nonfederal Systems and Organizations*	Provides federal agencies with recommended security requirements for protecting the confidentiality of Controlled Unclassified Information (CUI).	February 2020
FIPS-PUB-140-3	*Security Requirements for Cryptographic Modules*	Specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information.	March 22, 2019
FIPS-PUB-180-4	*Secure Hash Standards (SHS)*	Specifies hash algorithms to detect whether messages have not been altered since they were originally generated.	August 2015
FIPS-PUB-197	*Advanced Encryption Standards (AES)*	Specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data; the AES algorithm is a symmetric block cipher that can encrypt and decrypt information.	November 26, 2001
GTRI NSTIC Trustmark Framework	*Trustmark Framework Technical Specification*	Provides normative language that governs the structures that comprise the Trustmark Framework and the rules and policies related to the operational use of these structures.	Version 1.2 November 6, 2017

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NIST Special Publication 1800-13 (Draft)	*Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders (2nd Draft)*	Provides a method for public safety organizations to deploy an interoperable multifactor authentication and single sign-on tools to protect access to sensitive information.	May 2019 (2nd Draft)
NIST Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*	This framework consists of standards, guidelines and best practices to manage cybersecurity risk.	Version 1.1 April 16, 2018
NIST Special Publication 800-171A	*Assessing Security Requirements for Controlled Unclassified Information*	Provides procedures for assessing the CUI requirements in NIST Special Publication 800-171.	June 2018

Department of Homeland Security (DHS)

Name Department of Homeland Security (DHS)

Type Government Agency

Purpose DHS's mission is to secure the nation from threats. Five DHS core missions are to:

- Prevent terrorism and enhance security
- Secure and manage U.S. borders
- Enforce and administer U.S. immigration laws
- Safeguard and secure cyberspace
- Ensure resilience to disasters

Website http://www.dhs.gov/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
2019 National Emergency Communications Plan	*2019 National Emergency Communications Plan*	Outlines the six nationwide goals and 19 objectives to improve critical capabilities through partnerships, joint planning, and unified investments across levels of government.	September 2019
SAFECOM	*Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials*	Provides recommendations and best practices for public safety officials at all levels of government to establish, assess, and update governance structures that represent all emergency communications capabilities.	April 2019

Department of Justice (DOJ)

Name Department of Justice (DOJ)

Type Government Agency

Purpose DOJ's mission is to enforce the law and defend the interests of the U.S. according to the law; to ensure public safety against threats foreign and domestic; to provide federal leadership in preventing and controlling crime; to seek just punishment for those guilty of unlawful behavior; and to ensure fair and impartial administration of justice for all Americans.

Website http://www.justice.gov/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CJISD-ITS-DOC-08140-5.9	*Criminal Justice Information Services (CJIS) Security Policy*	Contains information security requirements for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI).	Version 5.9 June 1, 2020

Ericsson

Name Ericsson

Type Industry (Telecommunications)

Purpose Ericsson is a provider of information and communication technology (ICT) to service providers. Ericsson provides vendor-neutral services to the industry through its generic requirements (GRs), historically referred to as Telcordia requirements, development services.

Website https://www.ericsson.com
https://telecom-info.telcordia.com/site-cgi/ido/docs2.pl?ID=194307990&page=home

Document ID	Document Title	Document Description	Latest Revision/ Release Date
GR-63	*NEBS Requirements: Physical Protection*	Presents minimum spatial and environmental criteria for all new telecommunications equipment used in Central Offices (COs) and other environmentally controlled telephone equipment spaces.	Issue 5 Dec 2017
GR-78	*Generic Requirements for the Physical Design and Manufacture of Telecommunications Products and Equipment*	Contains industry requirements for how to design and build reliable electronics for telecom network use.	Issue 2 Sep 2007
GR-468	*Generic Reliability Assurance Requirements for Optoelectronic Devices Used in Telecommunications Equipment*	Presents generic reliability assurance practices for optoelectronic devices used in telecommunications equipment.	Issue 2 Sep 2004
GR-513	*Power Requirements in Telecommunications Plant*	Provides requirements for power systems designed for network telecommunications equipment in COs and similar locations.	Issue 2 Jan 2010

Document ID	Document Title	Document Description	Latest Revision/ Release Date
GR-1293	*Generic Requirements for Permanent AC & DC Backup Generators Including Fuel Cells for Remote Electronic Sites*	Provides requirements for standby engine-generator systems including fuel cells to be used in remote telecommunications sites.	Issue 1 Mar 2017
GR-1298	*AINGR: Switching Systems*	Provides requirements to implement the Advanced Intelligent Network (AIN) switching system technology in a public telephone network.	Issue 10 Nov 2004
GR-2953	*Enhanced MF Signaling: E9-1-1 Tandem to PSAP Interface*	Provides requirements to support enhanced MultiFrequency (MF) signaling for the E911 tandem to PSAP interface and associated generic requirements for the E911 tandem and its selective routing functionality.	Issue 1, Rev01 Dec 1998
GR-2956	*CCS/SS7 Generic Requirements in Support of E9-1-1 Service*	Provides requirements for Signaling System 7 (SS7) signaling to support E911 service.	Issue 5 Dec 2002
GR-3017	*Generic Requirements for an AIN-Based Implementation of E9-1-1 Service*	Provides requirements to support an AIN-based architecture for E911 service.	Issue 4 Dec 2002
GR-3028	*Thermal Management In Telecommunications Central Offices: Thermal GR-3028*	Provides NEB-related thermal management information, guidelines, targets, objectives, and requirements for equipment manufacturers and service providers for ensuring network integrity.	Issue 1 Dec 2001
GR-3112	*Emergency Services Network Interconnection*	Focuses on the interconnection of client company Emergency Services Networks and ESInets with SIP-based originating networks.	Issue 5 Oct 2007

Document ID	Document Title	Document Description	Latest Revision/ Release Date
GR-3118	*Voice over Internet Protocol (VoIP) Positioning Center (VPC) Generic Requirements*	Defines the required functions and interfaces that must be supported by the VPC to facilitate the routing of emergency calls and to ensure the delivery of location information related to VoIP emergency call originations.	Issue 4 Sep 2008
GR-3119	*Emergency Service Zone (ESZ) Routing Database (ERDB) Generic Requirements*	Provides requirements for an ERDB to support VoIP-originated calls.	Issue 4 Oct 2008
GR-3129	*Emergency Services Gateway (ESGW) Generic Requirements*	Provides requirements for an ESGW to support the routing of VoIP-originated 911 calls to legacy PSAPs via traditional emergency services networks.	Issue 2 Dec 2007
GR-3130	*Location Validation Database (VDB) Generic Requirements in Support of E9-1-1 Service*	Provides requirements for the functions and interfaces supported by a VDB as a key element of the NENA i2 Solution.	Issue 2 Nov 2007
GR-3157	*Emergency Services Routing Proxy (ESRP) Generic Requirements*	Provides the requirements for the functions and interfaces that need to be supported at the ESRP.	Issue 3 Jul 2010
GR-3158	*Generic Requirements for a Service Provider Location Information Server (LIS)*	Details requirements for the functionality and interfaces of a LIS providing location capabilities in a service provider network.	Issue 2 Jun 2009
GR-3160	*Generic Requirements for Telecommunications Data Center Equipment and Spaces*	Presents spatial and environmental requirements for data center equipment and spaces.	Issue 2 Jul 2013
GR-3162	*Legacy Network Gateway Generic Requirements*	Provides requirements for a Legacy Network Gateway to support the routing of 911 calls that originate in the legacy wireline or wireless networks to IP-enabled (i3) PSAPs via ESInets.	Issue 4 Apr 2012

Document ID	Document Title	Document Description	Latest Revision/ Release Date
GR-3165	*Emergency Services Border Control Function (BCF) Generic Requirements*	Describes the functionality, interfaces, and operations requirements associated with an emergency service BCF.	Issue 2 Feb 2010
GR-3166	*Legacy Public Safety Answering Point (PSAP) Gateway Generic Requirements*	Describes the functionality, interfaces, and operations requirements associated with a legacy PSAP gateway routed via i3 ESInets.	Issue 3 Dec 2012
GR-3170	*Legacy Selective Router (SR) Gateway Generic Requirements*	Addresses the functions, interfaces, and data that must be supported by a legacy SR gateway to facilitate the interconnection of i3 ESInets with legacy SRs and IP selective routing (IPSR) functional elements.	Issue 1 Oct 2010

European Telecommunications Standards Institute (ETSI)

Name European Telecommunications Standards Institute (ETSI)

Type Regional Standards Organization

Purpose ETSI develops standards for information and communications technologies, including fixed, mobile, radio, converged, broadcast, and internet technologies.

Website http://www.etsi.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI TR 103 582	*EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations*	Prepares the requirements for communications involving IoT devices in all types of emergency situations.	Version 1.1.1 July 2019
ETSI TS 103 605-2	*EMTEL; Testing - Conformance test specifications for core elements for network independent access to emergency services (NG112); Part 2: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)*	Contains the Abstract Test Suite (ATS) for core elements for network independent access to emergency services (NG112) as defined in standards listed in clause 2.1 of the present document.	Version 1.1.1 January 2020
ETSI TS 103 625	*Emergency Communications (EMTEL); Transporting Handset Location to PSAPs for Emergency Calls - Advanced Mobile Location*	Describes the transport methods used for AML messages with handset derived location information and associated data, the content of the AML messages, and allows for the data sent within the message to include further attributes than supported in current deployments.	Version 1.1.1 December 2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI TS 103 650	*EMTEL; Testing - Conformance test specifications for core elements for network independent access to emergency services (NG112); Part 1: Protocol Implementation Conformance Statement (PICS), Test Suite Structure and Test Purposes (TSS & TP)*	Provides the Protocol Implementation Conformance Statement (PICS) and Test Suite Structure and Test Purposes (TSS & TP) for core elements for network independent access to emergency services (NG112) as defined in standards listed in clause 2.1 of the present document.	Version 1.1.1 January 2020
ETSI TS 123 167	*Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions*	Defines the stage 2 service description for emergency services in the IP Multimedia Core Network Subsystem (IMS), including the elements necessary to support IP Multimedia (IM) emergency services and IM emergency services for eCall.	Version 15.7.0 July 2020
ETSI TS 183 036	*Core Network and Interoperability Testing (INT); ISDN/SIP interworking; Protocol specification*	Specifies the stage three protocol description of the signaling interworking between ISDN DSS1 protocol and SIP.	Version 3.6.2 April 2020
ETSI 203 178	*Functional architecture to support European requirements on emergency caller location determination and transport*	Describes the unified functional architecture to support European requirements on emergency caller location determination and transport, in particular for the case where VoIP service provider and one or several network operators - all serving the customer in the establishment of an emergency call - are independent enterprises needing to co-operate to determine the location of the (nomadic) caller.	Version 1.1.1 February 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI ES 203 283	*Protocol Specifications for Emergency Service Caller Location Determination and Transport*	Describes the protocol specifications for emergency service caller location determination and transport architecture as specified in ETSI ES 203 178	Version 1.1.1 November 2017
ETSI ES 282 007	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture*	Describes the IMS core component of the TISPAN NGN functional architecture and its relationship to other subsystems and components.	Version 2.1.1 November 2008
ETSI SR 002 777	*Emergency Communications (EMTEL); Test/verification procedure for emergency calls*	Outlines test procedures for emergency calls from individuals (citizens) to authorities.	Version 1.1.1 July 2010
ETSI TR 102 180	*Emergency Communications (EMTEL); Basis of requirements for communication of individuals with authorities/ organizations in case of distress (Emergency call handling)*	Provides the requirements for communication from individuals to authorities and organizations in all types of emergencies.	Version 1.5.1 July 2015
ETSI TR 102 476	*Emergency Communications (EMTEL); Emergency calls and VoIP: possible short and long term solutions and standardization activities*	Provides an overview of standardization activities and summarizes different methods for VoIP providers to deliver emergency communication services.	Version 1.1.1 July 2008
ETSI TR 102 641	*Satellite Earth Stations and Systems (SES); Overview of present satellite emergency communications resources*	Provides an overview of concepts, systems and initiatives related to the use of space resources in the context of disaster management.	Version 1.2.2 August 2013

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI TR 103 201	*Emergency Communications (EMTEL); Total Conversation for Emergency Communications; Implementation Guidelines*	Contains recommendations and guidelines on the implementation of Total Conversation for emergency service access and provision.	Version 1.1.1 March 2016
ETSI TR 103 393	*Emergency Communications (EMTEL); Advanced Mobile Location for emergency calls*	This document focusses on circuit switched emergency voice calls and location transport via SMS.	Version 1.1.1 (March 2016)
ETSI TR 103 470	*Emergency Communications (EMTEL); Total Conversation Access to Emergency Services*	Describes conditions for using Total Conversation for emergency services and makes access of emergency services possible to people with disabilities.	Version 1.1.1 November 2013
ETSI TR 187 002	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis*	Presents the results of the Threat Vulnerability Risk Analysis (TVRA) for the NGN.	Version 3.1.1 April 2011
ETSI TS 101 470	*Emergency Communications (EMTEL); Total Conversation Access to Emergency Services*	Defines conditions for using Total Conversation for emergency services with more media than in the regular voice call providing opportunities to more rapid, reliable and confidence-creating resolution of the emergency service cases.	Version 1.1.1 November 2013
ETSI TS 102 164	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols*	Specifies the protocol that is used by the local emergency operator to obtain the location information that is registered on the operator location server.	Version 1.3.1 September 2006

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI TS 102 424	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements of the NGN network to support Emergency Communication from Citizen to Authority*	Contains the requirements of an NGN to support EMTEL from the citizen to authority.	Version 1.1.1 September 2005
ETSI TS 102 660	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Signalling Requirements and Signalling Architecture for supporting the various location information protocols for Emergency Service on a NGN*	Makes recommendations on the standards to be used for the acquisition and conveyance of location information associated with emergency calls.	Version 1.1.1 July 2008
ETSI TS 103 284	*Satellite Earth Stations and Systems (SES); Satellite Emergency Communications (SatEC); Device classes for Emergency Communication Cells over Satellite (ECCS)*	Defines classes of Emergency Communication Cell over Satellite (ECCS) devices [i.1].	Version 1.1.1 August 2014
ETSI TS 123 167	*Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions*	Defines the stage two service description for emergency services in the IMS, including the elements necessary to support IM emergency services.	Version 16.2.0 July 2020
ETSI TS 182 009	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Architecture to support emergency communication from citizen to authority*	Defines the architectural description for emergency services in the IMS, including the elements necessary to support IM emergency services.	Version 2.1.1 October 2008

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ETSI TS 187 001	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements*	Defines the security requirements pertaining to TISPAN NGN Release 3.	Version 3.9.1 July 2014
ETSI TS 187 003	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture*	Defines the security architecture of NGN.	Version 3.4.1 March 2011
ETSI TS 187 005	*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Lawful Interception; Stage 1 and Stage 2 definition*	Specifies the stage two model for Lawful Interception of TISPAN NGN services.	Version 3.1.1 June 2012

Federal Communications Commission (FCC)

Name Federal Communications Commission (FCC)

Type Government Agency

Purpose The FCC is an independent U.S. government agency charged with regulating interstate and international communications by radio, television, wire, satellite, and cable.

