The National 911 Program

Next Generation 911 (NG911) Standards Identification and Review

A compilation of existing and planned standards for NG911 systems

Washington, DC
March 2015

DOCUMENT CHANGE HISTORY

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

Table of Contents

Introduction

One of the most critical aspects of transforming the nation's public safety answering points (PSAP) 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 will be 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 was begun on NG911 standards in 2003 when the National Emergency Number Association (NENA) initiated technical requirements and definition work on the core Internet Protocol (IP) functionality and architecture.

Beyond the walls of the 911 Public Safety Answering Point (PSAP), 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 U.S. Department of Transportation's (USDOT) National Highway Traffic Safety Administration (NHTSA), has compiled this list of standards activities related to NG911. The contents of this document have been vetted by the standards development organizations (SDOs) mentioned herein, to assess the status of specific standards. This is a living document, and the National 911 Program will publish,[1] monitor, support, and promote the activities of SDOs in establishing a comprehensive set of standards for NG911.

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.

What Is a Standard?

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

> ***A 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

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

[2] ISO, *ISO/IEC Directives, Part 2: Rules for the structure and drafting of International Standards.* Available at: http://isotc.iso.org/livelink/livelink?func=ll&objId=4230456&objAction=browse&sort=subtype (last accessed February 26, 2015).

in generic medications), standards guide the quality, safety, and security of products or processes. Standards are widely used in all areas throughout the U.S. government, 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 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

Open standards are not proprietary, which means the standard is available to anyone. The 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:

"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.

---

[3] Standards.gov, *What Are Standards?* Available at: http://www.nist.gov/standardsgov/definestandards.cfm (last accessed February 26, 2015).

[4] RITA Intelligent Transport Systems, *What Are Standards?* Available at: http://www.standards.its.dot.gov/LearnAboutStandards/ITSStandardsBackground (last accessed February 26, 2015).

[5] ANSI Essential Requirements: Due process requirements for American National Standards, January 2015. As viewed at http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2015_ANSI_Essential_Requirements.pdf(last viewed February 26, 2015).

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 center, Internet, infrastructure, wireline, and wireless service providers
- Transportation agencies
- Local, state, and federal governments
- 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.

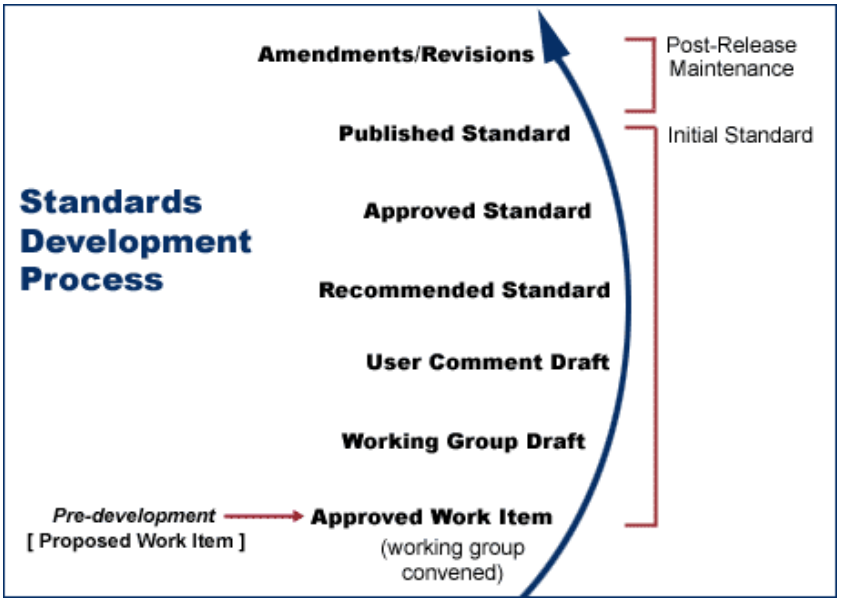
How Are Standards Developed?

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,

[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.

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]



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. For this reason, the majority of standards require periodic review and, potentially, revision. As a general rule, organizations such as ANSI and ISO assert that standards should be reviewed at intervals of not more than 5 years.[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

[9] Research and Innovative Technology Administration (RITA) Intelligent Transportation Systems (ITS), *Standards Development Process.* http://www.standards.its.dot.gov/LearnAboutStandards/StandardsDevelopment (last accessed February 26, 2015).
[10] IEEE Volunteer Training Program, *How are Standards Made?* Available at: http://standards.ieee.org/develop/process.html (last accessed February 26, 2015).
[11] ANSI Essential Requirements: Due process requirements for American National Standards, January 2015. As viewed at http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/American%20National%20Standards/Procedures,%20Guides,%20and%20Forms/2015_ANSI_Essential_Requirements.pdf (last viewed February 26, 2015).

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 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

In an effort to organize the numerous standards that are of interest and applicability to the NG911 community, this document groups standards into the following six categories:

- **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.

The Need for Standards in NG911

It is imperative that the necessary NG911-related standards and technology are determined and available for the 911 Authorities and PSAPs to support transitioning to an open, non-proprietary NG911 system. Without the critical standards and technologies in place, service and equipment providers may develop new, vendor-

[12] ANSI Standards Activities, *Domestic Programs (American National Standards) Overview.* Available at: http://www.ansi.org/standards_activities/domestic_programs/overview.aspx (last accessed February 26, 2015).

specific solutions. This un-standardized, 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 carriers 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 the 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.

Standards and Best Practices Organizations

The following 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, a summary of the organization includes its purpose (e.g., charter, mission statement), pertinent subgroups within the organization (e.g., committees, working groups), standards involvement, formal activities coordinated with other SDOs, and a statement of the effect of its activities on NG911 implementation. In each case, the information was reviewed by the SDO. Additionally, the 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 Appendix A.

[13] P.L. 104-113. Available at: http://www.nist.gov/standardsgov/nttaa-act.cfm (last accessed February 26, 2015).

3rd Generation Partnership Project (3GPP)

Name 3rd Generation Partnership Project (3GPP)

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

Summary The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standards development organizations (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]), known as "Organizational Partners," and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies.

Purpose The purpose of 3GPP is to prepare, approve, and maintain globally applicable technical specifications and technical reports for a 3rd Generation Mobile System based on the evolved Global System for Mobile Communications (GSM) core networks, and the radio access technologies supported by the Organizational Partners (i.e., Universal Terrestrial Radio Access [UTRA], both frequency division duplex [FDD] and time division duplex [TDD] modes), to be transposed by the Organizational Partners into appropriate deliverables (e.g., standards).[14]

Relevant Specification Groups

- TSG CT: The Technical Specification Group (TSG) Core Network and Terminals (CT) is responsible for specifying terminal interfaces (logical and physical), terminal capabilities (e.g., execution environments) and the core network element of 3GPP systems.[15]
- TSG SA: The TSG Service and System Aspects (TSG-SA) is responsible for the overall architecture and service capabilities of systems based on 3GPP specifications and, as such, has a responsibility for cross TSG coordination.[16]

[14] 3GPP, *Third Generation Partnership Project Agreement.* Available at: http://www.3gpp.org/ftp/Inbox/2008_web_files/3gppagre.pdf (last accessed February 26, 2015).
[15] 3GPP, *CT Plenary Core Networks and Terminals.* Available at: http://www.3gpp.org/CT (last accessed February 26, 2015).
[16] 3GPP, *Service and System Aspects.* Available at: http://www.3gpp.org/-SA- (last accessed February 26, 2015).