Relevant Bureaus Public Safety and Homeland Security Bureau (PSHSB): The PSHB promotes the public's access to reliable 911, emergency alerting, and first responder communications. The PSHSB develops and implements policies to ensure that the public have access to effective and reliable communications. This includes issues related to but not limited to 911, Enhanced 911, and NG911, including location accuracy and text-to-911; network reliability, resiliency, security and interoperability; and public safety communications.

Website http://www.fcc.gov/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CSRIC Best Practices Database	*CSRIC Best Practices*	Includes search features by number, text, type and keywords to locate best practices resulting from work performed by CSRIC, NRIC and other related FCC initiatives.	Ongoing
CSRIC II Working Group 4B Transition to Next Generation 9-1-1	*Transition to Next Generation 9-1-1*	Frames several transition issues, within the context of the CSRIC process, and offers recommendations for further action.	March 2011
CSRIC IV Working Group 1 Next Generation 9-1-1 Task 1 Subtask 1	*Final Report - Investigation into Location Improvements for Interim SMS (Text) to 9-1-1*	Reviews approaches to provide enhanced location information and evaluates associated limitations and challenges for SMS text to 911 services.	June 2014
CSRIC IV Working Group 1 Next Generation 9-1-1 Task 1 Subtask 2	*Final Report - PSAP Requests for Service for Interim SMS Text-to-9-1-1*	Provides recommended best practices for 911 authorities to utilize when requesting the interim SMS text-to-911 service.	May 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CSRIC IV Working Group 1 Next Generation 9-1-1 Task 2	*Final Report - Location Accuracy and Testing for Voice-over-LTE Networks*	Provides information on the impact VoLTE implementation will have on carriers' ability to comply with existing wireless E911 location accuracy levels.	September 2014
CSRIC IV Working Group 1 Next Generation 9-1-1 Task 3	*Final Report - Specification for Indoor Location Accuracy Test Bed*	Provides guidance to the Commission on establishing a permanent entity to design, develop, and manage an ongoing public test bed for indoor location technologies.	June 2014
CSRIC IV Working Group 4 Cybersecurity Risk Management	*Cybersecurity Risk Management and Best Practices*	Provides recommendations on voluntary mechanisms to assure communication providers are taking necessary measures to manage cybersecurity risks and implementation guidance to help adapt the voluntary NIST Cybersecurity Framework.	March 2015
CSRIC V Working Group 1: Evolving 911 Services Task 1	*Final Report – Task 1: Optimizing PSAP Re-Routes*	Documents the efforts undertaken by the CSRIC V Working Group 1 with respect to its Task 1 to review existing Best Practices, identify gaps in those Best Practices and make recommendations towards Best Practices that optimize PSAP reroutes.	March 2016
CSRIC V, Working Group 1: Evolving 911 Services Task 2	*Final Report – 911 Location-Based Routing*	Reviews and identifies several location-based routing methods that could be used for wireless 911 call routing. It also reviews transition considerations for NG911 ESInets.	September 2016
CSRIC V, Working Group 6: Secure Hardware and Software – Security by Design	*Best Practice Recommendations for Hardware and Software Critical to the Security of the Core Communications Network*	Identifies voluntary recommendations and best practices to enhance the security of hardware and software in the core public communications network.	March 2016

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CSRIC V, Working Group 6: Secure Hardware and Software – Security by Design	*Final Report: Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network*	Describes the attestation framework that could be used by companies to demonstrate the success of the recommendations/best practices.	September 2016
TFOPA Working Group 1	*Optimal Cybersecurity Approach for PSAPs*	Identifies cybersecurity issues and documentation of recommended cybersecurity practices for PSAPs.	December 10, 2015
TFOPA Working Group 1	*Optimal Cybersecurity Approach for PSAPs, Supplemental Report*	Provides expanded cost estimates to include implementation of proposed cybersecurity options at the local, State and Regional levels and operational costs based on graded levels of service and traffic.	December 2, 2016
TFOPA Working Group 2	*Phase II Supplemental Report: NG9-1-1 Readiness Scorecard,*	Provides an overview of a tool for public safety entities to assess their level of NG911 readiness.	December 2, 2016
TFOPA Working Group 2	*Task Force on Optimal PSAP Architecture (TFOPA)*	Provides recommendations to the Commission regarding actions PSAPs can take to optimize their security, operations, and funding as they migrate to NG911.	January 29, 2016
TFOPA Working Group 3	*Funding Sustainment Model*	Outlines a funding sustainment model that can be used by state and 911 authorities to calculate their financial needs to support a transitional NG911 implementation.	December 2, 2016

Federal Geographic Data Committee (FGDC)

Name Federal Geographic Data Committee (FGDC)

Type Interagency Committee

Purpose FGDC coordinates development, use, sharing, and dissemination of geospatial data on a national basis. The FGDC develops or adopts geospatial standards for implementing the National Spatial Data Infrastructure (NSDI). The NSDI is a physical, organizational, and virtual network designed to enable the development and sharing of U.S. digital geographic information resources.

Website http://www.fgdc.gov/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
FGDC-STD-016-2011	*Map Position Proposal for 2015 Revision of the United States Thoroughfare, Landmark, and Postal Address Data Standard*	Provides a data content, classification, quality, and exchange standard for thoroughfare, landmark and postal addresses, and for address reference systems; provides a complete XML schema description for exchange of address data.	Version 1.8 November 2015
FGDC-STD-016-2011	*United States Thoroughfare, Landmark, and Postal Address Data Standard*	Provides a data content, classification, quality, and exchange standard for thoroughfare, landmark and postal addresses, and for address reference systems; provides a complete XML schema description for exchange of address data.	Version 2.0 February 2011

Information Security Forum (ISF)

Name Information Security Forum (ISF)

Type Global Information Systems Security and Risk Management Organization

Summary ISF investigates, clarifies and resolves issues in information security and risk management, by developing best practice methodologies, processes and solutions.

Website https://www.securityforum.org

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISF Standard of Good Practice for Information Security	*Standard of Good Practice for Information Security 2020*	Provides a business-orientated focus on current and emerging information security issues and helps organizations develop a framework for information security policies, standards and procedures	2020

Information Sharing and Analysis Organization (ISAO)

Name Information Sharing and Analysis Organizations (ISAO)

Type Government Project

Purpose ISAO works with information sharing organizations, owners and operators of critical infrastructure, relevant agencies, and other public- and private-sector stakeholders through a voluntary consensus standards development process to identify a common set of voluntary standards for the creation and functioning of ISAOs. These standards address, but are not be limited to, contractual agreements, business processes, operating procedures, technical specifications and privacy protections.

Website https://www.isao.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISAO 400-1	*Emerging State and Local Cybersecurity Laws and Regulations Impacting Information Sharing*	Provides an overview of state laws and general legislation that can influence the roles of information sharing entities within geographical areas. Is designed to provide insights into the laws, initiatives and regulations nationwide that ISAOs should understand and monitor.	Version 1.0 April 20, 2020
ISAO 300-1	*Introduction to Information Sharing*	Describes a conceptual framework for information sharing, information sharing concepts, the types of cybersecurity information an organization may want to share, ways an organization can facilitate information sharing, as well as privacy and security concerns to be considered.	Version 1.01 October 14, 2016
ISAO 600-1	*A Framework for State-Level Information Sharing and Analysis Organizations*	Provides a resource for facilitating cybersecurity sharing and analysis within states.	Version 1.0 June 11, 2018

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISAO 600-2	*U.S. Government Relations, Programs, and Services*	Identifies preliminary matters of policy and principles, state and local government perspectives, and relevant federal laws regarding cybersecurity information sharing within the United States.	Version 1.01 October 14, 2016
ISAO SP 4000	*Protecting Consumer Privacy in Cybersecurity Information Sharing*	Outlines actions for information sharing while minimizing the impact on privacy interests.	Version 1.0 July 26, 2017

Institute of Electrical and Electronics Engineers (IEEE)

Name Institute of Electrical and Electronics Engineers (IEEE)

Type Professional Association

Purpose IEEE is a technical professional organization dedicated to the advancement of technology through the pursuit of standards and global collaboration.

Website https://www.ieee.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
IEEE 802.3CG-2019	*IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors*	Specifies additions to and appropriate modifications of IEEE Std 802.3 to add 10 Mb/s Physical Layer (PHY) specifications and management parameters for operation, and associated optional provision of power, on single balanced twisted-pair copper cabling.	February 5, 2020
IEEE 802.3CM-2020	*IEEE Standard for Ethernet -- Amendment 7: Physical Layer and Management Parameters for 400 Gb/s over Multimode Fiber*	Defines PHY specifications and management parameters for the transfer of Ethernet format frames at 400 Gb/s over fewer than 16 pairs of multimode fiber physical media.	March 30, 2020
IEEE 802.3CQ-2020	*IEEE Standard for Ethernet Amendment 6: Maintenance #13: Power over Ethernet over 2 pairs*	Contains editorial and technical corrections, refinements, and clarifications to Clause 33, Power over Ethernet over 2 pairs, and related portions of the standard.	March 13, 2020
IEEE Std 802.3ca/D3.1	*IEEE Draft Standard for Ethernet Amendment: Physical Layer Specifications and Management Parameters for 25 Gb/s and 50 Gb/s Passive Optical Networks*	Amends IEEE Std 802.3 to add physical layer specifications and management parameters for point-to-multipoint passive optical networks supporting MAC data rates of 25 Gb/s or 50 Gb/s.	February 1, 2020

Document ID	Document Title	Document Description	Latest Revision/ Release Date
P3005.4/D10	*Approved Draft recommended practice for design and operational considerations for improving the reliability of emergency and stand-by power systems*	Describes how to improve the reliability of emergency and stand-by power systems.	June 16, 2020
IEEE 802.1AB-2016	*Station and Media Access Control Connectivity Discovery*	Defines a protocol and a set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802(R) LANs.	March 11, 2016
IEEE 802.1AC-2016/Cor 1-2018	*Media Access Control (MAC) Service Definition - Corrigendum 1: Logical Link Control (LLC) Encapsulation EtherType*	Defines the MAC service found in LANs and MANs, and the Internal Sublayer Service and External Internal Sublayer Service provided within MAC Bridges, in abstract terms of their semantics, primitive actions and events, and the parameters of, interrelationship between, and valid sequences of, these actions and events.	Nov. 9, 2018
IEEE 802.1AR-2018	*Local and Metropolitan Area Networks - Secure Device Identity*	Specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device to its identifiers, the relationship between an initially installed identity and subsequent locally significant identities, and interfaces and methods for use of DevIDs with existing and new provisioning and authentication protocols.	Aug. 2, 2018
IEEE 802.3-2018	*IEEE Standard for Ethernet*	Specifies selected speeds of operation from 1 Mb/s to 100 Gb/s using a common MAC specification and management information base (MIB) for Ethernet LAN operation.	Aug. 31, 2018

Document ID	Document Title	Document Description	Latest Revision/ Release Date
IEEE 802.11-2016	*Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*	Specifies technical corrections and clarifications to IEEE Standard 802.11 for WLANS as well as enhancements to the existing MAC and PHY functions.	Dec. 14, 2016
IEEE 802.16-2017	*Air Interface for Broadband Wireless Access Systems*	Specifies the air interface, including the MAC and PHY, of combined fixed and mobile point-to-multipoint broadband wireless access (BWA) systems providing multiple services.	March 2, 2018
IEEE 802.19.1-2018	*Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 19: Wireless Network Coexistence Methods*	Specifies radio technology independent methods for coexistence among dissimilar television band devices (TVBDs) and dissimilar or independently operated networks of TVBDs.	Nov. 2, 2018
IEEE 1903-2011	*Functional Architecture of Next Generation Service Overlay Networks*	Specifies a functional architecture for a Next Generation Service Overlay Network, consisting of a set of functional entities, their functions, reference points and information flows to illustrate service interaction and media delivery.	Oct. 7, 2011

International Organization of Standardization (ISO)

Name International Organization of Standardization (ISO)

Type International Standards Organization

Purpose ISO is a network of the national standards institutes that focuses on developing consensus-based standards.

Website http://www.iso.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO/IEC 27007:2020	*Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*	Provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditor.	January 2020
ISO/IEC 27031:2011	*Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*	Describes the concepts and principles of ICT readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects for improving an organization's ICT readiness to ensure business continuity.	March 1, 2011 Edition 1
ISO 19115-1:2014	*Geographic information — Metadata — Part 1: Fundamentals*	Defines the schema required for describing geographic information and services by means of metadata; provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services.	April 1, 2014 First Edition
ISO 19115-1:2014/AMD 1: 2018	*Geographic information — Metadata — Part 1: Fundamentals — Amendment 1*	Amends 19115-1.	February 2018 First Edition

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO 19165-1:2018	*Geographic information — Preservation of digital data and metadata — Part 1: Fundamentals*	Identifies the requirements of the geospatial archival IP and details of the geospatial submission and the dissemination IPs.	May 2018 Edition 1
ISO/IEC 20000-1:2018	*Information technology — Service management — Part 1: Service management system requirements*	Updates 2011 requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS; includes the design, transition, delivery and improvement of services to fulfill agreed service requirements.	September 9, 2018 Edition 3
ISO/IEC 24760-1:2019	*IT Security and Privacy – IT Security and Privacy A framework for identity management – Part 1: Terminology and concepts*	Defines terms for identity management and specifies core concepts of identity and identity management, and their relationships.	May 2019 Edition 2
ISO/IEC 24760-2:2015	*Information technology — Security techniques — A framework for identity management – Part 2: Reference architecture and requirements*	Provides guidelines for the implementation of systems for the management of identity information and specifies requirements for the implementation and operation of a framework for identity management.	June 1, 2015 Edition 1
ISO/IEC 24760-3:2016	*Information technology — Security techniques — A framework for identity management – Part 3: Practice*	Provides guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2.	August 2, 2016
ISO/IEC 27000:2018	*Information technology — Security techniques — Information security management systems – Overview and vocabulary*	Provides an overview of ISMS, and terms and definitions commonly used in the ISMS family of standards.	February 2018 Edition 5
ISO/IEC 27001	*Information Security Management*	Provides requirements for an ISMS.	Ongoing

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO/IEC 27001:2013	*Information technology — Security techniques — Information security management systems – Requirements*	Specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS within the context of the organization; includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.	October 10, 2013 Edition 2
ISO/IEC 27002:2013	*Information technology — Security techniques — Code of practice for information security controls*	Provides guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).	October 1, 2013 Edition 2
ISO/IEC 27003:2017	*Information technology — Security techniques — Information security management systems — Guidance*	Focuses on the critical aspects needed for successful design and implementation of ISMS; describes the process of ISMS specification and design from inception to the production of implementation plans.	March 1, 2017 Edition 2
ISO/IEC 27004:2016	*Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*	Provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented ISMS and controls or groups of controls.	December 15, 2016 Edition 2
ISO/IEC 27005:2018	*Information technology — Security techniques — Information security risk management*	Provides guidelines for information security risk management; is designed to assist the satisfactory implementation of information security based on a risk management approach.	July 2018 Edition 3

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO/IEC 27011:2016	*Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*	Provides guidelines for supporting the implementation of information security management in telecommunications organizations.	December 2016 Edition 2
ISO/IEC 27032:2012	*Information technology – Security techniques – Guidelines for cybersecurity*	Covers the baseline security practices for stakeholders in the Cyberspace.	July 2012
ISO/IEC 27033-1:2015	*Information technology — Security techniques — Network security — Part 1: Overview and concepts*	Provides an overview of network security and related definitions and describes the concepts associated with, and provides management guidance on, network security.	August 15, 2015 Edition 2
ISO/IEC 27033-2:2012	*Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*	Provides guidelines for organizations to plan, design, implement and document network security.	August 2012
ISO/IEC 27033-3:2010	*Information technology — Security techniques — Network security — Part 3: Reference Networking scenarios – Threats, design techniques and control issues*	Describes the threats, design techniques and control issues associated with reference network scenarios; provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks.	December 2010
ISO/IEC 27033-4:2014	*Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*	Provides guidance for securing communications between networks using security gateways in accordance with a documented information security policy of the security gateways.	March 1, 2014 Edition 1

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO/IEC 27033-5:2013	*Information technology — Security techniques — Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*	Provides guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using VPN connections to interconnect networks and connect remote users to networks.	August 2019 Edition 1
ISO/IEC 27033-6:2016	*Information technology — Security techniques — Network security – Part 6: Securing wireless IP network access*	Describes the threats, security requirements, security control and design techniques associated with wireless networks. Provides guidelines for the selection, implementation and monitoring of the technical controls necessary to provide secure communications using wireless networks.	June 2016 Edition 1
ISO/IEC 27035-1:2016	*Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*	Presents basic concepts and phases of information security incident management with concepts and principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learned.	November 2016 Edition 1
ISO/IEC 27035-2:2016	*Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*	Provides the guidelines to plan and prepare for incident response.	November 2016 Edition 1
ISO/IEC 27037:2012	*Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*	Provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value.	October 2010 Edition 1

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISO/IEC 29115:2013	*Information technology – Security techniques – Entity authentication assurance framework*	Provides a framework for managing entity authentication assurance in a given context.	April 1, 2013 Edition 1
ISO/IEC 29146:2016	*Information technology – Security techniques – A framework for access management*	Provides guidelines for the identity proofing of a person; specifies levels of identity proofing, and requirements to achieve these levels.	June 2016 Edition 1
ISO/IEC TS 29003:2018	*Information technology – Security techniques – Identity proofing*	Provides security techniques for identity proofing.	March 2018 Edition 1
ISO/TS 19115-3:2016	*Geographic information — Metadata — Part 3: XML schema implementation for fundamental concepts*	Describes the procedure used to generate XML schema from ISO geographic information conceptual models related to metadata.	August 2016 Edition 1

International Telecommunication Union (ITU)

Name International Telecommunications Union (ITU)

Type International Association

Purpose ITU facilitates international connectivity in communications networks, allocates global radio spectrum and satellite orbits, and develops technical network standards.

Website https://www.itu.int/en/Pages/default.aspx

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ITU-T X.509	*Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*	Defines frameworks for public-key certificates and attribute certificates.	September 5, 2019 Edition 9
ITU-T P.800.2	*Mean opinion score interpretation and reporting*	Introduces common types of mean opinion score (MOS) and describes information that should accompany MOS values to enable them to be correctly interpreted.	July 29, 2016
ITU-T Y.1271	*Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks*	Presents an overview of the requirements, features, and concepts for emergency telecommunications that evolving networks are capable of providing.	July 18, 2014
ITU-T Y.2705	*Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)*	Provides security requirements for the inter-network interconnection of ETS, allowing ETS to be supported with the necessary security protection between different national networks with bilateral and/or multilateral agreements in times of disaster and emergencies.	March 1, 2013

Internet Engineering Task Force (IETF)

Name Internet Engineering Task Force (IETF)

Type International Standards Organization—Industry (Networking)

Purpose IETF produces technical and engineering documents that address the design, use, and management of the internet. These documents include protocol standards, current best practices, and informational documents of various kinds.

Website http://www.ietf.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 2328	*OSPF Version 2*	Describes the OSPF protocol implementation.	January 21, 2020
RFC 2474	*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*	Defines the fields used by the Differentiated Code Point (DSCP) protocol to provide QoS traffic prioritization in an IP network.	January 21, 2020
RFC 3261	*SIP: Session Initiation Protocol*	Describes SIP, an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (including Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.	January 21, 2020
RFC 3262	*Reliability of Provisional Responses in Session Initiation Protocol (SIP)*	Describes an extension to SIP providing reliable provisional response messages; the extension uses the option tag "100rel" and defines the Provisional Response Acknowledgement (PRACK) method.	January 21, 2020
RFC 3264	*An Offer/Answer Model with Session Description Protocol (SDP)*	Describes a mechanism by which two entities can make use of the SDP to arrive at a common view of a multimedia session.	January 21, 2020

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 3265	*Session Initiation Protocol (SIP)-Specific Event Notification*	Describes a SIP extension to provide an extensible framework by which SIP nodes can request notification from remote nodes indicating that certain events have occurred.	January 21, 2020
RFC 3413	*Simple Network Management Protocol (SNMP) Applications*	Describes five types of SNMP applications that make use of an SNMP engine as described in RFC 3411.	January 21, 2020
RFC 3414	*User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*	Describes the USM for SNMP version 3 for use in the SNMP architecture.	January 21, 2020
RFC 3415	*View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*	Describes the VACM for use in the SNMP architecture.	January 21, 2020
RFC 3416	*Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*	Defines version 2 of the protocol operations for SNMP; defines the syntax and elements of procedure of sending, receiving, and processing SNMP PDUs.	January 21, 2020
RFC 3856	*A Presence Event Package for the Session Initiation Protocol (SIP)*	Describes the usage of SIP for subscriptions and notifications of presence.	January 21, 2020
RFC 3863	*Presence Information Data Format (PIDF)*	Specifies the Common Profile for Presence (CPP) PIDF as a common presence data format.	January 21, 2020
RFC 4119	*A Presence-based GEOPRIV Location Object Format*	Describes an object format for carrying geographical information on the Internet.	January 21, 2020
RFC 4271	*A Border Gateway Protocol 4 (BGP-4)*	Discusses the BGP, which is an inter-Autonomous System routing protocol; provides a set of mechanisms for supporting Classless Inter-Domain Routing.	January 21, 2020

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 5246	*The Transport Layer Security (TLS) Protocol Version 1.2*	Specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements.	January 21, 2020
RFC 5340	*OSPF for IPv6*	Describes the modifications to Open Shortest Path First (OSPF) to support IPv6.	January 21, 2020
RFC 5880	*Bidirectional Forwarding Detection (BFD)*	Describes a protocol intended to detect faults in the bidirectional path between two forwarding engines, including interfaces, data link, and the forwarding engines themselves where possible.	January 21, 2020
RFC 5881	*Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*	Describes the particulars necessary to use BFD in the IPv4 and IPv6 environments.	January 21, 2020
RFC 6739	*Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol*	Defines an XML protocol to exchange these mappings between two nodes.	January 21, 2020
RFC 8447	*Updates registries related to Transport Layer Security (TSL) and Datagram Transport Layer Security (DTLS)*	Updates RFC 4680, RFC 7301, RFC 5705, RFC 5077, RFC 3749, RFC 5878, RFC 6520, RFC 5246 registries and registration policies.	March 10, 2020
Internet Draft (draft-ietf-ecrit-similar-location-08	*A LoST extension to return complete and similar location info*	Describes a LOST extension to return completed or similar form to the original input civic location, based on whether valid or invalid civic address elements are returned within the findServiceResponse message.	July 22, 2019
Internet Draft draft-ietf-mmusic-msrp-usage-data-channel-23	*MSRP over Data Channels*	Specifies how MSRP can be instantiated as a data channel sub-protocol.	July 22, 2020

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 2475	*An Architecture for Differentiated Services*	Describes a protocol that provides QoS in an IP network.	March 2, 2013
RFC 3263	*Session Initiation Protocol (SIP): Locating SIP Servers*	Describes the DNS procedures to resolve SIP URI into the IP address, port, and transport protocol of the next hop to contact.	December 7, 2015
RFC 3411	*An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*	Describes an architecture for describing SNMP management frameworks.	October 14, 2015
RFC 3412	*Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*	Describes the message processing and dispatching for SNMP messages within the SNMP architecture; defines the procedures for dispatching potentially multiple versions of SNMP messages.	October 14, 2015
RFC 3417	*Transport Mappings for the Simple Network Management Protocol (SNMP)*	Defines the transport of SNMP messages over various protocols.	October 14, 2015
RFC 3418	*Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*	Defines managed objects which describe the behavior of an SNMP entity.	January 21, 2020
RFC 3550	*RTP: A Transport Protocol for Real-Time Applications*	Describes the Real-time Transport Protocol (RTP), suitable for transmitting real-time information such as voice, video, and other delay-sensitive media.	October 14, 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 4079	*A Presence Architecture for the Distribution of GEOPRIV Location Objects*	Examines some existing IETF work on the concept of presence, shows how presence architectures map onto GEOPRIV architectures, and demonstrates that tools already developed for presence could be reused to simplify the standardization and implementation of GEOPRIV.	March 2, 2013
RFC 4103	*RTP Payload for Text Conversation*	Specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements.	December 20, 2018
RFC 4975	*The Message Session Relay Protocol (MSRP)*	Describes MSRP, a protocol for transmitting a series of related instant messages in the context of a session.	September 2007
RFC 4976	*Relay Extensions for the Message Sessions Relay Protocol (MSRP)*	Introduces the concept of message relay intermediaries to MSRP and describes the extensions necessary to use them.	September 2007
RFC 5012	*Requirements for Emergency Context Resolution with Internet Technologies*	Defines terminology and enumerates requirements for the context resolution of emergency calls placed by the public using VoIP and general Internet multimedia systems, where Internet protocols are used end to end.	October 14, 2015
RFC 5069	*Security Threats and Requirements for Emergency Call Marking and Mapping*	Reviews the security threats associated with the marking of signaling messages to indicate that they are related to an emergency, and with the process of mapping locations to URIs that point to PSAPs.	January 2008

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 5139	*Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*	Defines an XML format for the representation of civic location.	October 14, 2015
RFC 5194	*Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)*	Lists the requirements for real-time Text-over-IP (ToIP) and defines a framework for implementation of all required functions based on SIP and RTP.	October 14, 2015
RFC 5223	*Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)*	Describes how a LoST client can discover other LoST servers using DHCP.	December 20, 2018
RFC 5341	*The Internet Assigned Number Authority (IANA) tel Uniform Resource Identifier (URI) Parameter Registry*	Is the registry for *tel* URI parameters and their values.	October 14, 2015
RFC 5411	*A Hitchhiker's Guide to the Session Initiation Protocol (SIP)*	Provides high-level overview of SIP.	October 14, 2015
RFC 5582	*Location-to-URL Mapping Architecture and Framework*	Describes an architecture for a global, scalable, resilient, and administratively distributed system for mapping geographic location information to URLs, using the LoST protocol.	October 14, 2015
RFC 5882	*Generic Application of Bidirectional Forwarding Detection (BFD)*	Describes the generic application of the BFD protocol.	September 28, 2016
RFC 6135	*An Alternative Connection Model for the Message Session Relay Protocol (MSRP)*	Defines an alternative connection model MSRP User Agents (UAs); uses the connection-oriented media (COMEDIA) mechanism in order to create the MSRP transport connection.	February 2011

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 6155	*Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*	Extends the HELD protocol to allow the location request message to carry device identifiers; privacy and security considerations.	December 20, 2018
RFC 6280	*An Architecture for Location-based services usage and privacy*	Describes access control, usage rules and privacy requirements for location-based services regarding the geographic location of an individual or device.	October 14, 2015
RFC 6443	*Framework for Emergency Calling Using Internet Multimedia*	Describes how component parts of placing emergency calls are used to support emergency calls from citizens and visitors to authorities.	October 14, 2015
RFC 6446	*Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control*	Specifies mechanisms for adjusting the rate of SIP event notifications.	October 14, 2015
RFC 6447	*Filtering Location Notifications in the Session Initiation Protocol (SIP)*	Describes filters that limit asynchronous location notifications to compelling events.	October 14, 2015
RFC 6665	*SIP-Specific Event Notification*	Describes an extension to the SIP defined by RFC 3261.	December 20, 2018
RFC 6714	*Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)*	Defines an MSRP extension, CEMA; support of this extension is optional.	August 2012
RFC 6753	*A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)*	Describes how to use HTTP over TLS as a dereferencing protocol to resolve a reference to a PIDF-LO.	October 2012
RFC 6772	*Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information*	Defines an authorization policy language for controlling access to location information and location-specific access control.	January 2013