Standards

- 3GPP TS 23.167: *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions*
- 3GPP TS 23.228: *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2*
- 3GPP TS 23.517: *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Functional Architecture.*
- 3GPP TS 24.229: *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*
- 3GPP TS 29.010: *3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 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)*
- 3GPP TSG SA Release 12*: 3rd Generation Partnership Project; Exploits new business opportunities such as Public safety and Critical Communications, Explores Wi-Fi integration and system capacity and stability*

Coordinated Activities

- Open Mobile Alliance (OMA): Based on the "OMA-3GPP Standardization Collaboration," the OMA and the 3GPP will work to update on a regular basis the list of dependencies between each organization's specifications and work in progress.[17]

Effects on NG911

- Develops standards that enable text and multimedia transmission from the caller to the NG911 system (transport of data).
- Develops standards adhered to by originating service providers' (OSP) network and applications services for emergency calling.
- Supports location requirements and standards.

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

[17] Open Mobile Alliance, *3GPP Dependencies.* Available at: http://www.openmobilealliance.org/Technical/3gpp.aspx (last accessed February 26, 2015).

3rd Generation Partnership Project 2 (3GPP2)

Name 3rd Generation Partnership Project 2 (3GPP2)

Type International Standards Organization—Industry (Mobile Broadband/UMTS)

Summary

The 3GPP2 is a collaboration among groups of telecommunications associations to develop a globally applicable 3G mobile telephone system specification within the scope of the IMT-2000 project of the International Telecommunication Union (ITU). 3GPP2 specifications are based on the Code Division Multiple Access 2000 (CDMA2000) 3G mobile technology standards. 3GPP2 can be characterized as a collaborative 3G telecommunications specifications-setting project:

- Comprising North American and Asian interests developing global specifications for ANSI/Telecommunications Industry Alliance (TIA)/Electronics Industry Alliance (EIA)-41 Cellular Radio Telecommunication Intersystem Operations network evolution to 3G.
- Developing global specifications for the radio transmission technologies (RTT) supported by ANSI/TIA/EIA-41.

3GPP2 was born out of the ITU's IMT-2000 initiative covering high-speed, broadband, and IP-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming, and seamless services independent of location. IMT-2000 is intended to bring high-quality mobile multimedia telecommunications to a worldwide mass market by achieving the goals of increasing the speed and ease of wireless communications, responding to the problems faced by the increased demand to pass data via telecommunications, and providing "anytime, anywhere" services.[18]

Relevant Specification Groups

- TSG-S: The Services and Systems Aspects TSG (TSG-S) is responsible for development of service capability requirements for systems based on 3GPP2 specifications. It is also responsible for high-level architectural issues, as required, to coordinate service development across the various TSGs.[19]
- TSG-X: The TSG Core Networks (TSG-X) is responsible for the specifications of the core network part of systems, based on 3GPP2 specifications.[20]

Standards

- 3GPP2 S.R0006-529-A: *Wireless Features Description: Emergency Services*
- 3GPP2 X.S0049-0: *All-IP Network Emergency Call Support*
- 3GPP2 X.S0057-A: *E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects*
- 3GPP2 X.S0060-0: *HRPD Support for Emergency Services*

[18] 3GPP2, *About 3GPP2: What is 3GPP2?* Available at: http://www.3gpp2.org/Public_html/Misc/AboutHome.cfm (last accessed February 26, 2015).
[19] 3GPP2, *TSG-S Services and Systems Aspects.* Available at: http://www.3gpp2.org/Public_html/S/index.cfm (last accessed February 26, 2015).
[20] 3GPP2, *TSG-X Core Networks.* Available at: http://www.3gpp2.org/Public_html/X/index.cfm (last accessed February 26, 2015).

Coordinated Activities	• Open Mobile Alliance (OMA): Based on the OMA-3GPP2 Standardization Collaboration, the OMA and the 3GPP2 will work to update on a regular basis the list of dependencies between each organization's specifications and work in progress.[21] • Telecommunications Industry Association (TIA): 3GPP2 is a collaborative effort among five officially recognized SDOs—Association of Radio Industries and Businesses (ARIB), China Communications Standards Association (CCSA), Telecommunications Technology Association (TTA), Telecommunications Technology Committee (TTC), and TIA.
Effects on NG911	• Develops standards that enable text and multimedia transmission from the caller to the NG911 system (transport of data). • Supports location requirements and standards.
Cross-Reference to Published Standards	• 3GPP2 specifications and reports are converted into standards by each of the Project's Organizational Partners. http://www.3gpp2.org/Public_html/specs/index.cfm
Website	http://www.3gpp2.org/

[21] Open Mobile Alliance, *3GPP2 Dependencies.* Available at: http://www.openmobilealliance.org/Technical/3gpp2.aspx (last accessed February 26, 2015).

American National Standards Institute (ANSI)

Name	American National Standards Institute (ANSI)
Type	National Standards Organization
Summary	ANSI is a private, not-for-profit organization that oversees development of voluntary consensus standards in the United States. Activities include accrediting programs, assessing conformance, and approving standards developed by organizations such as Alliance for Telecommunications Industry Solutions (ATIS) and Association of Public-Safety Communications Officials (APCO). ANSI, itself, does not set standards, but approves and accredits other SDOs. Membership is composed of government agencies, academic and international bodies, and individuals. ANSI is the official U.S. representative to the ISO and, via the U.S. National Committee, the IEC.
Mission	To enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.[22]
Relevant Standards Panel	• Homeland Security Standards Panel (HSSP): ANSI's Homeland Security Standards Panel (ANSI-HSSP) has as its mission to identify existing consensus standards, or, if none exist, assist the Department of Homeland Security (DHS) and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors to meet the needs of the nation in this critical area.[23]
Coordinated Activities	• National Institute of Standards and Technology (NIST): A Memorandum of Understanding (MOU) exists between NIST and ANSI that agrees on the need for a unified national approach to develop the best possible national and international standards.[24] • ISO: ANSI is the sole U.S. representative and dues-paying member of the ISO. As a founding member of the ISO, ANSI plays a strong leadership role in its governing body.[25]
Effects on NG911	• Validates the standards development process for SDOs that produce standards affecting NG911.
Website	http://www.ansi.org/

[22] American National Standards Institute, *About ANSI Overview.* Available at: http://www.ansi.org/about_ansi/overview/overview.aspx (last accessed February 26, 2015).
[23] ANSI Standards Activities, *Homeland Security Standards Panel.* Available at: http://www.hssp.org/standards_activities/standards_boards_panels/hssp/overview.aspx (last accessed February 26, 2015).
[24] National Institute of Standards of Technology Standards Coordination and Conformity Group, *Memorandum of Understanding between the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST)*. Available at: http://gsi.nist.gov/global/docs/ANSINISTMOU2000.pdf (last accessed February 26, 2015).
[25] American National Standards Institute, *ANSI Accredited of U.S. Technical Advisory Groups (TAGs) to ISO.* Available at: http://www.ansi.org/standards_activities/iso_programs/tag_iso.aspx (last accessed February 26, 2015).

Association of Public-Safety Communications Officials (APCO)

Name Association of Public-Safety Communications Officials (APCO)

Type National Standards Organization (American National Standards Institute [ANSI] Accredited)

Summary APCO International is the world's largest organization dedicated to public safety communications and is an ANSI-accredited SDO committed to ensuring public safety communications personnel have a role in the development of standards that affect the industry. APCO's standards development activities have a broad scope, ranging from actual development of standards to representation of public safety communications organizations in other standards development areas.[26]

Mission APCO International develops standards and disseminates information about critical issues such as wireless 911, staffing and retention, and the impact of emerging technologies. APCO participates in numerous committees, partnerships, and government initiatives. APCO supports agencies around the country grappling with the industry's toughest issues by delivering a variety of resources and engaging in the latest research to find common solutions.[27]

Relevant Committees

- 911/Emerging Technologies: The 911/Emerging Technologies Committee provides subject-matter experts to the International Committee related to U.S. 911 issues, has established at least two strategic alliances related to the mission of APCO, provides leadership opportunities for committee members by establishing work groups within the 911/Emerging Technologies Committee, and has established a 911 public policy work group to identify key areas of public policy that APCO should influence or advocate for related 911 operations.[28]

[26] APCO, *About APCO.* Available at: http://apcointl.org/about-apco.html and https://www.apcointl.org/standards.html (last accessed February 26, 2015).
[27] APCO, *911 Resources.* Available at: http://apcointl.org/resources.html(last accessed February 26, 2015).
[28] APCO, *9-1-1 Emerging Technologies Committee.* Available at: https://apconetforum.org/eweb/DynamicPage.aspx?Webcode=APCOCommDescript&APCOcmt_key=11e96d6f-46f8-4044-be27-a7aa8233b72f (last accessed February 26, 2015).