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 6848	*Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)*	Updates RFC 4776 and RFC 5222 by defining new fields for adding civic address elements to the Geopriv civic address format.	January 2013
RFC 6874	*Representing IPv6 Zone Identifiers in Address Literals and Uniform Resource Identifiers*	Extends RFC 3986 to include IPv6 to include zone identifiers and address literals	July 29, 2020
RFC 6881	*Best Current Practice for Communications Services in Support of Emergency Calling*	Describes best current practice on how devices, networks, and services using IETF protocols should use such standards to make emergency calls.	March 2013
RFC 6915	*Flow Identity Extension for HTTP-Enabled Location Delivery (HELD)*	Specifies an XML schema and an URN sub-namespace for a Flow Identity Extension for HELD.	April 2013
RFC 7035	*Relative Location Representation*	Defines an extension to the PIDF-LO for the expression of location information that is defined relative to a reference point.	October 2013
RFC 7044	*An Extension to the Session Initiation Protocol (SIP) for Request History Information*	Defines a standard mechanism for capturing the history information with a SIP request.	October 14, 2015
RFC 7090	*Public Safety Answering Point (PSAP) Callback*	Discusses shortcomings of the current PSAP call-back mechanisms and illustrates additional scenarios where better-than-normal call treatment behavior would be desirable.	April 2014
RFC 7105	*Using Device-Provided Location-Related Measurements in Location Configuration Protocols*	Describes a protocol for a device to provide location-related measurement data to a LIS within a request for location information.	January 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 7163	*URN for Country-Specific Emergency Services*	Updates the registration guidance provided in Section 4.2 of RFC 5031, which allows the registration of service URNs with the "sos" service type only for emergency services "that are offered widely and in different countries;" updates those instructions to allow such registrations.	March 2014
RFC 7199	*Location Configuration Extensions for Policy Management*	Extends the current location configuration protocols to provide hosts with a reference to the rules that are applied to a URI so that the host can view or set these rules.	April 2014
RFC 7216	*Location Information Server (LIS) Discovery Using IP Addresses and Reverse DNS*	Describes the configuration challenge of discovering a LIS when a residential gateway is present, requiring a method that is able to work around the obstacle presented by the gateway.	April 2014
RFC 7378	*Trustworthy Location*	Describes threats to conveying location, particularly for emergency calls, and describes techniques that improve the reliability and security of location information.	December 2014
RFC 7406	*Extensions to the Emergency Services Architecture for Dealing with Unauthenticated and Unauthorized Devices*	Provides a problem statement, introduces terminology and describes an extension for the base IETF emergency services architecture to address scenarios involving situations dealing with unauthenticated and unauthorized devices making emergency calls.	December 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
RFC 7459	*Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO)*	Defines concepts of uncertainty and confidence as they pertain to location information in the PIDF-LO.	February 2015
RFC 7701	*Multi-party Chat Using the Message Session Relay Protocol (MSRP)*	Defines the tools for establishing multi-party chat sessions, or chat rooms, using MSRP.	December 2015
RFC 7840	*A Routing Request Extension for the HTTP-Enabled Location Delivery (HELD) Protocol*	Describes a routing request extension for the HELD protocol.	May 9, 2016
RFC 7852	*Additional Data Related to an Emergency Call*	Describes data structures and mechanisms to convey information about the call, caller or location to a PSAP.	December 20, 2018
RFC 7977	*The WebSocket Protocol as a Transport for the Message Session Relay Protocol (MSRP)*	Specifies a new WebSocket sub-protocol as a reliable transport mechanism between MSRP clients and relays.	September 21, 2016
RFC 8148	*Next-Generation Vehicle-Initiated Emergency Calls*	Describes how to use IP-based emergency services mechanisms to support the next generation of emergency calls placed by vehicles	December 20, 2018
RFC 8262	*Location Conveyance, messaging and metadata for the Session Initiation Protocol*	Defines content-ID URL to reference a complete message-body and metadata as provided by some SIP header fields.	December 20, 2018

ISACA®

Name ISACA®

Type Global Information Systems Security Organization

Purpose ISACA® provides a centralized source of IT information and guidance on information governance, control, security and auditing.

Websites https://www.isaca.org/
https://cobitonline.isaca.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
COBIT® 2019	COBIT® 2019 Toolkit	Provides a framework for the governance and management of enterprise information and technology, aimed at the whole enterprise.	2019
NIST CSF Implementation	*Implementing the NIST Cybersecurity Framework Using COBIT 2019*	Provides an approach to integrate cybersecurity standards and enterprise governance of information and technology.	2019
NIST CSF V1.1	*NIST Cybersecurity Framework V1.1/COBIT 2019 Mapping*	Provides a mapping from the latest version of the NIST Cybersecurity Framework to COBIT 2019.	2019

National Emergency Number Association (NENA)

Name National Emergency Number Association (NENA)

Type National Standards Organization (ANSI-accredited)

Purpose NENA contributes to 911 through research, standards development, education, outreach, and advocacy.

Websites http://www.nena.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA 02-014 v1	*NENA GIS Data Collection and Maintenance Standards*	Provides necessary guidelines for collecting and maintaining GIS data.	July 17, 2007 Version 1
NENA 02-015 v1	*NENA Standard for Reporting and Resolving ANI/ALI Discrepancies & No Records Found on Wireline, Wireless and VoIP Technologies*	Sets forth standards for PSAP jurisdictions, access infrastructure providers, service providers and database management system providers in reporting and resolving ANI/ALI discrepancies that occurred during an E911 call.	June 6, 2009 Version 1
NENA 03-509 v1	*NENA Femtocell and Universal Mobil Access (UMA) Technical Information Document and UMA Appendix*	Describes the current state of femtocell and UMA deployments with respect to call processing of E911 calls and identifies the impacts to PSAPs of receiving and processing calls from femtocells.	January 27, 2011, Version 1
NENA 04-005 v1	*NENA ALI Query Service Standard*	Defines the NENA XML ALI Query Service (AQS) that specifies new protocols between the PSAP and the next generation emergency services network; provides the rationale behind the AQS and how it relates to the current ALI protocol.	November 21, 2006

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA 08-001 v2	*NENA Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)*	Provides an outline of an interim architecture to connect callers in the IP domain with PSAPs supported by the existing E911 service provider network.	August 11, 2010 Version 2
NENA 08-002 v1	*NENA Functional and Interface Standards for Next Generation 9-1-1 Version 1.0 (i3)*	Describes the ESInet, which is designed as an IP-based inter-network shared by all agencies that may be involved in any emergency; specifies that all calls enter the ESInet using SIP signaling.	December 18, 2007 Version 1
NENA 08-501 v1	*Interface between the E9-1-1 Service Provider Network and the Internet Protocol (IP) PSAP Information Document*	Provides technical information to guide manufacturers of network equipment and PSAP CPE in the development of IP-based interfaces between the network and PSAP CPE and to assist E911 network service providers and PSAPs in implementing such interfaces.	June 15, 2004 Version 1
NENA 08-503 v1	*VoIP Characteristics Technical Information Document*	Provides an overview of VoIP technology.	June 10, 2004 Version 1
NENA 08-505 v1	*NENA Method(s) for Location Determination to Support IP-Based Emergency Services*	Describes solutions that meet the proposed requirements for automatically determining the location of IP devices inside a residential broadband network.	December 21, 2006 Version 1
NENA 08-751 v1	*NENA i3 Requirements Document*	Specifies the requirements the i3 standard should meet.	September 28, 2006 Version 1
NENA 08-752 v1	*Location Information to Support IP-Based Emergency Services Requirements Document*	Provides the NENA requirements for providing information to support emergency calling.	December 21, 2006 Version 1
NENA 54-750 v1	*NENA Human Machine Interface & PSAP Display Requirements*	Prescribes the requirements for the human machine interface (HMI) display for the NG911 system.	October 20, 2010 Version 1

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA 71-501 v1	*NENA Synchronizing Geographic Information System Databases with MSAG & ALI Information Document*	Provides PSAP management, vendors, and other interested parties the necessary guidelines for synchronizing GIS data with existing 911 databases.	September 8, 2009 Version 1
NENA 71-502 v1	*An Overview of Policy Rules for Call Routing and Handling in NG9-1-1*	Provides an overview of what policy rules are, how policy is defined, and the ways that they may be used.	August 24, 2010 Version 1
NENA 73-501 v1	*Use Cases & Suggested Requirements for Non-Voice-Centric (NVC) Emergency Services Information Document*	Identifies suggested requirements for NVC emergency service.	January 11, 2011 Version 1
NENA 75-001	*NENA Security for Next-Generation 9-1-1 Standard (NG-SEC)*	Establishes guidelines and requirements for the protection of NG911 assets or elements within a changing business environment.	February 6, 2020
NENA 75-502 v1	*Next Generation 9-1-1 Security (NG-SEC) Audit Checklist*	Provides a summary of the requirements and recommendations detailed in the NG-SEC standard and provides the educated user a method to document an NG-SEC audit.	December 14, 2011 Version 1
NENA/APCO-INF-005	*Emergency Incident Data Document (EIDD)*	Provides a standardized, industry-neutral National Information Exchange Model (NIEM) conformant (XML-based) specifications for exchanging emergency incident information to agencies and regions that implement NG911.	January 8, 2014
NENA-ADM-000.23-2020	*NENA Master Glossary of 9-1-1 Terminology*	Defines the terms, acronyms, and definitions associated with the 911 industry.	January 20, 2020
NENA-INF-003.1-2013	*NENA Potential Points of Demarcation in NG9-1-1 Networks Information Document*	Identifies points of demarcation.	March 21, 2013

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA-INF-004.1.2-2018	*NENA Operational Impacts of Devices & Sensors Information Document*	Assists PSAPs and governing 911 authorities with information for evaluating the operational impacts of devices and sensors that may interface with the PSAP.	August 17, 2018
NENA-INF-007.1-2013	*NENA Handling Text-to-9-1-1 in the PSAP Information Document*	Provides a guideline for PSAPs with recommendations for emergency calling to 911 using text messaging.	October 9, 2013
NENA-INF-008.2-2013	*NENA NG9-1-1 Transition Plan Considerations Information Document*	Focuses on the aspect of transitioning data from the legacy environment to the NG911 environment.	November 20, 2013 Version 2
NENA-INF-009.1-2014	*Requirements for a National Forest Guide Information Document*	Gathers a set of requirements for a national, authoritative Forest Guide in order to allow an entity to procure the technology and services required from this NG911 functional element.	August 14, 2014
NENA-INF-010.2-2018	*NENA Succession Planning Information Document*	Assists PSAPs and governing 911 authorities with information to identify and plan for changes in critical tasks positions.	May 24, 2018
NENA-INF-011.2-2020	*NENA NG9-1-1 Policy Routing Rules Operations Guide*	Assists 911 governing authorities in using policy routing rules during the full lifecycle of an NG911 system.	June 18, 2020
NENA-INF-012.2-2015	*NENA Inter-Agency Agreements Model Recommendations Information Document*	Provides a model for the development of mutual aid agreements and MOUs between PSAPs and affiliated or support organizations.	January 8, 2015
NENA-INF-014.1-2015	*NENA Information Document for Development of Site/Structure Address Point GIS Data for 9-1-1*	Provides guidelines for the development of a site/structure GIS layer, including sub-address level attribute fields and address point placement.	September 18, 2015

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA-INF-015.1-2016	*NENA Next Generation 9-1-1 Security (NG-SEC) Information Document*	Provides detail of the mechanisms and best practices relative to security of the i3 system.	December 8, 2016
NENA-INF-016.2-2018	*Emergency Services IP Network Design (ESIND) Information Document*	Provides information that will assist in the development of requirements necessary to design ESInets that meet industry standards and best practices related to the NG911 systems that will depend on them for services.	April 5, 2018
NENA-INF-018.1-2017	*NENA Non-Mobile Wireless Service Interaction Information Document*	Analyzes current wireless home phone, small cell, femtocell and CMRS handsets with Wi-Fi voice capability and makes recommendations for how to provide the most accurate 911 location information.	February 16, 2017
NENA-INF-019.2-2016	*NENA Resource, NENA Hazard and Vulnerability Analysis Information Document*	Assists PSAPs with the development of hazard and vulnerability analyses.	September 10, 2016
NENA-INF-023.1.1-2020	*NENA Call Blocking Standard*	Defines NG911 core services which allow a PSAP to identify the source of a call that is adversely affecting its ability to operate normally and continue receiving legitimate calls.	February 25, 2020
NENA-INF-024.2-2018	*NENA E9-1-1 PSAP Site Characteristics Information Document*	Sets characteristics of the PSAP facilities that house the supporting CPE, including the equipment and facilities that support PSAP operations, except call-taker- or dispatch-related equipment that is located in the workspace.	February 14, 2018

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA-INF-025.2-2017	*NENA Virtual PSAP Management Information Document*	Guides PSAP staff and policy makers in evaluating and considering the opportunities and challenges presented with NG911 systems as they relate to personnel and PSAP management.	December 21, 2017
NENA-INF-040.1-202Y	*Monitoring and Managing NG9-1-1*	Will address specific operational topics and procedures associated with the transition to monitoring and managing NG911 software functions and infrastructure.	In Progress
NENA-REF-002.2-2014	*PSAP Interim Text-to-9-1-1 Support Documents*	Provides support information and education materials for PSAPs planning on moving forward with the interim solution for text-to-911.	December 2, 2014
NENA-REF-003.1-2015	*NENA Recommended Public Education Plan for Interim SMS Text-to-9-1-1 Public Education*	Provides guidance when reaching out to local decision makers to educate them on NG911.	March 31, 2015
NENA-REF-010.2-2019	*NENA NG9-1-1 Go-To Handbook*	Provides guidance to help 911 authorities create a smooth, timely and efficient project management approach and transition plan to accomplish implementation of NG911.	May 7, 2019
NENA-REQ-001.1.2.2018	*NENA Next Generation 9-1-1 Public Safety Answering Point Requirements Document*	Describes the application service environment of the NENA i3 PSAP and the interfaces required for processing of an incident.	June 10, 2018
NENA-REQ-002.1-2016	*NENA Next Generation 9-1-1 Data Management Requirements*	Defines discrepancy reports and performance reports associated with processes within the NG911 system.	March 10, 2016
NENA-STA-003.1.1-2014	*NENA Standard for NG9-1-1 Policy Routing Rules*	Identifies templates to be used when drafting policy rules to address how and where calls are diverted if the target PSAP is unreachable.	December 1, 2014

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA-STA-004.1.1-2014	*NENA Next Generation United States Civic Location Data Exchange Format (CLDXF) Standard*	Supports the exchange of U.S. civic location address information about 911 calls, both within the U.S. and internationally.	March 23, 2014 Version 1
NENA-STA-005.1-2017	*NENA Standards for the Provisioning and Maintenance of GIS data to ECRFs and LVFs*	Identifies the operational processes and procedures necessary to support the i3 ECRF and LVF; identifies ECRF/LVF performance and implementation tradeoffs for 911 authorities' consideration.	August 10, 2017
NENA-STA-006.1.1-2020	*NENA Standard for NG9-1-1 GIS Data Model* *Also includes NENA-REF-006.1-2020 and NG9-1-1 GIS Template Files.*	Defines the GIS data model, which supports the NENA Next Generation Core Services of location validation and routing, geospatial call routing, and appropriate agency for dispatch.	February 18, 2020
NENA-STA-008.2-2014	*NENA Registry System Standard*	Describes how registries are created and maintained in NENA.	October 6, 2014
NENA-STA-010.2-2016	*Detailed Functional and Interface Specification for the NENA i3 Solution*	Builds upon prior NENA publications including i3 requirements and architecture documents and provides a baseline to other NG911-related specifications.	September 10, 2016 Update in Progress
NENA-STA-012.2-2017	*NG9-1-1 Additional Data Standard*	Covers the use of additional data associated with a call, a location, a caller and a PSAP.	December 21, 2017
NENA-STA-015.10-2018	*NENA Standard Data Formats for E9-1-1 Data Exchange & GIS Mapping*	Sets forth NENA standard formats for ALI-related data exchange between service providers and data base management system providers, a GIS data model, a data dictionary, and formats for data exchange between the ALI database and PSAP controller equipment.	August 12, 2018

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA-STA-019.1.2018	*NENA NG9-1-1 Call Processing Metrics Standard*	Identifies normalized NG911 call-processing metrics for computing useful statistics so that independent implementations can derive the same comparable measurements.	July 2, 2018
NENA-STA-020.1-2020	*NENA Standard for 9-1-1 Call Processing*	Defines the processing of 911 calls by a PSAP, including call answering standards.	April 16, 2020
NENA-STA-027.3-2018	*NENA E9-1-1 PSAP Equipment Standards*	Sets the PSAP equipment requirements (for E911) intended for use by users, manufacturers, and providers of E911 CPE.	July 2, 2018
NENA-STA-028.2-2018	*NENA Generic Standards for E9-1-1 PSAP Intelligent Workstations (IWS) Equipment*	Identifies PSAP IWS equipment requirements.	June 16, 2018
Next Generation 9-1-1 Transition Policy Implementation Handbook	*Next Generation 9-1-1 Transition Policy Implementation Handbook*	Provides guidance for 911 leaders and government officials responsible for ensuring that federal, state and local 911 laws and regulations effectively enable the implementation of NG911 systems.	March 2010
Recommended NG9-1-1 Public Education Plan for Elected Officials and Decision Makers	*Recommended NG9-1-1 Public Education Plan for Elected Officials and Decision Makers*	Provides guidance when reaching out to local decision-makers to educate them on NG911 and the need to address funding, legislative and regulatory issues to enable the transition to NG911.	September 24, 2013
SMS Text-to-9-1-1 Resources for PSAPs & 9-1-1 Authorities	Different documents to assist NENA members in reaching out to the public, special interest groups, and other key stakeholders regarding the implementation of Interim SMS Text-to-9-1-1	Provides public education guidelines, logos and planning strategies.	Varies

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NENA EPRC	*The NENA Enhanced PSAP Registry and Census*	Is a secure database, web portal and map that contains information about PSAPs throughout the U.S.	2020
NENA 006.1.1-2020	*NENA Standard for NG9-1-1 GIS Data Model*	Provides information on the GIS data model, which supports the NENA NG911 Core Services (NGCS) of location validation and routing, both geospatial call routing or to the appropriate agency for dispatch.	February 18, 2020

National Fire Protection Association (NFPA)

Name National Fire Protection Association (NFPA)

Type National Standards Organization (ANSI-accredited)

Purpose NFPA is devoted to eliminating death, injury, property and economic loss due to fire, electrical and related hazards.