Relevant Projects

- Project 25: A joint effort of APCO and the National Association of State Telecommunications Directors, Project 25 concerns the development of standards for digital telecommunications technology, including an objective to determine consensus standards for digital radio equipment embracing elements of interoperability, spectrum efficiency, and cost economies.[29]
- Project 36: This project was developed to research and develop universal standards for Computer Aided Dispatch (CAD) and CAD-to-CAD exchanges. The goal was to develop effective processes for the exchange of data between third-party call centers such as alarm companies and PSAPs.[30]
- Project 42 (Global Operating Picture): The goal of Project 42 is to identify those areas where standards are needed to achieve system interoperability and create a common operating picture at all levels, horizontal and vertical.[31]

[29] APCO, *911 Resources APCO Projects.* Available at: http://apcointl.org/about-apco/apco-projects.html (last accessed February 26, 2015).
[30] APCO, *911 Resources APCO Projects.* Available at: http://apcointl.org/about-apco/apco-projects.html (last accessed February 26, 2015).
[31] APCO, *911 Resources APCO Projects.* Available at: http://apcointl.org/about-apco/apco-projects.html (last accessed February 26, 2015).

Standards

- APCO ANS 1.101.2-2010: *Standard for Public Safety Telecommunicators When Responding to Calls of Missing, Abducted, and Sexually Exploited Children* (In Revision)
- APCO/NENA ANS 1.102.2-2010: Public Safety Answering Point (PSAP) Service Capability Criteria Rating Scale
- APCO ANS 1.103.2-2013: *Wireless 9-1-1 Deployment and Management Effective Practices Guide*
- APCO/NENA ANS 1.105.1-2009: *Standard for Telecommunicator Emergency Response Taskforce (TERT) Deployment* (In Revision)
- APCO/NENA 1.107.1-201x: *Quality Assurance / Quality Improvement* (In Development)
- APCO 1.108.1-201x: *Minimum Operational Standards for the Use of TTY/TDD devices in the Public Safety Communications Center* (In Development)
- APCO 1.110.1-201x: *Unified Computer Aided Dispatch Functional Requirements (UCADFR*) (In Development)
- APCO ANS 1.111.1-2013: *Public Safety Communications Common Disposition Codes for Data Exchange*
- APCO ANS 1.112.1-2014: *Best Practices for the Use of Social Media in Public Safety Communications*
- APCO 1.114.1-201x: *Vehicle Telematics Best Practices* (In Development)
- APCO 1.115.1-201x: *Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications* (In Development)
- APCO/CSAA 2.101.2-2014: *Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)* (In Revision)
- APCO 2.102.1.201x: *Advanced Automatic Collision Notification (AACN) Data Set* (In Development)
- APCO ANS 2.103.1-2012: *Public Safety Communications Common Incident Types For Data Exchange*
- APCO/NENA 2.105.1201x *NG9-1-1 Emergency Incident Data Document (EIDD)* (In Development)
- APCO ANS 3.101.2-2013: *Core Competencies and Minimum Training Standards for Public Safety Communications Training Officer (CTO)*
- APCO ANS 3.102.1-2012: *Core Competencies and Minimum Training Requirements for Public Safety Communications Supervisor*
- APCO ANS 3.103.1-2010: *Minimum Training Standards for Public Safety Telecommunicators* (In Revision)
- APCO ANS 3.104.1.2012 : *Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator*
- APCO 3.105.1.201x: *Minimum Training Standard for TTY/TDD Use in the Public Safety Communications Center* (In Development)
- APCO ANS 3.106.1.2013: *Core Competencies and Minimum Training Standards for Public Safety Communications Quality Assurance Evaluator* (QAE)
- APCO 3.107.1.201x: *Core Competencies and Minimum Training Standards for Public Safety Communications Technician* (In Development)
- APCO ANS 3.108.1.2014: *Core Competencies and Minimum Training Standards for Public Safety Communications Instructor*
- APCO ANS 3.109.2.2014: *Core Competencies and Minimum Training Standards for Public Safety Communications Manager/Director*

Coordinated Activities

- ANSI: As an ANSI-accredited Standards Developer (ASD), APCO International is dedicated to ensuring public safety communications personnel have a role in the development of standards that affect communications professionals.[32]
- Vehicular Emergency Data Set (VEDS): The Vehicular Emergency Data Set (VEDS) provides useful and critical data elements and the schema set needed to facilitate an efficient emergency response to vehicular emergency incidents. [33]

Websites

http://www.apcointl.org/
http://www.apcostandards.org/

[32] APCO, *911 Resources.* Available at: http://apcointl.org/standards.html (last accessed February 26, 2015).
[33] APCO, *AACN/VEDS Overview*. Available at: http://apcointl.org/resources/aacn-and-veds.html (last accessed February 26, 2015).

Alliance for Telecommunications Industry Solutions (ATIS)

Name Alliance for Telecommunications Industry Solutions (ATIS)

Type Standards Setting Organization—Industry (Telecommunications)

Summary ATIS is a standards organization that develops technical and operational standards for the telecommunications industry. Member companies include telecommunications service providers, equipment manufacturers, public sector entities, and others. ATIS is accredited by ANSI; is a member organization of other standards organizations, including the Radio Communication Sector (ITU-R) and Standardization Sector (ITU-T) of the ITU; and is an Organizational Partner of 3GPP.

ATIS prioritizes a wide range of industry technical and operational issues and creates interoperable, implementable standards and solutions in a manner that efficiently allocates and coordinates industry resources. Its activities provide the basis for the industry's delivery of:

- Existing and next generation IP-based infrastructures
- Reliable converged multimedia services, including Internet Protocol television (IPTV)
- Enhanced operations support systems and business support systems
- Improved levels of service quality and performance[34]

[34] ATIS, *About ATIS.* Available at: http://www.atis.org/about/ (last accessed February 26, 2015).

Relevant Committees/ Subcommittees

- Emergency Services Interconnection Forum (ESIF): ESIF, composed of wireless and wireline network service providers, manufacturers, public sector entities, and providers of support services, facilitates identification and resolution of technical issues related to the interconnection of telephony and emergency services networks.[35]
    - Next Generation Emergency Services (NGES) Subcommittee: The NGES Subcommittee coordinates emergency services needs and issues with and among SDOs and industry forums/committees, and within and outside ATIS; and develops emergency services (e.g., Enhanced 911 [E911]) standards and other documentation related to advanced (i.e., next generation) emergency services architectures, functions, and interfaces for communications networks.[36]
- Next Generation Interconnection Interoperability Forum (NGIIF): The NGIIF addresses next-generation network interconnection and interoperability issues associated with emerging technologies. It develops operating procedures that involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security and testing between network operators, with a current focus on call completion.[37]
- Packet Technologies and Systems Committee (PTSC): PTSC develops and recommends standards and technical reports related to packet services and packet service architectures, in addition to related subjects under consideration in other North American and international standards bodies.[38]
- Wireless Technologies and Systems Committee (WTSC): WTSC develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC also develops and recommends positions on related subjects under consideration in other North American, regional, and international standards bodies.[39]

[35] ATIS, *Committees & Forums.* Available at: http://www.atis.org/committees/index.asp (last accessed February 26, 2015).
[36] ATIS, *NGES: Next Generation Emergency Services Subcommittee.* Available at: http://www.atis.org/esif/nges.asp (last accessed February 26, 2015).
[37] ATIS, *NGIIF: Next Generation Interconnection Interoperability Forum*. Available at: http://www.atis.org/NGIIF/index.asp (last accessed February 26, 2015).
[38] ATIS, *The Packet Technologies and Systems Committee (PTSC).* Available at: http://www.atis.org/0191/index.asp (last accessed February 26, 2015).
[39] ATIS, *The Wireless Technologies and Systems Committee (WTSC).* Available at: http://www.atis.org/0160/index.asp (last accessed February 26, 2015).

Standards

- ATIS-0500002.2008(R2013): *Emergency Services Messaging Interface (ESMI)*
- ATIS-0500003: *Routing Number Authority (RNA) for pseudo Automatic Number Identification Codes (pANIs) Used for Routing Emergency Calls: pANI Assignment Guidelines and Procedures*
- ATIS-0500005: *Standard Wireless Text Message Case Matrix*
- ATIS-0500006.2008(R2013): *Emergency Information Services Interfaces (EISI) ALI Service*
- ATIS-0500007.2008(R2013): *Emergency Information Services Interface (EISI) Implemented with Web Services*
- ATIS-0500013: *Approaches to Wireless E9-1-1 Indoor Location Performance Testing*
- ATIS-0500015.2010: *Flexible LDF-AMF (Location Determination Function – Access Measurement Function) Protocol (FLAP) Specification*
- ATIS-0500017: *Technical Report - Considerations for an Emergency Services Next Generation Network (ES-NGN)*
- ATIS-0500018: *P-ANI Allocation Tables for ESQKs, ESRKs, and ESRDs*
- ATIS-0500019.2010: *Request for Assistance Interface (RFAI) Specification*
- ATIS-0500023: *Applying 3GPP Common IMS to NG9-1-1 Networks*
- ATIS-0500024: *Technical Report - Comparison of SIP Profiles*
- 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*
- ATIS-0700015.v002: *ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination*
- ATIS-1000026: *Session Border Controller Functions and Requirements*
- ESIF Issue 76: *Analysis of Unwanted User Service Interactions with NG911 Capabilities*
- ESIF Issue 81: *Applying Common IMS to NG911 networks (Stage 2 & 3 Specification)* (In Development)
- ESIF Issue 82: *IMS-based Next Generation Emergency Services Network Interconnection*
- ESIF Issue 85: *Supplemental Guide to ATIS-0700015 for Public Safety*
- J-STD-036-B (R2013): *Enhanced Wireless 9-1-1 Phase 2*
- J-STD-110: *Joint ATIS/TIA Native SMS to 911 Requirements & Architecture Specification*
- J-STD-110.01: *Joint ATIS/TIA Implementation Guideline for J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification*
- J-STD-110.a: *Joint ATIS/TIA Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification*

Coordinated Activities	• 3GPP, ETSI, ITU, and NENA: The NGES Subcommittee emphasizes standards development as it relates to North American communications networks, in coordination with the development of standards activities, including relevant ATIS committees (e.g., PTSC), ITU, 3GPP, ETSI, and NENA. [40] • ANSI: ATIS is an ANSI-accredited SDO.[41] • Telecommunications Industry Association (TIA): An MOU exists between ATIS and TIA to jointly sponsor and work cooperatively in the development of joint standards documents that are of mutual interest.[42]
Effects on NG911	• Develops standards adhered to by originating service providers' (OSP) network and applications services for emergency calling. • Supports location requirements and standards.
Websites	http://www.atis.org/

[40] ATIS, *NGES: Next Generation Emergency Services Subcommittee*. Available at: http://www.atis.org/esif/nges.asp (last accessed February 26, 2015).
[41] ANSI, *ANSI Accredited Standards Developers.* Available at: http://publicaa.ansi.org/sites/apdl/Lists/American%20National%20Standards/AllItems.aspx (last accessed February 26, 2015).
[42] ATIS, *General Principles in Sponsorship of Joint Standards Activities Between the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA).* Available at: http://www.atis.org/legal/Docs/MOU/TIA.pdf (last accessed February 26, 2015).

Broadband Forum (BBF)

Name	Broadband Forum (BBF)
Type	Industry (Broadband)
Summary	The BBF is the central organization driving broadband wireline solutions and empowering converged packet networks worldwide to better meet the needs of vendors, service providers, and their customers.
Mission	Develop multi-service broadband packet networking specifications addressing interoperability, architecture, and management. BBF's work enables home, business, and converged broadband services, encompassing customer, access, and backbone networks. [43]
Relevant Working Groups	• End-to-End Architecture: This group's mission is to oversee and coordinate all access architecture and transport-related technical work within the Forum. Scope includes access architecture encompassing interface definitions and nodal functional requirements—from residential gateway (RG) through access node, aggregation network, and broadband network gateway (BNG) to peering interfaces with network and application service providers. The focus is end-to-end service delivery across this domain encompassing equipment requirements to support capabilities such as quality of service (QoS) and multicast functionality. Working group interests also encompass policy and control of the key network elements and protocol interworking requirements. All broadband wireline access technologies are within the scope of this access architecture work (e.g., Digital Subscriber Line [DSL], Gigabit Passive Optical Network [GPON], and point-to-point fiber). Wireless broadband access technologies are addressed via liaison with the appropriate standards body (e.g., WiMAX Forum, 3GPP, etc.). Consideration is also given to the relative energy efficiency aspects of access architectures.[44] • Broadband Home: This group's mission is to provide the Broadband industry with technical specifications that define the devices in the DSL broadband home and eases the deployment and management of broadband services. [45]
Coordinated Activities	• WiMAX Forum, 3GPP: BBF works alongside mobile-related partners to ensure all their work is aligned.[46]
Website	http://www.broadband-forum.org/

[43] Broadband Forum, *Technical Working Groups.* Available at: http://www.broadband-forum.org/technical/technicalworkinggroups.php (last accessed February 26, 2015).
[44] Broadband Forum, *Technical Working Groups.* Available at: http://www.broadband-forum.org/technical/technicalworkinggroups.php (last accessed February 26, 2015).
[45] Broadband Forum, *Technical Working Groups.* Available at: http://www.broadband-forum.org/technical/technicalworkinggroups.php (last accessed February 26, 2015).
[46] Broadband Forum, *Frequently Asked Questions.* Available at: http://www.broadband-forum.org/about/faqbroadbandforum.php (last accessed February 26, 2015).

Commission on Accreditation for Law Enforcement Agencies (CALEA)

Name	Commission on Accreditation for Law Enforcement Agencies (CALEA)
Type	Professional Organization
Summary	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). The purpose of CALEA's Accreditation Program is 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; establishing and administering an accreditation process; and recognizing professional excellence.[47]
Relevant Committees	• Standards Review and Interpretation Committee (SRIC)
Standards	• Standards for Law Enforcement Agencies • Standards for Public Safety Communications Agencies
Website	http://www.calea.org/

[47] CALEA, *About Us,* Available at: http://www.calea.org/content/commission (last accessed February 26, 2015).