Website http://www.nfpa.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NFPA 70	*National Electrical Code® (NEC)*	Addresses the installation of electrical conductors, equipment, and raceways; signaling and communications conductors, equipment, and raceways; and optical fiber cables and raceways in commercial, residential, and industrial occupancies.	2020 Edition
NFPA 72	*National Fire Alarm and Signaling Code*	Provides safety provisions for fire detection, signaling, and emergency communications; includes requirements for mass notification systems used for weather emergencies; terrorist events; biological, chemical, and nuclear emergencies; and other threats.	2019 Edition
NFPA 76	*Standard for the Fire Protection of Telecommunications Facilities*	Provides requirements for fire protection of telecommunications facilities providing telephone, data, internet transmission, wireless, and video services to the public as well as life safety for the occupants plus protection of equipment and service continuity.	2020 Edition

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NFPA 950	*Standard for Data Development and Exchange for the Fire Service*	Standardizes data for operable information sharing in support of the all-hazards response.	2020 Edition
NFPA 1061	*Professional Qualifications for Public Safety Telecommunications Personnel*	Identifies job performance requirements for public safety telecommunicators.	2018 Edition
NFPA 1201	*Standard for Providing Fire and Emergency Services to the Public*	Contains requirements on the structure and operations of fire emergency service organizations to help protect lives, property, critical infrastructure, and the environment from the effects of hazards.	2020 Edition
NFPA 1221	*Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*	Describes the installation, performance, operation, and maintenance of public emergency services communications systems and facilities.	2019 Edition
NFPA 1600	*Standard on Continuity, Emergency, and Crisis Management*	Covers the development, implementation, assessment, and maintenance of programs for prevention, mitigation, preparedness, response, continuity, and recovery.	2019 Edition
NFPA 2400	*Standard for Small Unmanned Aircraft Systems (sUAS) Used for Public Safety Operations*	Covers requirements relating to the operation, deployment, and implementation of sUAS for public safety operations.	2019 Edition

National Information Exchange Model (NIEM)

Name National Information Exchange Model (NIEM)

Type Government Project

Purpose NIEM is a common vocabulary that enables efficient information exchange across diverse public and private organizations. NIEM connects communities of people who share a common need to exchange information in order to advance their mission.

Website http://niem.gov

Document ID	Document Title	Document Description	Latest Revision/ Release Date
NEIM 4.2	*National Information Exchange Model*	Supports enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the U.S.	Version 4.2 November 1, 2019

North American Electric Reliability Corporation (NERC)

Name North American Electric Reliability Corporation (NERC)

Type Professional Organization

Purpose NERC is a regulatory authority whose mission is to reduce risks to the reliability and security of the grid. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.

Website http://www.nerc.com/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CIP-003-8	*Cyber Security — Security Management Controls*	Specifies security management controls that establish responsibility and accountability to protect Bulk Electrical System (BES) cyber systems against compromise that could lead to misoperation or instability in the BES.	April 1, 2020
CIP-002-5.1a	*Cyber Security — BES Cyber System Categorization*	Identifies and categorizes BES cyber systems and their associated BES cyber assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES cyber systems could have on the operation of the BES.	December 27, 2016
CIP-004-6	*Cyber Security — Personnel & Training*	Requires that personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.	July 1, 2016

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CIP-005-5	*Cyber Security — Electronic Security Perimeter(s)*	Requires the identification and protection of the Electronic Security Perimeter(s) inside which all critical cyber assets reside, as well as all access points on the perimeter.	July 1, 2016
CIP-006-6	*Cyber Security — Physical Security of BES Cyber Systems*	Manages physical access to BES cyber systems by specifying a physical security plan in support of protecting BES cyber systems against compromise.	July 1, 2016 Version 5
CIP-007-6	*Cyber Security — System Security Management*	Manages system security by specifying select technical, operational, and procedural requirements in support of protecting BES cyber systems against compromise.	July 1, 2016 Version 5
CIP-008-5	*Cyber Security — Incident Reporting and Response Planning*	Mitigates the risk to the reliable operation of the BES as the result of a cyber security incident by specifying incident response requirements.	July 1, 2016 Version 5
CIP-009-6	*Cyber Security — Recovery Plans for BES Cyber Systems*	Recovers reliability functions performed by BES cyber systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.	July 1, 2016 Version 5
CIP-010-2	*Cyber Security — Configuration Change Management and Vulnerability Assessments*	Prevents and detects unauthorized changes to BES cyber systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES cyber systems from compromise.	July 1, 2016 Version 1

Document ID	Document Title	Document Description	Latest Revision/ Release Date
CIP-011-2	*Cyber Security — Information Protection*	Prevents unauthorized access to BES cyber system information by specifying information protection requirements in support of protecting BES cyber systems against compromise.	July 1, 2016

Open Geospatial Consortium (OGC®)

Name Open Geospatial Consortium (OGC)

Type Standards-Setting Organization (Community)

Purpose OGC develops standards and supports services that promote geospatial interoperability.

Website http://www.opengeospatial.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
	OGC API - Features - Part 2: Coordinate Reference System by Reference		Anticipated 2020
	OGC API - Features - Part 3: Common Query Language		Anticipated 2020
	OGC API - Features - Part 4: Simple Transactions		Anticipated 2020
	OGC API - Records		Anticipated 2020
	OGC API - Tiles		Anticipated 2020
	OGC API - Maps		Anticipated 2021
OGC 04-094r1	*Web Feature Service Implementation Specification with Corrigendum*	Defines interfaces for data access and manipulation operations on geographic features using HTTP as the distributed computing platform.	October 26, 2016 Version 1.1.3
OGC 06-042	*OpenGIS® Web Map Server Implementation Specification*	Specifies the behavior of a service that produces spatially referenced maps dynamically from geographic information; specifies operations to retrieve a description of the maps offered by a server to retrieve a map, and to query a server about features displayed on a map.	March 15, 2006 Version 1.3.0

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OGC 07-006r1	*OpenGIS® Catalogue Services Specification*	Specifies the interfaces, bindings, and a framework for defining application profiles required to publish and access digital catalogues of metadata for geospatial data, services, and related resource information.	February 23, 2007 Version 2.02
OGC 07-057r7	*OGC Web Map Tile Service*	Defines an OGC standard for a Web Map Tile Service (WMTS) interface standard; a WMTS enabled server application can serve map tiles of spatially referenced data using tile images with predefined content, extent, and resolution.	April 6, 2010 Version 1.0
OGC 07-074	*OpenGIS® Location Services (OpenLS): Core Services*	Defines OpenLS: Core Services, Parts 1-5, which consists of the composite set of basic services comprising the OpenLS Platform.	September 9, 2008 Version 1.2
OGC 09-025r2	*OGC® Web Feature Service 2.0 Interface Standard – With Corrigendum*	Specifies discovery operations, query operations, locking operations, transaction operations and operations to manage stored, parameterized query expressions.	Version 2.0.2 July 10, 2014
OGC 09-083r4	*GeoAPI 3.0.1 Implementation Standard with Corrigendum*	Defines application programming interface (API) which can be used for the manipulation of geographic information.	April 15, 2018 Version 3.0.1
OGC 10-129r1	*OGC® Geography Markup Language (GML) – Extended schemas and encoding rules*	Defines the XML schema syntax, mechanisms and conventions that provide an open, vendor-neutral framework for the description of geospatial application schemas for the transport and storage of geographic information in XML.	February 7, 2012 Version 3.3.0

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OGC 11-030r1	*OGC®: Open GeoSMS Standard – Core*	Defines an encoding for location enabling a text message to be communicated using SMS.	January 19, 2012 Version 1.0
OGC 12-019	*OGC City Geography Markup Language (CityGML) Encoding Standard*	Is an open data model and XML-based format for the storage and exchange of virtual 3D city models.	March 9, 2012 Version 2.0.0
OGC 12-168r6	*OGC® Catalogue Services 3.0 - General Model*	Supports the ability to publish and search collections of descriptive information (metadata records) for geospatial data, services, and related information.	June 10, 2016 Version 3.0
OGC 13-131r1	*OGC® Publish/Subscribe Interface Standard 1.0 - Core*	Supports the core components and concepts of the Publish/Subscribe message exchange pattern with OGC Web Services.	August 22, 2016 Version 1.0
OGC 13-133r1	*OGC® Publish/Subscribe Interface Standard 1.0 SOAP Protocol Binding Extension*	Supports the core components and concepts of the Publish/Subscribe message exchange pattern with OGC Web Services.	August 22, 2016 Version 1.0
OGC 16-120r3	*OGC Moving Features Access*	Defines Moving Features Access information on a relation between a trajectory object and one or more geometry objects, and information on a relation between two trajectory objects from a database storing trajectory data of moving features.	March 12, 2017 Version 1.0
OGC 17-069r3	*OGC API - Features - Part 1: Core*	Provides API building blocks to create, modify and query features on the Web.	October 14, 2019 Version 1.0
OGC 18-075	*OGC® Moving Features Encoding Part I: XML Core*	Specifies standard encoding representations of movement of geographic features. The primary use case is information exchange.	January 14, 2019 Version 1.0

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OGC 19-008r4	*OGC GeoTIFF Standard*	Defines the Geographic Tagged Image File Format (GeoTIFF) by specifying requirements and encoding rules for using the Tagged Image File Format (TIFF) for the exchange of georeferenced or geocoded imagery.	September 14, 2019 Version 1.1
OGC KML 2.3	*OGC KML 2.3*	Defines three conformance classes (levels) for KML resources, indicating the relative importance or priority of a particular set of constraints; the highest level (CL3) indicates full conformance.	August 4, 2015 Version 1.0

Open Mobile Alliance (OMA)

Name Open Mobile Alliance (OMA)

Type International Standards Organization

Purpose OMA develops specifications for creating interoperable services that work across all geographical boundaries, on any bearer network.

Website http://www.openmobilealliance.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OMA SEC_CF 1.1	*OMA Application Layer Security Common Functions V1.1*	Supports OMA Push services, enablers over SIP and UDP protocols, delegated authentication for Web services, and DTLS, GBA Push, and IPSec profiles.	July 31, 2012 Version 1.1
OMA-ERELD-LOCSIP-V1_0-201201717-A	*OMA Location in SIP/IP Core V1.0*	Provides mechanisms to expose location information to application servers connected to a SIP/IP core network.	January 17, 2012 Version 1.0
OMA-ERELD-LPPe-V2_0-20141202-C	*OMA LPP Extensions (LPPe) v2.0*	Outlines the enabler release definition for LPPe Enabler and the respective conformance requirements for clients and servers claiming compliance to it as defined by OMA across the specification baseline.	December 2014 Version 2.0
OMA-ERP-MLP-V3_1-20110920-A	*OMA Mobile Location Protocol V3.1*	Identifies the MLP, an application-level protocol for getting the position of mobile stations independent of underlying network technology.	September 20, 2011 Version 3.1

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OMA-ERP-SUPL-V3_0_2-20110920-C	*OMA Secure User Plane Location Architecture Candidate Version 3.0*	Outlines the enabler release definition for SUPL Enabler and the respective conformance requirements for clients and servers claiming compliance to it as defined by OMA across the specification baseline.	September 20, 2011 Version 3.0

Organization for the Advancement of Structured Information Standards (OASIS)

Name Organization for the Advancement of Structured Information Standards (OASIS)

Type Standards-Setting Organization (Community)

Purpose OASIS is a consortium that develops, converges, and adopts standards for the global information society.

Website http://www.oasis-open.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OASIS CAP v1.2	*Common Alerting Protocol*	Defines and describes CAP, which provides an open, non-proprietary digital message format for all types of alerts and notifications.	July 1, 2010 Version 1.2
OASIS EDXL-DE v1.0	*Emergency Data Exchange Language (EDXL) Distribution Element, v. 1.0*	Describes a standard message distribution framework for data sharing among emergency information systems using the XML-based EDXL.	May 1, 2006 Version 1.0
OASIS EDXL-HAVE	*Emergency Data Exchange Language (EDXL) Hospital Availability Exchange Version (HAVE) 2.0 Specification 02*	Specifies an XML document format that allows the communication of the status of a hospital, its services and resources.	March 18, 2019 Version 2.0
OASIS EDXL-RM	*Emergency Data Exchange Language Resource Messaging (EDXL-RM) 1.0*	Describes a suite of standard messages for data sharing among emergency and other information systems that deal in requesting and providing emergency equipment, supplies, people and teams.	December 22, 2009 Version 1.0

Document ID	Document Title	Document Description	Latest Revision/ Release Date
OASIS EDXL-SitRep v1.0	*Emergency Data Exchange Language Situation Reporting (EDXL-SitRep) Version 1.0 Committee Specification 2.0*	Describes a set of standard reports and elements that can be used for data sharing among emergency information systems, and that provide incident information for situation awareness on which incident command can base decisions.	October 6, 2016 Version 1.0
OASIS EDXL-TEC	*Emergency Data Exchange Language (EDXL) Tracking of Emergency Clients (TEC) Client Registry Exchange Version 1.0*	Provides a standard messaging format for the creation and exchange of client records in and among publicly-accessible registries to assist in tracking and repatriation of displaced individuals during emergencies, disasters, and routine day-to-day incidents.	June 13, 2014 Version 1.0
OASIS EDXL-TEP	*Emergency Data Exchange Language (EDXL) Tracking of Emergency Patients (TEP) Version 1.1 Committee Specification 02*	Provides XML messaging standard for exchange of emergency patient and tracking information during patient encounter through admission or release.	September 21, 2018 Version 1.1

Society of Cable Telecommunications Engineers (SCTE)

Name Society of Cable Telecommunications Engineers (SCTE)

Type Standards Setting Organization—Industry (Cable Telecommunications) (ANSI)

Purpose SCTE provides standards and workforce education related to cable telecommunications engineering.