Department of Commerce (DOC)

Name Department of Commerce (DOC)

Type Government Agency

Summary The U.S. DOC promotes job creation, economic growth, sustainable development and improved standards of living for all Americans by working in partnership with businesses, universities, communities, and our nation's workers. The department touches the daily lives of the American people in many ways, with a wide range of responsibilities in the areas of trade, economic development, technology, entrepreneurship and business development, environmental stewardship, and statistical research and analysis.[48]

Relevant Agencies

- NIST: The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the DOC. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.[49]
  - Information Technology Laboratory (ITL): ITL is one of the major research components of NIST. ITL accelerates the development and deployment of information and communications systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.[50]
  - Physical Measurement Laboratory (PML): The PML develops and disseminates the national standards of length, mass, force and shock, acceleration, time and frequency, electricity, temperature, humidity, pressure and vacuum, liquid and gas flow, and electromagnetic, optical, microwave, acoustic, ultrasonic, and ionizing radiation. Its activities range from fundamental measurement research through the provisioning of measurement services, standards, and data. It supports the research community in such areas as communication, defense, electronics, energy, environment, health, lighting, manufacturing, microelectronics, radiation, remote sensing, space, and transportation.[51]
  - Office of Law Enforcement Standards (OLES) Special Programs Office (SPO): The SPO fosters communication and collaboration between NIST and external communities focused on critical national needs. The focus areas include: environment, energy, forensic science, healthcare, homeland security, information technology (IT) and cybersecurity, manufacturing, and physical infrastructure. In order to do this, the SPO works closely and forges

[48] Department of Commerce, *About the Department of Commerce.* Available at: http://www.commerce.gov/about-department-commerce (last accessed February 26, 2015).
[49] National Institutes of Standards and Technology, *NIST General Information.* Available at: http://www.nist.gov/public_affairs/general_information.cfm (last accessed February 26, 2015).
[50] National Institutes of Standards and Technology, *Information Technology Laboratory.* Available at: http://www.nist.gov/itl/index.cfm (last accessed February 26, 2015).
[51] National Institutes of Standards and Technology, *Information Technology Laboratory.* Available at: http://www.nist.gov/itl/index.cfm (last accessed February 26, 2015).

partnerships among government, military, academia, professional organizations, and the private industry to provide world-class leadership in standards and technology innovation to respond to these critical national needs.[52]

- National Telecommunications and Information Administration (NTIA): NTIA is an agency in the DOC that serves as the Executive Branch agency principally responsible for advising the President on telecommunications and information policies. In addition to representing the Executive Branch in both domestic and international telecommunications and information policy activities, NTIA also manages the federal use of spectrum; performs cutting-edge telecommunications research and engineering, including resolving technical telecommunications issues for the federal government and private sector; and administers infrastructure and public telecommunications facilities grants.[53]
    - Institute for Telecommunication Sciences (ITS): ITS is the research and engineering laboratory of the NTIA. ITS supports such NTIA telecommunications objectives as promotion of advanced telecommunications and information infrastructure development in the United States, enhancement of domestic competitiveness, improvement of foreign trade opportunities for U.S. telecommunications firms, and facilitation of more efficient and effective use of the radio spectrum.[54]

Standards

- Federal Information Processing Standards Publications (FIPS PUB)
    - FIPS-PUB-140-2: *Security Requirements for Cryptographic Modules*
    - FIPS-PUB-180-4: *Secure Hash Standard (SHS)*
    - FIPS-PUB-197: *Advanced Encryption Standard (AES)*

Frameworks

- Framework for Improving Critical Infrastructure Cybersecurity

Coordinated Activities

- ANSI: An MOU exists between NIST and ANSI that agrees on the need for a unified national approach to develop the best possible national and international standards.
- DHS Office of Interoperability and Compatibility (OIC): NIST OLES' Public Safety Communications Systems program provides technical expertise to the DHS OIC.

Effects on NG911

- Manages grant programs that may be used for NG911 purposes
- May affect IP networking and ESInet aspects
- Develops standards related to handling emergency data sets

Website http://www.commerce.gov/

[52] National Institutes of Standards and Technology, About the Special Programs Office. Available at: http://www.nist.gov/director/spo (last accessed February 26, 2015).
[53] National Telecommunications and Information Administration, *About NTIA Standards.* Available at: http://www.ntia.doc.gov/ (last accessed February 26, 2015).
[54] National Telecommunications and Information Administration, *Institute for Telecommunications Science Standards.* Available at: http://www.its.bldrdoc.gov/ (last accessed February 26, 2015).

Department of Homeland Security (DHS)

Name Department of Homeland Security (DHS)

Type Government Agency

Summary The DHS vision is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards. There are five core missions for DHS:

- Prevent terrorism and enhance security
- Secure and manage our borders
- Enforce and administer our immigration laws
- Safeguard and secure cyberspace
- Ensure resilience to disasters[55]

Relevant Directorates

- National Protection and Programs Directorate: The goal of the National Protection and Programs Directorate is to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.[56]
  - Office of Cybersecurity and Communications (CS&C): CS&C is responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure.[57]
    - Office of Emergency Communications (OEC): OEC supports emergency communications interoperability by offering training, tools, and workshops; by providing regional support; and by providing guidance documents and templates. These services assist OEC's stakeholders in ensuring that they have communications during steady state and emergency operations. OEC plays a key role in ensuring federal, state, local, tribal and territorial agencies have the necessary plans, resources, and training needed to support operable and advanced interoperable emergency communications.[58]
- Science & Technology (S&T) Directorate: The S&T Directorate is the primary research and development arm of DHS. The S&T Directorate's mission is to help strengthen America's security and resiliency by providing assessments, analysis and reports, and by developing innovative technology solutions for the Homeland Security Enterprise.[59]
  - Office for Interoperability and Compatibility (OIC): OIC strengthens interoperable wireless communications and improves effective information

[55] U.S. Department of Homeland Security, Our Mission. Available at: http://www.dhs.gov/our-mission (last accessedFebruary 26, 2015).
[56] U.S. Department of Homeland Security, *National Protection and Programs Directorate.* Available at: http://www.dhs.gov/xabout/structure/editorial_0794.shtm or http://www.dhs.gov/about-national-protection-and-programs-directorate (last accessed February 26, 2015).
[57] U.S. Department of Homeland Security, *Office of Cybersecurity and Communications.* Available at: http://www.dhs.gov/office-cybersecurity-and-communications (last accessed February 26, 2015).
[58] U.S. Department of Homeland Security, *Office of Emergency Communications.* Available at: http://www.dhs.gov/about-office-emergency-communications (last accessed February 26, 2015).
[59] U.S. Department of Homeland Security, *Science and Technology Directorate.* Available at: http://www.dhs.gov/science-and-technology/about-st (last accessed February 26, 2015).

sharing by developing tools—such as standards, reports, and guidelines—and technologies to enhance overall planning and coordination at all levels of government.[60]

Relevant Programs and Projects

- Wireless Public Safety Interoperable Communications Program (SAFECOM): SAFECOM is a federal program that assists federal, state, and local public safety agencies in identifying wireless interoperable communications requirements and ensures those entities can communicate and share information to effectively respond to emergency incidents.[61]
- Integrated Public Alert Warning System (IPAWS) Project: The IPAWS project supports the advancement of interoperability and state-of-the-art technologies for alerts and warnings through standards development and adoption, conformity assessment, industry capability analysis, and technology evaluation. The result of these efforts will enable local, tribal, and state practitioners to provide reliable and accurate alerts and warnings to a wider public. As a result, there will be a significant reduction in the loss of life and property from all hazards.[62]
- Interoperability Continuum: The Interoperability Continuum is designed to help the emergency response community and local, tribal, state, and federal policymakers address critical elements for success as they plan and implement interoperability solutions. These elements include governance, standard operating procedures, technology, training and exercises, and use of interoperable communications. Updated in 2008, the Continuum's technology element was divided into data and voice elements to reflect the modern path to improving interoperability via information sharing and voice communications.[63]
- Voice over Internet Protocol (VoIP): To connect radio systems, emergency responders rely on bridging systems technology components that connect radio systems. Bridging systems are increasingly using IP-based connections known as VoIP to transmit voice communications across radio systems. Although VoIP is based on standards, the technology lacks a single standard adopted by all manufacturers. CID is working with emergency responders, NIST and the ITS to define a specification for bridging devices that use VoIP.[64]

Standards

- NIEM: *National Information Exchange Model*

Coordinated Activities

- National Information Exchange Model (NIEM): The National Information Exchange Model is a partnership of the U.S. Department of Justice (DOJ) and DHS created to develop, disseminate, and support enterprise-wide information exchange standards and

[60] U.S. Department of Homeland Security, National Emergency Communications Plan, July 2008. (Washington: Secretary of Homeland Security) pg 65. Available at: http://www.safecomprogram.gov/natlemergencycommplan.html (last accessed February 26, 2015).
[61] U.S. Department of Homeland Security, *Wireless Public Safety Interoperable Communications Program (SAFECOM).* Available at: http://www.safecomprogram.gov/default.aspx (last accessed February 26, 2015).
[62] Federal Emergency Management Agency, *Integrated Public Alert and Warning System (IPAWS.)* Available at: http://www.fema.gov/integrated-public-alert-warning-system (last accessed February 26, 2015).
[63] U.S. Department of Homeland Security, *SAFECOM Interoperability Continuum.* Available at: http://www.safecomprogram.gov/oec/interoperability_continuum_brochure_2.pdf (last accessed February 26, 2015).
[64] U.S. Department of Homeland Security, *SAFECOM Public Safety Voice over Internet Protocol Working Group.* Available at: http://www.safecomprogram.gov/currentprojects/voip/Default.aspx (last accessed August 12, 2013, however, link is not active as of February 26, 2015).

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 nation.[65]

- Office of Emergency Communications (OEC): The OIC, in coordination with OEC, is developing a Standard Operating Procedures (SOP) Development Guide, a Shared Channel Guide v2.0, and a brochure on plain language.[66]

Effects on NG911

- Develops standards related to handling emergency data sets.

Website

http://www.dhs.gov/
http://www.niem.gov/

[65] National Information Exchange Model, *National Information Exchange Model.* Available at: http://www.niem.gov/ (last accessed February 26, 2015).

[66] United States Department of Homeland Security, National Emergency Communications Plan, July 2008. (Washington: Secretary of Homeland Security) pg 26. Available at: http://www.safecomprogram.gov/natlemergencycommplan.html (last accessed February 267, 2015).

Department of Justice (DOJ)

Name	Department of Justice (DOJ)
Type	Government Agency
Summary	The DOJ mission is to enforce the law and defend the interests of the United States 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. [67]
Relevant Directorates	• Office of Justice Programs (OJP): OJP's mission is to increase public safety and improve the fair administration of justice across America through innovative leadership and programs. [68]
Relevant Bureaus & Offices	• Bureau of Justice Assistance (BJA): BJA's mission is to provide leadership and services in grant administration and criminal justice policy development to support local, state, and tribal justice strategies to achieve safer communities. BJA supports programs and initiatives in the areas of law enforcement, justice information sharing, countering terrorism, managing offenders, combating drug crime and abuse, adjudication, advancing tribal justice, crime prevention, protecting vulnerable populations, and capacity building.[69]
Standards	• NIEM: *National Information Exchange Model.*
Coordinated Activities	• National Information Exchange Model (NIEM): NIEM is a partnership of DOJ and DHS created to develop, disseminate, and support 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 nation.[70]
Effects on NG911	• Develops standards related to handling emergency data sets, specifically pertaining to interoperability for data sharing.
Website	http://www.justice.gov/ http://www.niem.gov/

[67] United States Department of Justice, *About DOJ.* Available at: http://www.justice.gov/about/about.html (last accessed February 26, 2015).
[68] Office of Justice Programs, *Mission and Vision.* Available at: http://www.ojp.usdoj.gov/about/mission.htm (last accessed February 26, 2015).
[69] Office of Justice Programs, *About the Bureau of Justice Assistance.* Available at: https://www.bja.gov/About/index.html (last accessed February 26, 2015).
[70] National Information Exchange Model, *National Information Exchange Model.* Available at: http://www.niem.gov/ (last accessed February 26, 2015).

Department of Transportation (USDOT)

Name Department of Transportation (USDOT)

Type Government Agency

Summary USDOT serves the United States by ensuring a fast, safe, efficient, accessible, and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future. [71]

Relevant Administrations

- National Highway Traffic Safety Administration (NHTSA): NHTSA directs the highway safety and consumer programs established by the National Traffic and Motor Vehicle Safety Act of 1966, the Highway Safety Act of 1966, the 1972 Motor Vehicle Information and Cost Savings Act, and succeeding amendments to these laws.[72]
- Research and Innovative Technology Administration (RITA): RITA coordinates USDOT's research and education programs and is working to bring advanced technologies into the transportation system.[73]
    - Intelligent Transportation Systems (ITS): The USDOT ITS program focuses on intelligent vehicles, intelligent infrastructure, and the creation of an intelligent transportation system through integration with and between these two components. The federal ITS program supports the overall advancement of ITS through investments in major initiatives, exploratory studies, and a deployment support program. Increasingly, the federal investments are directed at targets of opportunity—major initiatives—that have the potential for significant payoff in improving safety, mobility, and productivity.[74]
    - Transportation Safety Advancement Group (TSAG): The TSAG serves an important function on behalf of the USDOT, RITA, and its ITS-Joint Program Office (ITS-JPO). Through its members and allied stakeholder groups, TSAG identifies surface transportation-based technologies and applications, and promotes a national dialogue regarding public safety practitioners' first-hand experiences, corresponding best practices, and lessons learned. [75]

Relevant Programs and Projects

- Next Generation 911 (NG911) Initiative: The nation's current 911 system is designed around telephone technology and cannot handle the text, data, images, and video that are increasingly common in personal communications and critical to future transportation safety and mobility advances. The NG911 Initiative has established

[71] United States Department of Transportation, *About DOT.* Available at: http://www.dot.gov/about.html (last accessed February 26, 2015).
[72] National Highway Traffic Safety Administration, *About NHTSA.* Available at: http://www.nhtsa.gov/About (last accessed January 6, 2015).
[73] Research and Innovation Technology Administration, *Welcome to RITA.* Available at: http://www.rita.dot.gov/ (last accessed February 26, 2015).
[74] Intelligent Transportation Systems, *ITS Overview.* Available at: http://www.its.dot.gov/factsheets/overview_factsheet.htm (last accessed February 26, 2015).
[75] Transportation Safety Advancement Group, *About TSAG.* Available at: http://www.tsag-its.org/whatistsag.php (last accessed February 26, 2015).

the foundation for public emergency communications services in a wireless mobile society.[76]

- National 911 Program: The National 911 Program, in coordinating the efforts of states, technology providers, public safety officials, 911 professionals and other groups, seeks to ensure a smooth, reliable, and cost-effective transition to a 911 system that takes advantage of new communications technologies to enhance public safety nationwide.[77]

Coordinated Activities

- European Telecommunications Standards Institute (ETSI): A memorandum of cooperation exists between USDOT/RITA/ITS and ETSI
- Federal Communications Commission, Communications Security, Reliability, and Interoperability Council (CSRIC): Seminars and coordination
- Emergency Services Workshop (ESW): Participate and monitor actions

Websites

http://www.dot.gov/
http://911.gov/

[76] Research and Innovation Technology Administration, *Next Generation 911.* Available at: http://www.its.dot.gov/ng911/index.htm (last accessed February 26, 2015).
[77] 911.gov, *About The Program.* Available at: http://www.911.gov/about.html (last accessed February 26, 2015).

Emergency Services Workshop (ESW)

Name	Emergency Services Workshop (ESW)
Type	Standards Coordination Group
Summary	The Emergency Services Workshop series is an ongoing effort in the emergency services community to coordinate global standards and technologies for emergency calling and emergency notification. The primary focus of the workshop series is to foster coordination among the many SDOs involved in emergency services, as they all work toward a global solution for emergency communications using Internet technologies.[78]
Coordinated Activities	The ESW is made up of representatives from many of the SDOs listed in this document.
Website	http://www.emergency-services-coordination.info/

[78] Emergency Services Workshop, *The Emergency Services Workshop Series.* Available at: http://www.emergency-services-coordination.info/ (last accessed February 26, 2015).