Website http://www.scte.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/SCTE 18 2018 (ANSI J-STD-42-C)	*Emergency Alert Messaging for Cable*	Defines an emergency alert signaling method for use by cable TV systems in the U.S. to signal emergencies to digital receiving devices.	Oct. 1, 2018
ANSI/SCTE 165-10 2020	*IPCablecom 1.5 Part 10: Security*	Describes the IPCablecom security architecture, protocols, algorithms, associated functional requirements and any technological requirements that can provide for the security of the system for the IPCablecom network.	2020
ANSI/SCTE 165-16 2016	*IPCablecom 1.5 Part 16: Management Event Mechanism*	Describes the general event reporting mechanism, which consists of a set of protocols and interfaces that can be used by individual elements and components in the IPCablecom architecture, and framework.	2016
ANSI/SCTE 165-2 2016	*IPCablecom 1.5 Part 2: Audio/Video Codecs*	Addresses interfaces between IPCablecom client devices for audio and video communication.	2016
ANSI/SCTE 165-21 2016	*IPCablecom 1.5 Part 21: Signaling Extension MIB*	Specifies new objects that are being introduced beyond IPCablecom 1.0 for Signaling MIBS so that the additional changes made can be tracked easily.	2016

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/SCTE 24-03 2016	*IPCablecom Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems*	Describes a profile of the Media Gateway Control Protocol (MGCP) for IPCablecom embedded clients.	2016
ANSI/SCTE 24-04 2016	*IPCablecom 1.0 Part 4: Dynamic Quality of Service for the Provision of Real-Time Services over Cable Television Networks Using Data Modems*	Describes a dynamic QoS mechanism for the IPCablecom project; facilitates design and field-testing leading to the manufacture and interoperability of conforming hardware and software by multiple vendors.	2016
ANSI/SCTE 24-1 2016	*IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services over Cable Television Networks Using Cable Modems*	Provides the architectural framework that will enable cable television operators to provide time-critical services over their networks that have been enhanced to support cable modems.	2016
ANSI/SCTE 24-21 2017	*BV16 Speech Codec Specification for Voice over IP Applications in Cable Telephony*	Contains the description of the BV16 speech codec; gives detailed description of the BV16 encoder and decoder, and contains sufficient details to allow those skilled in the art to implement bit-stream compatible and functionally equivalent BV16 encoders and decoders.	2017
ANSI/SCTE 24-22 2018	*iLBCv2.0 Speech Codec Specification for Voice over IP Applications in Cable Telephony*	Contains the description of an algorithm for coding of speech signals sampled at 8 kHz.	2018
ANSI/SCTE 24-23 2017	*BV32 Speech Codec Specification for Voice over IP Applications in Cable Telephony*	Contains the description of the BV32 speech codec.	2017
ANSI/SCTE-162 2019	*Emergency Alert Signaling for the Home Network*	Defines an emergency alert signaling method for use by cable TV systems to signal emergencies.	2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
SCTE 164 2019	*Emergency Alert Metadata Descriptor*	Defines a container usable by cable system operators for the delivery of emergency alert metadata into the consumer domain.	2019
SCTE 165-01 2019	*IPCablecom 1.5 Part 1: Architecture Framework Technical Report*	Identifies the specifications that define the IPCablecom 1.5 reference architecture.	2019
SCTE 165-04 2019	*IPCablecom 1.5 Part 4: Dynamic Quality-of-Service*	Specifies a comprehensive mechanism for a client device to request a specific Quality of Service from the DOCSIS® network.	2019
SCTE 165-05 2019	*IPCablecom 1.5 Part 5: Media Terminal Adapter (MTA) Device Provisioning*	Defines the provisioning of MTA components of the embedded MTA device.	2019
SCTE 165-06 2019	*IPCablecom 1.5 Part 6: MIBS Framework*	Provides information on the management requirements of IPCablecom-compliant devices and functions and how these requirements are supported in the MIB modules.	2019
SCTE 165-07 2019	*IPCablecom 1.5 Part 7: MTA MIB*	Describes the IPCablecom 1.5 MTA MIB requirement.	2019
SCTE 165-08 2019	*IPCablecom 1.5 Part 8: Signaling MIB*	Describes the IPCablecom Signaling (SIG) MIB requirements.	2019
SCTE 165-11 2019	*IPCablecom 1.5 Part 11: Analog Trunking for PBX Specification*	Defines extensions to the IPCablecom Network-based Call Signaling (NCS) protocol to support analog trunking for PBX interfaces on an embedded VoIP client device in an IPCablecom environment.	2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
SCTE 165-13 2019	*IPCablecom 1.5 Part 13: Electronic Surveillance Standard*	Defines the interface between a telecommunications carrier that provides telecommunications services to the public for hire using IPCablecom capabilities and a law enforcement agency (LEA) to assist the LEA in conducting lawfully authorized electronic surveillance.	2019
SCTE 165-14 2019	*IPCablecom 1.5 Part 14: Embedded MTA Analog Interface and Powering*	Defines a set of requirements that will enable a service that is sufficiently reliable to meet an assumed consumer expectation of constant availability, including availability during power failure at the customer's premises, and (assuming the service is used to connect to the PSTN), access to emergency services (911, etc.).	2019
SCTE 165-15 2019	*IPCablecom 1.5 Part 15: Management Event MIB Specification*	Provides a common data and format definition for events (informative, alarm, etc.).	2019
SCTE 165-17 2019	*IPCablecom 1.5 Part 17: Audio Server Protocol*	Describes the architecture and protocols that are required for playing announcements in VoIP IPCablecom networks.	2019
SCTE 165-19 2019	*IPCablecom 1.5 Part 19: CMS Subscriber Provisioning Specification*	Defines the interface used between the CMS and Provisioning server for the exchange of service provisioning information to facilitate interoperability of conforming hardware and software from multiple vendors.	2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
SCTE 165-20 2019	*IPCablecom 1.5 Part 20: MTA Extension MIB*	Specifies new objects that are being introduced beyond IPCablecom 1.0 for MTA MIBS so that the additional changes made can be tracked easily.	2019

Standards Coordinating Council (SCC)

Name Standards Coordinating Council (SCC)

Purpose SCC is an advisory group composed of an industry consortium and SDOs that provide advice and counsel on matters related to information sharing standards and interoperability best practices.

Website http://www.standardscoordination.org

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ISE I^2F	*Information Sharing Environment Information Interoperability Framework (I2F)*	Guides the implementation of the ISE information sharing capabilities.	March 2014 Version 0.5
IS&S Playbook	*Information Sharing and Safeguarding (IS&S) Playbook*	Aids users to create or enhance an IS&S environment.	October 31, 2016 Version 2

Telecommunications Industry Association (TIA)

Name Telecommunications Industry Association (TIA)

Type National Standards Organization—Industry (Telecommunications) (ANSI accredited)

Purpose TIA provides information and usable resources, strategic guidance and business intelligence for technology, government affairs, and standard and business performance.

Website https://tiaonline.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
ANSI/TIA-607-D	*Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises*	Specifies requirements for telecommunications bonding and grounding infrastructure and its interconnection to electrical systems and telecommunications systems.	July 29, 2019
TIA J-STD-110.01.v002	*Joint ATIS/TIA Implementation Guideline for J-STD-110, Joint ATIS/TIA Native SMS/MMS Text to 9-1-1 Requirements and Architecture Specification Release 2*	Addresses CMSP and TCC service provider deployment considerations of J-STD-110.	May 2015
TIA J-STD-110.A	*ATIS/TIA Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements & Architecture Specification*	Provides errata and clarifications to the *Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification*.	November 2013
TIA J-STD-110.v002	*Joint ATIS/TIA Native SMS/MMS Text to 9-1-1 Requirements and Architecture Specification Release 2*	Outlines the requirements, architecture, and procedures for text messaging to 911 emergency services using native CMSP SMS or MMS capabilities for the existing generation and NG911 PSAPs.	May 2015
TIA TSB-102.BACC	*Project 25 Interface-RF-Subsystem Interface Overview*	Provides an overview of technical aspects and considerations supporting specification of the ISSI.	November 2011 Revision B

Document ID	Document Title	Document Description	Latest Revision/ Release Date
TIA TSB-102.BAGA	*Project 25 Console Subsystem Interface Overview*	Provides information relevant to the development of standards supporting voice services, and certain supplemental services involving the CSSI.	January 2013
TIA TSB-102.BAJA	*Project 25 Location Services Overview*	Describes LMR location services and a two-tiered approach to providing location services.	November 2017 Revision B
TIA TSB-146	*Telecommunications IP Telephony Infrastructures IP Telephony Support for Emergency Calling Service*	Covers issues associated with support of ECS from IP telephony terminals connected to an enterprise network; describes network architecture elements needed to support ECS, and the functionality of those elements.	November 2012
TIA TSB-5021	*Guidelines for the Use of Installed Category 5e and Category 6 Cabling to Support 2.5GBASE-T and 5GBASE-T*	Describes the evaluation of category 5e and category 6 cabling configurations for support of 2.5GBASE-T and 5GBASE-T applications as specified in IEEE 802.3bz.	January 2017
TIA/EIA/IS-834	*G3G CDMA-DS to ANSI/TIA/EIA-41*	Provides requirements and Upper Layer (Layer 3) signaling radio protocols and procedures for the DS-41 radio interface.	March 2000
TIA-102 Series	*Telecommunications, Land Mobile Communications*	Defines LMR technologies and operational needs.	April 2019
TIA-102.BAED	*Project 25 Packet Data Logical Link Control Procedures*	Specifies the LLC procedures that permit the conveyance of Common Air Interface (CAI) data packets between air interface endpoints for all relevant packet data configurations.	September 26, 2013

Document ID	Document Title	Document Description	Latest Revision/ Release Date
TIA-222 Revision H	*Structural Standard for Antenna Supporting Structures, Antennas and Small Wind Turbine Support Structures*	Provides the requirements for the structural design and fabrication of new and the modification of existing antenna supporting structures, antennas, small wind turbine supporting structures, appurtenance mounting systems, structural components, guy assemblies, insulators and foundations.	June 25, 2018
TIA-568 Set	*TIA Commercial Building Telecommunications Cabling Standard Set*	Describes the standards for structured cabling system in commercial buildings, and between buildings in campus environments; defines cabling types, distances, connectors, cable system architectures, cable termination standards and performance characteristics, cable installation requirements and methods of testing installed cable.	January 2019
TIA-569	*Telecommunications Pathways and Spaces*	Specifies requirements for telecommunications pathways and spaces.	May 23, 2019 Revision E
TIA-606	*Administration Standard for Telecommunications Infrastructure*	Specifies administration systems for telecommunications infrastructure within and between buildings.	June 19, 2017 Revision C
TIA-664.529	*Wireless Features Description: Emergency Services (9-1-1)*	Describes services and features so that the manner in which a subscriber may place calls using such features and services may remain reasonably consistent from system to system.	January 30, 2013 Revision B
TIA-942	*Telecommunications Infrastructure Standard for Data Centers*	Specifies data center design guidelines, structured cabling systems, and network design.	July 12, 2017 Revision B
TIA-1039	*QoS Signaling for IP QoS Support and Sender Authentication*	Provides a QoS signaling standard for use within IPv4 and IPv6 network-layer protocols.	August 2011 Revision A

Document ID	Document Title	Document Description	Latest Revision/ Release Date
TIA-1057	*Telecommunications IP Telephony Infrastructure Link Layer Discovery Protocol for Media Endpoint Devices*	Defines extensions to the IEEE 802.1AB protocol requirements that support VoIP equipment in IEEE 802-based LAN environments.	August 26, 2011
TIA-1191	*Callback to an Emergency Call Origination Stage 1 Requirements*	Specifies access network requirements for callback to an emergency call origination; pertains to 1x circuit switched (1xCS) calls routed to a 1xCS access network and 1xCS calls routed to a non-1xCS access network.	August 2011
TIA-4973.201	*Requirements for Mission Critical PTT and Related Supplementary Services*	Identifies requirements for mission critical push-to-talk services intended to operate over broadband networks.	January 2014
TIA-4973.211	*Requirements for the Mission Critical Priority and QoS Control Service*	Describes requirements for a mission critical priority and QoS control service for a wireless broadband network.	August 2014
TIA-5017	*Telecommunications Physical Network Security Standard*	Establishes functional performance of different physical network security elements and provides additional considerations to enhance the physical security of the telecommunications infrastructure.	February 19, 2016

USTelecom

Name USTelecom

Type Industry (Broadband)

Purpose USTelecom is a trade association that represents U.S. telecommunications-related businesses committed to investing in a network infrastructure that encourages and supports broadband connectivity.

Website https://www.ustelecom.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
2019 USTelecom Cybersecurity Toolkit	*USTelecom Cybersecurity Toolkit*	Includes a collection of cybersecurity initiatives and practical guidance related to IoT, cybercrime, cyber norms, cyber workforce, information sharing, guidance for businesses and supply chain risk management.	2019

Additional Resources

This section identifies professional organizations that contribute to standards development and are active in the industry. As with the SDOs, the organization is identified with its purpose. Additionally, some organizations have documents or other resources that may be of benefit to the reader.

American National Standards Institute (ANSI)

Name American National Standards Institute (ANSI)

Type National Standards Organization

Purpose ANSI oversees the development of voluntary consensus standards in the U.S. Activities include accrediting programs, assessing conformance, and approving standards developed by organizations. ANSI, itself, does not set standards, but approves and accredits other SDOs.

Website http://www.ansi.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
Homeland Defense and Security Standardization Collaborative (HDSSC)	*Standards Panel: Homeland Defense and Security Standardization Collaborative*	Identifies existing consensus standards, or, if none exist, assists government agencies and those sectors requesting assistance to develop and adopt consensus standards for homeland security and homeland defense.	

Broadband Forum (BBF)

Name	Broadband Forum (BBF)
Type	Industry (Broadband)
Purpose	BBF is focused on broadband innovation, standards, and ecosystem development. BBF's projects span across 5G, Connected Home, Cloud, and Access.
Website	http://www.broadband-forum.org/

Commission on Accreditation for Law Enforcement Agencies (CALEA)

Name Commission on Accreditation for Law Enforcement Agencies (CALEA®)

Type Professional Organization

Purpose CALEA® was created as a credentialing authority through the joint efforts of law enforcement's major executive associations—International Association of Chiefs of Police (IACP), National Organization of Black Law Enforcement Executives (NOBLE), National Sheriffs' Association (NSA), and the Police Executive Research Forum (PERF).