European Telecommunications Standards Institute (ETSI)

Name	European Telecommunications Standards Institute (ETSI)
Type	Regional Standards Organization
Summary	ETSI is an independent, not-for-profit organization that produces globally applicable standards for information and communication technology (ICT), including fixed, mobile, radio, converged, broadcast, and Internet technologies.[79]
Relevant Committees and Other Bodies	• EMTEL—Emergency Communications: EMTEL addresses a broad spectrum of issues related to the use of telecommunications services in emergency situations.[80] • TISPAN - Telecommunications & Internet converged Services & Protocols for Advanced Networks: ETSI TISPAN has been the key standardization body in creating the Next Generation Networking (NGN) specifications.[81]
Standards	• ETSI TS 101 470: *Emergency Communications (EMTEL); Total Conversion Access to Emergency Services* • ETSI TS 102 164: *Telecommunications and converged Services and Protocols for Advanced Networking (TISPAN); Emergency Location Protocols* • 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* • ETSI TS 123 167: *Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsytem (IMS) emergency sessions* • 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* • ETSI ES 203 178: *Functional architecture to support European requirements on emergency caller location determination and transport* • ETSI ES 282 007: *Telecommunications and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture*
Coordinated Activities	• 3GPP • U.S. Department of Transportation (USDOT): A memorandum of cooperation exists between USDOT/ RITA/ITS and ETSI

[79] European Telecommunications Standards Institute, *Introduction.* Available at: http://www.etsi.org/index.php/about/introduction (last accessed February 26, 2015).
[80] European Telecommunications Standards Institute, *EMTEL Overview.* Available at: http://www.emtel.etsi.org/overview.htm (last accessed January 7, 2015).
[81] European Telecommunications Standards Institute, *Telecoms & Internet Services & Protocols for Advanced Network. Overview.* Available at: http://www.etsi.org/tispan/ (last accessed February 26, 2015).

Effects on NG911

- Develops standards that enable text and multimedia transmission from the caller to the NG911 system (transport of data).
- Develops standards adhered to by originating service providers' (OSP) network and applications services for emergency calling.
- Supports location requirements and standards.

Website http://www.etsi.org/

Federal Communications Commission (FCC)

Name Federal Communications Commission (FCC)

Type Government Agency

Summary The FCC is an independent United States government agency charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. [82]

Relevant Bureaus

- Public Safety and Homeland Security Bureau (PSHSB): The FCC's Public Safety and Homeland Security Bureau (PSHSB) is responsible for developing, recommending, and administering the agency's policies pertaining to public safety communications issues. These policies include 911 and E911; operability and interoperability of public safety communications; communications infrastructure protection and disaster response; and network security and reliability. PSHSB also serves as a clearinghouse for public safety communications information and emergency response issues.[83]

Relevant Advisory Committees

- Communications Security, Reliability, and Interoperability Council (CSRIC) III: CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.[84] The following are CSRIC III working groups relevant to NG911:
  - Working Group 1—NG911: Responsible for recommending additional standards work needed to enable NG911 network architecture, particularly those related to the National Emergency Number Association's (NENA's) i3 standard, and related standards needed from other organizations such as IETF, 3GPP, and ATIS. The working group shall identify gaps in NG911 network architecture standards and label them.[85]
  - Working Group 3—E911 Location Accuracy: Responsible for examining E911/public safety indoor and outdoor location technologies in use today, identifying current performance and limitations for use in next generation public safety applications. More specifically, the working group is examining emerging E911/public safety location technologies and recommending options to CSRIC for improvement of E911 location accuracy, including implementation timelines.[86]
  - Working Group 8 – E911 Best Practices: Responsible for reviewing the existing

[82] FCC, *About the FCC.* Available at: http://www.fcc.gov/aboutus.html (last accessed February 26, 2015).
[83] FCC, *Public Safety and Homeland Security Bureau, About Us.* Available at: http://www.fcc.gov/help/public-safety-and-homeland-security-bureau-about-us (last accessed February 26, 2015).
[84] Public Safety and Homeland Security Bureau, *The Communications Security, Reliability and Interoperability Council*. Available at: http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council (last accessed February 26, 2015).
[85] Communications Security, Reliability, and Interoperability Council, *CSRIC III Working Group Descriptions.* Available at: http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions_2-28-12.pdf (last accessed February 26, 2015).
[86] Communications Security, Reliability, and Interoperability Council, *CSRIC III Working Group Descriptions.* Available at: http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions_2-28-12.pdf (last accessed February 26, 2015).

CSRIC/NRIC 911 best practices and recommending ways to improve them, accounting for the passage of time, technology changes, operational factors, and any identified gaps. As part of this effort, the working group will also provide recommendations regarding the creation of two new, non-industry best practice categories: (i) PSAP and (ii) 911 Consumer. The working group also will provide recommendations regarding how to better engage PSAPs in the best practice process.[87]

- Communications Security, Reliability and Interoperability Council (CSRIC) IV: CSRIC's mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communication systems, including telecommunications, media, and public safety.[88] The following are CSRIC IV working groups relevant to NG911:
    - Working Group 1 – NG911: The working group will study and report on the technical feasibility for wireless carriers to include E911 Phase 2 location accuracy and information in texts sent to 911, and make recommendations for including enhanced location information in texts to 911. In addition, the working group will recommend best practices—including testing and trialing—operational procedures, and security requirements that wireless carriers, PSAPs, and third-party service providers should follow in provisioning PSAP requests for text-to-911 service.[89]
- Emergency Response Interoperability Center (ERIC): The mission of ERIC is to establish a technical and operational framework that will ensure nationwide operability and interoperability in deployment and operation of the 700 megahertz (MHz) public safety broadband wireless network. ERIC will adopt, implement, and coordinate interoperability regulations, license requirements, grant conditions and technical standards. DHS, NIST, DOJ, and DOC contribute to ERIC's functions.[90]
- Emergency Access Advisory Committee (EAAC): The EAAC Charter expired In July 2013. EAAC was chartered to determine the most effective and efficient technologies and methods by which to enable equal access to emergency services by individuals with disabilities as part of the nation's migration to Next Generation 911 (NG9-1-1), and to make recommendations to the Commission on how to achieve those effective and efficient technologies and methods.[91]
- Network Reliability and Interoperability Council (NRIC)- NRIC was an advisory council, chartered by the FCC to engagePartner with the FCC, the communications industry and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the burgeoning telecommunications industry. There were seven assemblies of NRIC since 1992. As a note, the NRIC is no

[87] Communications Security, Reliability, and Interoperability Council, *CSRIC III Working Group Descriptions.* Available at: http://transition.fcc.gov/pshs/advisory/csric3/wg-descriptions_2-28-12.pdf (last accessed February 26, 2015).
[88] Public Safety and Homeland Security Bureau, *Communications Security, Reliability and Interoperability Council IV*. Available at: https://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv (last accessed February 26, 2015).
[89] Communications Security, Reliability, and Interoperability Council, *CSRIC IV Working Group Descriptions*. Available at: http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_12_31_13.pdf (last accessed February 26, 2015).
[90] Federal Communication Commission, Public Safety and Homeland Security Bureau, *Emergency Response Interoperability Center (ERIC).* Available at: http://www.fcc.gov/pshs/eric.html (last accessed February 26, 2015).
[91] Federal Communication Commission, Emergency Access Advisory Committee (EAAC). Available at: http://www.fcc.gov/encyclopedia/emergency-access-advisory-committee-eaac (last accessedFebruary 26, 2015).

longer active and has been superseded by the Communication Security, Reliability, and Interoperability Council (CSRIC) within the FCC. The documents from NRIC can be reachedaccessed from the CSRIC website.