CALEA's accreditation program seeks to improve the delivery of public safety services, primarily by maintaining a body of standards, developed by public safety practitioners, that covers a wide range of up-to-date public safety initiatives; by establishing and administering an accreditation process; and by recognizing professional excellence.

Website http://www.calea.org/

Document ID	Document Title	Document Description	Latest Revision/ Release Date
Standards for Campus Security Security	*CALEA Standards for Campus Security Accreditation*	Designed for educational campus security organizations that primarily employ non-sworn security officers and identify themselves as a campus security entity. Focuses on the safety and security of students and applies standards that require organizations to consider critical issues such as facility risks, regulatory reporting, technology-based security monitoring, preventive patrol, and a host of other issues that provide comprehensive service delivery.	2019

Document ID	Document Title	Document Description	Latest Revision/ Release Date
Standards for Law Enforcement Agencies	*CALEA® Standards for Law Enforcement Agencies*	Identifies law enforcement standards that define law enforcement agency's role in administration, operations, and facilities and equipment of communications center under their control.	2016
Standards for Communications Agencies	*CALEA® Standards for Communications Agencies*	Provides a management model for agency administration and operations, addressing seven critical areas of communications center operations.	2011

Department of Energy (DOE)

Name Department of Energy (DOE)

Type Government Agency

Purpose The DOE mission is to ensure America's security and prosperity by addressing energy, environmental and nuclear challenges through science and technology solutions.

Website http://www.energy.gov

Department of Transportation (USDOT)

Name Department of Transportation (USDOT)

Type Government Agency

Purpose USDOT is a cabinet department concerned with providing the U.S. an efficient and modern transportation system that supports the national interests, enhances the quality of life of the American people, and increases the productivity of American businesses.

Websites http://www.dot.gov/

Industrial Internet Consortium (IIC)

Name Industrial Internet Consortium (IIC)

Type Consortium of multinational corporations

Purpose IIC is a global, member-supported, organization that supports the Industrial Internet of Things (IIOT) by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data. This is accomplished using common architectures, interoperability and open standards.

Website http://www.iiconsortium.org/index.htm

International Academies of Emergency Dispatch (IAED)

Name International Academies of Emergency Dispatch (IAED)

Type Professional Organization

Purpose IAED' s mission is to support the public safety emergency telecommunications professional and ensure that citizens in need of emergency, health, and social services are matched with the most appropriate resource.

Website http://www.emergencydispatch.org/

National 911 Program

Name National 911 Program

Type Government Agency

Purpose The National 911 Program works with States, technology providers, public safety officials, and 911 professionals to assure a smooth transition to an updated 911 system that takes advantage of new communications technologies. The Program also creates and shares a variety of resources and tools to help 911 systems.

Websites http://911.gov/

Object Management Group® (OMG®)

Name Object Management Group (OMG)

Type Not-for-Profit Technology Standards Consortium

Purpose OMG is a technology standards consortium. OMG task forces develop enterprise integration standards for a wide range of technologies and industries. OMG also hosts organizations such as Consortium for Information & Software Quality™ (CISQ™), the DDS Foundation, BPM+ Health, the Industrial Internet Consortium® (IIC™) and the Industry IoT Consortium™.

Website http://www.omg.org

Wi-Fi Alliance

Name Wi-Fi Alliance®

Type Industry Organization

Summary Wi-Fi Alliance is a worldwide network of companies that promote Wi-Fi adoption and evolution. The Wi-Fi Alliance's work includes the development of technologies, requirements, and test programs that help ensure Wi-Fi is interoperable, secure, and reliable.

Website http://www.wi-fi.org/

WiMAX Forum

Name WiMAX Forum

Type Industry Organization

Summary WiMAX Forum is a non-profit organization that certifies and promotes interoperability of broadband wireless products, based on IEEE standard 802.16, in an effort to promote the adoption and expansion of WiMAX, AeroMACs and WiGRID technologies globally.

Website http://www.wimaxforum.org/

Moving Forward

It is important for NG911 stakeholders to be mindful of how an unstandardized, semi-planned approach to standards development can and will affect the ability of PSAPs and emergency response entities to effectively share information and be interoperable. To alleviate this issue, increased activities (e.g., state oversight, state/regional compliant designs, and federal coordination working groups) can ensure that a complete set of NG911 open standards are accepted and adopted by all relevant stakeholders. This should include active participation by all members of the 911 community. Additionally, increased national collaboration could be utilized to monitor progress on the options below to address standards, technological barriers, and issues identified in A *National Plan for Migrating to IP-Enabled 9-1-1 Systems*:

- Complete and accept IP-enabled 9-1-1 open standards and understand future technology trends to encourage system interoperability and emergency data sharing;
- Establish routing and prioritization protocols and business rules;
- Determine the responsible entity and mechanisms for location acquisition and determination;
- Establish system access and security controls to protect and manage access to the IP-enabled 9-1-1 system of systems; and
- Develop a certification and authentication process to ensure service providers and 9-1-1 Authorities meet security and system access requirements.[14]

Lastly, without processes and protocols (e.g., certification and authentication, routing business rules), the benefits of the NG911 system—including routing based on criteria beyond location and connection of service providers beyond common service providers to the 911 system—are unlikely to be fully realized.

A significant number and variety of standards will have a significant impact on the implementation of NG911. Continuing to actively monitor standards that have been completed, along with relevant standards that are likely to emerge, will be essential in ensuring the greatest benefit to the global 911 community. The National 911 Program will continue to monitor NG911 standards and update this "living" document to reflect the progress made by SDOs and SSOs.

[14] A *National Plan for Migrating to IP-Enabled 9-1-1 Systems.* Executive Summary, (C), Standards and Technology. Page 1-6. Available at: https://www.911.gov/pdf/National_NG911_Migration_Plan_FINAL.pdf.

Acronym List

ACRONYM	DESCRIPTION
3GPP	3rd Generation Partnership Project
AACN	Advanced Automatic Collision Notification
AES	Advanced Encryption Standard
AIN	Advanced Intelligent Network
ALI	Automatic Location Identification
AMF	Access Measurement Function
ANS	American National Standard
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communication Officials, International
API	Application Programming Interface
AQS	ALI Query Service
ARIB	Association of Radio Industries and Businesses
ASAP	Automated Secure Alarm Protocol
ASD	ANSI-accredited Standards Developer
ATIS	Alliance for Telecommunications Industry Solutions
BBF	Broadband Forum
BCF	Border Control Function
BES	Bulk Electric System
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BICSI	Building Industries Consulting Service International
BIM	Building Information Modeling
BJA	Bureau of Justice Assistance
BSS	Base Station System
BSS – MSC	Base Station System – Mobile-services Switching Center
BWA	Broadband Wireless Access
C2M2	Cybersecurity Capability Maturity Model
CAD	Computer Aided Dispatch
CALEA®	Commission on Accreditation for Law Enforcement Agencies, Inc.
CAP	Common Alerting Protocol
CCSA	China Communications Standards Association
CDMA	Code Division Multiple Access
CEMA	Connection Establishment for Media Anchoring
CET	Cybersecurity and Emerging Threats
CGEIT	Certified in the Governance of Enterprise IT
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CityGML	City Geography Markup Language
CJI	Criminal Justice Information

ACRONYM	DESCRIPTION
CJIS	Criminal Justice Information Services
CLDXF	Civic Location Data Exchange Format
CMAS	Commercial Mobile Alerts Service
CMM	Communication Center Manager (Certification)
CMRS	Commercial Mobile Radio Service
CMSP	Commercial Mobile Service Provider
CN	Core Network
COGO	Coalition of Geospatial Organizations
COMEDIA	Connection-oriented Media
COS	Class of Service
CPE	Customer Premise Equipment
CPP	Common Profile for Presence
CRISC	Certified in Risk and Information Systems Control
CS&C	Office of Cybersecurity and Communications
CSRIC	Communications Security, Reliability, and Interoperability Council
CSX	Cybersecurity Nexus™
CTO	Communications Training Officer
DAS	Distributed Antenna System
DHCP	Dynamic Host Control Protocol
DHS	Department of Homeland Security
DNS	Domain Name System
DOC	Department of Commerce
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DS	Differentiated Services
DSCP	Differentiated Code Point
DSL	Digital Subscriber Line
DSS	Data Security Standard
E911 or E9-1-1	Enhanced 911
EAAC	Emergency Access Advisory Committee
ECES	Entities Consuming Emergency Services
eCNAM	Enhanced Calling Name
ECRF	Emergency Call Routing Function
ecrit	Emergency Context Resolution with Internet Technologies
ECS	Emergency Calling Service
EDGE	Enhanced Data Rates for GSM Evolution
ED-Q	Emergency Dispatch Quality (QI Certification)
EDXL	Emergency Data Exchange Language
EDXL-DE	EDXL Distribution Element
EDXL-RM	EDXL Resource Messaging

ACRONYM	DESCRIPTION
EDXL-SitRep	EDXL Situation Reporting
EDXL-TEC	EDXL Tracking of Emergency Clients
EDXL-TEP	EDXL Tracking of Emergency Patients
EFD	Emergency Fire Dispatch
eHRPD	Evolved High Rate Packet Data
EIA	Electronics Industry Alliance
EIDD	Emergency Incident Data Document
EISI	Emergency Information Services Interface
ELOC	Emergency Location
EMD	Emergency Medical Dispatch
EM-TC	Emergency Management Technical Committee
EMTEL	Emergency Communications
ENUM	E.164 Number Mapping
EP	Emergency Preparedness
EPC	Evolved Packet Core
EPD	Emergency Police Dispatch
EPES	Entities Providing Emergency Services
ERIC	Emergency Response Interoperability Center
ESC	Executive Steering Council
ESGW	Emergency Services Gateway
ESIF	Emergency Services Interconnection Forum
ESInet	Emergency Services IP Network
ESM	Emergency Services & Methodologies
ESMI	Emergency Services Messaging Interface
ESNet	Emergency Services Network
ES-NGN	Emergency Services Next Generation Network
ESNI	Emergency Services Network Interfaces
ESQK	Emergency Services Query Key
ESRD	Emergency Services Routing Digit
ESRK	Emergency Services Routing Key
ESRP	Emergency Services Routing Proxy
ESS	Electronic Safety and Security
ESZ	Emergency Service Zone
ETC	Emergency Telecommunicator Certification
ETS	Emergency Telecommunications Service
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FGDC	Federal Geographic Data Committee
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication

ACRONYM	DESCRIPTION
FLAP	Flexible LDF-AMP Protocol
FRG	First Responders Group
GEOPRIV	Geographic Location/Privacy
GETS	Government Emergency Telecommunications Service
GIS	Geographic Information System
GML	Geography Markup Language
GPRS	General Packet Radio Service
GRA	Government and Regulatory Agency
GSM	Global System for Mobile Communications
HAVE	Hospital Availability Exchange
HDSSC	Homeland Defense and Security Standardizations Collaborative
HELD	HTTP-enabled Location Delivery
HMI	Human Machine Interface
HRPD	High Rate Packet Data
HSGW	eHRPD Serving Gateway
HSSP	Homeland Security Standards Panel
HTTP	Hypertext Transfer Protocol
I^2F	Information Interoperability Framework
IACP	International Association of Chiefs of Police
IAED	International Academies of Emergency Dispatch
ICE	Industry Collaboration Event
ICO	Implementation and Coordination Office
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IIOC	Industrial Internet of Things
IISF	Industrial Internet Security Framework
IJIS	Integrated Justice Information Systems
IM	IP Multimedia
IMIS	Incident Management Information Sharing
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
INP	Interim Number Portability
IoT	Internet of Things
IP	Internet Protocol
IPAWS	Integrated Public Alert and Warning System
IPR	Intellectual Property Rights
ISAO	Information Sharing and Analysis Organization
IS&S	Information Sharing and Safeguarding

ACRONYM	DESCRIPTION
ISDN	Integrated Services Digital Network
ISE	Information Sharing Environment
ISF	Information Security Forum
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ISUP	ISDN User Part
IT	Information Technology
ITL	Information Technology Laboratory
ITS	Institute for Telecommunication Sciences
ITS	Intelligent Transportation Systems
ITS JPO	Intelligent Transportation Systems Joint Program Office
ITU	International Telecommunication Union
ITU-R	ITU—Radiocommunication Sector
ITU-T	ITU—Standardization Sector
IWS	Intelligent Workstation
kHz	Kilohertz
LAN	Local Area Network
LCP	Location Configuration Protocol
LDF	Location Determination Function
LEXS	Logical Entity Exchange Specification
LIS	Location Information Server
LLC	Logical Link Control
LMR	Land Mobile Radio
LNP	Local Number Portability
LoST	Location-to-Service Translation
LTE	Long-term Evolution
LVF	Location Validation Function
M2M	Machine-to-machine
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Mobile Application Part
MDA®	Model Driven Architecture®
MGCP	Media Gateway Control Protocol
MHz	Megahertz
MIB	Management Information Base
MLP	Mobile Location Protocol
MLTS	Multi-line Telephone System
MMES	Multimedia Messaging Emergency Services
MMS	Multimedia Messaging Service
MOS	Mean Opinion Score
MOU	Memorandum of Understanding

ACRONYM	DESCRIPTION
MPC	Mobile Positioning Center
MS	Mobile Station
MS – BSS	Mobile Station – Base Station System
MSAG	Master Street Address Guide
MSC	Mobile-services Switching Center
MSRP	Message Session Relay Protocol
NBAC	NIEM Business Architecture Committee
NCMEC	National Center for Missing and Exploited Children
NE	Network Element
NEC	National Electrical Code®
NENA	National Emergency Number Association
NERC	North American Electric Reliability Corporation
NFPA	National Fire Protection Association
NG911	Next Generation 911
NGES	Next Generation Emergency Services
NGIIF	Next Generation Interconnection Interoperability Forum
NGN	Next Generation Network
NGP	Next Generation Protocols
NGPP	Next Generation Partner Program
NHTSA	National Highway Traffic Safety Administration
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NNI	Network to Network Interface
NOBLE	National Organization of Black Law Enforcement Executives
NPPD	National Protection and Programs Directorate
NPSBN	Nationwide Public Safety Broadband Network
NRIC	Network Reliability and Interoperability Council
NS	National Security
NSA	National Sheriffs' Association
NSDI	National Spatial Data Infrastructure
NTAC	NIEM Technical Architecture Committee
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OEC	Office of Emergency Communications
OGC®	Open Geospatial Consortium
OIC	Office of Interoperability and Compatibility
OJP	Office of Justice Programs
OMA	Open Mobile Alliance
OMB	Office of Management and Budget
OMG®	Object Management Group®
OpenLS	OpenGIS Location Service

ACRONYM	DESCRIPTION
OSP	Originating Service Provider
OSPF	Open Shortest Path First
OSS	Operations Support System
OST-R	Office of the Assistant Secretary for Research and Technology
OT	Operations Technology
pANI	Pseudo Automatic Number Identification
PBX	Private Branch Exchange
PCI	Payment Card Industry
PDE	Position Determining Equipment
PERF	Police Executive Research Forum
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format-Location Object
PML	Physical Measurement Laboratory
PMO	Program Management Office
PRACK	Provisional Response Acknowledgement
PSAP	Public Safety Answering Point
PSHSB	Public Safety and Homeland Security Bureau
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
PTT	Push-to-talk
QA	Quality Assurance
QAE	Quality Assurance Evaluator
QI	Quality Improvement
QoS	Quality of Service
R&D	Research and Development
RF	Radio Frequency
RFAI	Request for Assistance Interface
RFC	Request for Comment
RFI	Request for Information
RG	Residential Gateway
RITA	Research and Innovative Technology Administration
RNA	Routing Number Authority
RTP	Real-time Transport Protocol
RTT	Real-time Text
S&T	Science & Technology Directorate
S8HR	S8 Home Routing
SAFECOM	Wireless Public Safety Interoperable Communications Program
SBC	Session Border Controller
SCC	Standards Coordinating Council
SCTE	Society of Cable Telecommunications Engineers
SDN	Software-defined Networking

ACRONYM	DESCRIPTION
SDO	Standards Development Organization
SDP	Session Description Protocol
SEC	Security
SHS	Secure Hash Standard
SIP	Session Initiated Protocol
SIPREC	SIP Recording
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SPO	Special Programs Office
SR	Selective Router
SRIC	Standards Review and Interpretation Committee
SS7	Signaling System 7
SSO	Standards Setting Organization
SUPL	Secure User Plan Location
TCC	Text Control Center
TDD	Time Division Duplex
TDM	Time Division Multiplexing
TERT	Telecommunicator Emergency Response Taskforce
TFOPA	Task Force on Optimal PSAP Architecture
TIA	Telecommunications Industry Association
TIG	Trusted Identities Group
TISPAN	Telecommunications & Internet Converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TMOC	Telecom Management and Operations Committee
TSAG	Transportation Safety Advancement Group
TSB	Technical Service Bulletin
TSDSI	Telecommunications Standards Development Society, India
TSG	Technical Specification Group
TTA	Telecommunications Technology Association, Korea
TTC	Telecommunication Technology Committee, Japan
TTY/TDD	Teletypewriter/Telecommunications Device for the Deaf
TVRA	Threat Vulnerability Risk Analysis
U.S.	United States
UA	User Agents
UMA	Universal Mobile Access
UML®	Unified Modeling Language®
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URISA	Urban and Regional Information Systems Association

ACRONYM	DESCRIPTION
URL	Uniform Resource Locator
URN	Uniform Resource Number
US-CERT	United States Computer Emergency Readiness Team
USM	User-based Security Model
UTRA	UTMS Terrestrial Radio Access
VACM	View-based Access Control Model
VDB	Validation Database
VoDSL	Voice over Digital Subscriber Line
VoIP	Voice over Internet Protocol
VOP	Voice over Packet
VPC	VoIP Positioning Center
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WSP	Wireless Service Provider
WTSC	Wireless Technologies and Systems Committee
XML	eXtensible Markup Language

Appendix A: Standards Gap Analysis

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
UE (IMS)	• IETF RFC 6881 3GPP IMS Emergency Services • ATIS focus group on over the top applications • CableLabs	Several are still in development. There is no way to quantify all possible end user devices as related to standards.	**ESIF Issue 74** has been developed and defines an IMS counterpart to the NENA i3 specification. Access requirements are being addressed in **ESIF Issue 81.**

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Access Networks	• 3GPP wireless and broadband IMS networks • Generic IP access networks – IETF RFC 6881 • Cable networks • Legacy selective router • Legacy network gateway • Telecommunications network providers connecting by SS7 or centralized automatic message accounting (CAMA)	IMS networks for OTT origination. Cable networks for both cable specific VoIP and OTT origination, DSL networks for both DSL specific VoIP and OTT origination including possibly FTTC and FTTH. The gap for the legacy selective router gateway (LSRG) was the same as the legacy network gateway (LNG), defining a method for acquiring call related location to enable call routing in NG9-1-1 for legacy wireless calls. This method has been resolved and is documented in an approved update of the NENA-STA-010.2-2016 (i3) architecture standard.	Call routing partially addressed in **NENA-STA-010.2-2016**.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Origination Networks			
IMS Origination Networks	• 3GPP TS 23.228, 23.167, 24.229 • ATIS IMS ESInet project (P0030)	None	N/A
Non-IMS Origination Networks	• IETF RFC 6881 • CableLabs PKT-SP-CMSS1.5	Possibly cable networks for both cable specific VoIP and Over-the-top (OTT) origination, DSL networks for both DSL specific VoIP and OTT origination including possibly fiber-to-the-cabinet (FTTC) and fiber-to-the-home (FTTH).	**RFC 5985 (September 2010)** defines and describes an XML-based protocol that can be used to acquire device location information from an LIS within access networks employing both wired technology (DSL, cable) and wireless technology.
Third-party Originating Service Providers (e.g., OnStar, relay services)	• NENA-STA-010.2-2016 • IETF • TIA	Some are proprietary, but they must comply with ESInet interfaces using a standard public interface.	**NENA-STA-010.2-2016** specifies a SIP call interface.
Legacy Origination Networks	• Legacy selective router • Legacy network gateway • NENA-STA-010.2-2016 • Telecommunications network providers connecting by SS7 or CAMA	The gap for the LSRG was the same as the LNG, defining a method for acquiring call related location to enable call routing in NG911 for legacy wireless calls.	Call routing addressed in **NENA-STA-010.2-2016.** Legacy Selective Router Gateway technical standard still in development.
Femto Cell	• NENA 03-509 v1	Specification needs to be updated for NG911.	Still needs to be addressed.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
ESInet			
IP network	• NENA-STA-010.2-2016 • NENA-INF-016.2-2018	Testing, Operations Priority 1	Operations partially addressed in **NENA-STA-010.2-2016.**
Core functions (DNS, DHCP)	• IETF	None	N/A
Interconnect with other ESInets	• NENA-STA-010.2-2016 • EricssonGR-3112	None	N/A
Interconnect with origination networks	• NENA-STA-010.2-2016 • IETF RFC 6881 • EricssonGR-3112	None	N/A
Interconnect with access networks	• NENA-STA-010.2-2016 • IETF RFC 6881	None	N/A
ESInet to PSAP interface	• NENA-STA-010.2-2016	None	N/A
Interconnection with other emergency service entities	• NENA-STA-010.2-2016 • APCO/NENA 2.105.1-2017	None	N/A
Management	• NENA NG9-1-1 Planning Guidelines Information Document • Next Generation 9-1-1 Transition Policy Implementation Handbook	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Location	• 3GPP • ATIS IMS ESInet • IETF • NENA		
PIDF-LO - the location interchange format	• IETF RFC 4119	IMS and IETF/NENA location format incompatibilities.	Addressed by **RFC 477.** Provides a full set of parameters that may be used to describe a civic location.
Functional definition of LIS (and similar terms)	• NENA-STA-010.2-2016	None	N/A
IP-based Emergency Services	• NENA 08-505v.1	Initial version is incomplete. Future revisions of document are required.	**NENA 08-505** (December 2006) acknowledges the first edition of what will be a comprehensive document addressing many access network configurations. This edition has a narrow solutions focus and addresses only the automated mechanism for the residential broadband market.
Location Configuration Protocols		IMS OTT issues.	Still needs to be addressed.
Location Dereferencing Protocols	IETF RFC 6753	Depends on results of ATIS IMS ESInet work.	Still needs to be addressed.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Location Query Protocols (to the extent it is decided they are different from location configuration protocols [LCPs])		Pending other work.	N/A
Location Validation	• IETF RFC 5222 • IETF RFC 5223	None	N/A
Interwork to existing location sources, such as automatic location identification (ALI)	• NENA LSRG • NENA-STA-010.2-2016	None	N/A
GIS & 9-1-1 Attribute Data			
Address, political boundary, and service boundary layer	• NENA-STA-006.1.1-2020	None	N/A
Service boundary polygons – how call or vehicular routing occurs	• NENA-STA-010.2-2016	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Distribution to other entities outside the normal area of service	• NENA-STA-010.2-2016 • NENA-STA-0115-10-2018	Further work needed. In 2018, NENA began development of work that will define both the WFS (features) and WMS (image) to allow PSAPs and other authorized entities to select and download GIS data that can be used for allowing tactical map displays for handling 911 calls from otherwise out-of-service area PSAPs.	Still needs to be addressed.
Adjustment of polygon layers to match road centerline and parcel boundaries	• NENA Emergency Call Routing Function (ECRF)/Location Validation Function (LVF)	Further work needed.	**NENA-STA-010.2-2016**, describes the end state required for NG9-1-1.
Call Signaling			
Basic SIP call signaling	• IETF RFC 3261 • IETF RFC 6881	None	N/A
IMS SIP call signaling	• 3GPP	IMS ESINET identified some gaps.	Still needs to be addressed.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Call Routing			
Routing database (ECRF)	• IETF RFC 5222 • IETF RFC 5223 • NENA-STA-010.2-2016	None	N/A
Routing proxies (Emergency Services Routing Proxy [ESRP])	• IETF RFC 3261 • IETF RFC 6881 • NENA-STA-010.2-2016	None	N/A
Policy-based routing	• NENA-STA-010.2-2016	None	N/A
Media			
Voice	• 3GPP • IETF • NENA	None	N/A
Video	• 3GPP • IETF • NENA	None	N/A
Text	• 3GPP • IETF • NENA	None	N/A
Data only – "non-human initiated"	• 3GPP • IETF • NENA	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Real-time Text (RTT), IMS Multimedia Messaging Emergency Services (MMES), "total conversation"	• 3GPP • IETF • NENA	None	N/A
Accessibility			
EAAC issues and gaps in i3	• FCC EAAC • ATIS INES Incubator • FCC NG911 Notice of Proposed Rulemaking (NPRM)	Identify the teletypewriter (TTY) replacement technology, adoption of that technology, and method of delivering TTY replacement to the NG911 and PSAP. Output of FCC NG911 NPRM may identify additional gaps.	Still needs to be addressed. The FCC EAAC Report lists some gaps and makes recommendations to fill some of these gaps. **NENA-STA-010.2-2016** begins to identify these requirements. The FCC is developing a record on this issue.
Interface between IMS-originating networks and relay services	• FCC EAAC • ATIS	How calls originating from IMS connect to the relay service. Also, given that 911 calls originating on IMS are direct to the ESInet, how do responders get notification that a relay service needs to be involved? Need to have specification developed to define how IMS interfaces with relay services.	Still needs to be addressed.
Callback	• 3GPP • IETF • NENA		

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Additional Data about:	• NENA	NENA 71-001: NENA Standard for NG9-1-1 Additional Data – There are significant gaps on how this data is obtained, stored, accessed, secured, and maintained.	**NENA 71-001** describes the use of additional data available with NG9-1-1 (associated with a call, a location, a caller, and a PSAP) that assists in determining the appropriate call routing and handling. Version 2 will include the EIDD specification. **NENA STA-NG9-1-1,** additional data under review.
Call	• NENA-STA-010.2-2016 • NENA 71-001 • IETF additional data • 3GPP • ATIS IMS ESInet	None	N/A
Caller	• NENA-STA-010.2-2016 • NENA 71-001 • ATIS IMS ESInet	Emergency Medical Data Priority 2	Addressed by **NENA 71-001** Appendix A, page 23. **NENA 71-001** describes the use of additional data available with NG9-1-1 (associated with a call, a location, a caller, and a PSAP) that assists in determining the appropriate call routing and handling. Version 2 will include the EIDD specification. **NENA-STA-010.2-2016**, identifies an identity searchable additional data repository (IS-ADR) that can be used.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Premise (e.g., floor plans, alarm data, etc.)	• NENA-STA-010.2-2016 • NENA 71-001 • NIST	Further work needed.	Partially addressed by **NENA 71-001,** version 1, page 28. NENA 71-001, Version 2, and **NENA-STA-010.2-2016,** discuss floor plans as a source of additional data.
PSAP	• APCO • NENA • EIDD	Further NIEM work needed.	Still needs to be addressed.
Logging			
Within the ESInet and related functions	• NENA-STA-010.2-2016	NENA and APCO have identified a number of gaps, such as Radio over IP (RoIP). FirstNet may be an option in the future to address this.	**NENA-STA-010.2-2016** may address some of the gaps.
Within the PSAP	• NENA NG PSAP	None	N/A
Call origination	• NENA • IETF	Could have IMS and other origination network impacts.	N/A
Bridging/Conference Calls	• NENA • IETF	Could have IMS and other origination network impacts.	Still needs to be addressed.

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Security			
Credentials	• 3GPP • IETF • NENA • ATIS IMS ESInet • NIST	Accessibility and privacy controls across the enterprise and diverse systems are still in development.	NIST National Strategy for Trusted Identities in Cyberspace. NENA NG9-1-1 Interoperability Oversight Commission (NIOC) to operate the PSAP Credentialing Agency (PCA)
Securing protocol interaction including authentication, integrity protection, privacy	• IETF • NENA-STA-010.2-2016 • ATIS IMS ESInet • NIST	Accessibility and privacy controls across the enterprise and diverse systems are still in development.	NIST National Strategy for Trusted Identities in Cyberspace.
Attack Mitigation	• NENA-STA-010.2-2016 • NIST	None	N/A
End User Location Integrity	• IETF • ATIS IMS ESInet	Standards in development.	Still needs to be addressed.
Federated credentials for sharing credentials between systems			Still needs to be addressed.
Transition (including data)			
Wireline	• NENA	None	N/A
Wireless	• NENA	None	N/A
VoIP	• NENA	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
PSAP aspects	• NENA • ATIS RFAI	None	N/A
Relay services (e.g., IP relay, video relay, etc.)	• NENA	None	N/A
TTY	• NENA	None	N/A
Legacy PSAP	• NENA	None	N/A
Testing	• NENA	Several gaps associated with Testing.	**NENA 06-750** is a policy document that reflects changes in: IP technology; implementation and testing; training; and use of building code fire zones to facilitate the creation of the Emergency Response Location and MLTS.
Self-test	• IETF • NENA	None	N/A
Discrepancy Reporting	• NENA	None	N/A
Data Management and Maintenance	• NENA-REQ-002.1-2016	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Dispatch Systems			
Interface to call processing or CAD systems			
Sharing Call Information (EIDD)	• APCO/NENA	None	APCO/NENA 2.105 2017 is a standard that provides a standardized, industry-neutral NIEM conformant (XML-based) specifications for exchanging emergency incident information to agencies and regions that implement NG9-1-1 and IP-based emergency communications systems. NENA is updating the exchange data package with the Emergency Incident Data Object (EIDO)
Interface to dispatch broadband networks (FirstNet)	• N/A	N/A	Still needs to be addressed.