Standards

- 9-9-3215: *Mobile Switching Center (MSC) Default Route Operational Standard Recommendation*
- 9-9-3216: *Default Routing*
- 9-9-3217: *E911 Service Provider Contact Information*
- 9-9-3218: *Training on Obtaining E911 Phase II Data*
- 9-9-3219: *Training on E911 Phase II ALI Display*
- 9-9-3223: *Originating Source to E911 Selective Router Trunking Architecture*
- 9-9-3225: *Mobile Positioning Center (MPC) Capacity Reserve*
- 9-9-3226: *MPC 911 Network Operations Support*
- 9-9-3227: *911 Voice traffic and Location Data Concurrency*
- 9-9-3228: *Global Positioning System (GPS) Location accuracy for E911*
- 9-9-3229: *911 Performance Statistics and Logging*
- 9-9-3231: *Satellite Location Identification information Transfer Delay*
- 9-9-3232: *Handsets that use a GPS algorithm for E911*
- 9-9-3233: *E911 Phase II Accuracy Optimization Reporting and Resolution Process*
- 9-9-0567 – Unnamed
- 9-9-0569– Unnamed
- 9-9-0574– Unnamed
- 9-9-0900– Unnamed
- 9-9-3224– Unnamed
-

Website http://www.fcc.gov/

Federal Geographic Data Committee (FGDC)

Name	Federal Geographic Data Committee (FGDC)
Type	Interagency Committee
Summary	The FGDC is an interagency committee that promotes the coordinated development, use, sharing, and dissemination of geospatial data on a national basis. This nationwide data publishing effort is known as the National Spatial Data Infrastructure (NSDI). The NSDI is a physical, organizational, and virtual network designed to enable the development and sharing of this nation's digital geographic information resources. FGDC activities are administered through the FGDC Secretariat, hosted by the U.S. Geological Survey. [92]
Relevant Agencies	• FGDC Structure and Federal Agency and Bureau Representation: In accordance with Office of Management and Budget (OMB) Circular A-16, the FGDC is chaired by the Secretary of the Interior with the Deputy Director for Management, OMB as Vice-Chair.[93]
Standards	• FGDC-STD-014.0-2008: *Geographic Information Framework Data Content Standard* • FGDC-STD-016-2011: *United States Thoroughfare, Landmark, and Postal Address Data Standard* • FGDC-STD-001-1998: *Content Standard for Digital Geospatial Metadata*
Coordinated Activities	The U.S. Office of Management and Budget and the U.S. Congress set policy for federal agencies. The FGDC, a federal interagency coordinating committee, is guided by those policies in the design of programs, activities and technologies. The FGDC sets geospatial information policy in harmony with overall information policy. The FGDC Secretariat engages in on-going strategic planning to ensure continued investment of resources in high-value programs, activities and technologies. [94]
Effects on NG911	Develops standards pertaining to interoperability for data sharing.
Website	http://www.fgdc.gov/

[92] Federal Geographic Data Committee. Available at: http://www.fgdc.gov/ (last accessedFebruary 26, 2015).
[93] Federal Geographic Data Committee Structure. Available at: http://www.fgdc.gov/participation (last accessedFebruary 26, 2015).
[94] Federal Geographic Data Committee Policy and Planning. Available at: http://www.fgdc.gov/policyandplanning (last accessedFebruary 26, 2015).

Institute of Electrical and Electronics Engineers (IEEE)

Name Institute of Electrical and Electronics Engineers (IEEE)

Type Professional Organization

Summary IEEE is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.[95]

Relevant Committees

- IEEE 802 LAN/MAN Standards Committee: The IEEE 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee develops LAN standards and MAN standards.[96]
  - IEEE 802.1 Working Group: The IEEE 802.1 Working Group is chartered to concern itself with the development of standards and recommended practices in the following areas: 802 LANs, MANs and other wide area networks; 802 security; 802 overall network management, and protocol layers above the media access control (MAC) and logical link control (LLC) layers. The 802.1 working group has four active task groups: Interworking, Security, Audio/Video Bridging and Data Center Bridging.[97]
  - IEEE 802.11 Wireless Local Area Networks Working Group: Within the IEEE 802 LAN/MAN Standards Committee, the IEEE 802.11 Working Group develops standards and recommended practices to support development and deployment of wireless local area networks (WLANs).[98]
  - IEEE 802.16 Broadband Wireless Access Working Group: Within the IEEE 802 LAN/MAN Standards Committee, the IEEE 802.16 Working Group develops standards and recommended practices to support development and deployment of broadband wireless MANs.[99]
  - IEEE 802.23 Emergency Services Working Group: Within the IEEE 802 LAN/MAN Standards Committee, the IEEE 802.23 Working Group develops standards and recommended practices to support a framework that provides consistent access and data facilitating compliance with applicable civil authority requirements for communications systems that include IEEE 802 networks.[100] It should be noted that due to a lack of participation, this working group is no longer active (disbanded June 2011).

[95] IEEE, *About IEEE.* Available at: http://www.ieee.org/about/index.html (last accessedFebruary 26, 2015).
[96] IEEE, *IEEE 802 LAN / MAN Standards Committee.* Available at: http://grouper.ieee.org/groups/802/index.shtml (last accessedFebruary 26, 2054).
[97] IEEE, *IEEE 802.1 Working Group.* Available at: http://www.ieee802.org/1/ (last accessFebruary 26, 2015).
[98] IEEE, *IEEE 802.11 Wireless Local Area Networks.* Available at: http://www.ieee802.org/11/ (last accessedFebruary 26, 2015).
[99] IEEE, *IEEE 802.16 Working Group on Broadband Wireless Access Standards.* Available at: http://www.ieee802.org/16/ (last accessed February 26, 2015).
[100] IEEE, *IEEE 802.23 Emergency Services Working Group.* Available at: http://www.ieee802.org/23/ (last accessed February 26, 2015).

Standards

- IEEE 802.1AB: *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AC: *Media Access Control (MAC) Services Definition*
- IEEE 802.11: *Wireless Local Area Networks (WLANs)*
- IEEE 802.16: *Broadband Wireless Metropolitan Area Network*
- IEEE 802.23: *Emergency Services for Internet Protocol (IP) Based Citizen to Authority Communications (Draft)*
- IEEE 1512: 2006: *Standard for Common Incident Management Message Sets for use by Emergency Management Centers*
- IEEE 1903: *Standard for the Functional Architecture of Next Generation Service Overlay Networks*
- IEEE 446-1995: *Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*

Coordinated Activities

- WiMAX Forum
- 3GPP
- IETF
- ANSI: IEEE is an ANSI-accredited SDO

Website http://www.ieee.org/

Internet Engineering Task Force (IETF)

Name Internet Engineering Task Force (IETF)

Type International Standards Organization—Industry (Networking)

Summary The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet, in such a way as to make the Internet work better. These documents include protocol standards, current best practices, and informational documents of various kinds.[101]

Relevant Working Groups

- Emergency Context Resolution with Internet Technologies (ECRIT): In a number of areas, the public switched telephone network (PSTN) has been configured to recognize an explicitly specified number as a call for emergency services. These numbers (e.g., 911, 112) relate to an emergency service context and depend on a broad, regional configuration of service contact methods and a geographically constrained context of service delivery. Successful delivery of an emergency service call within those systems requires both an association of the physical location of the originator with an appropriate emergency service center and call routing to deliver the call to the center. Calls placed using Internet technologies do not use the same systems to achieve those goals, and the common use of overlay networks and tunnels (either as virtual private networks [VPNs] or for mobility) makes meeting them more challenging. There are, however, Internet technologies available to describe location and to manage call routing. This working group will describe when these may be appropriate and how they can be used, and is considering emergency services calls that might be made by any user of the Internet.[102]
- Geographic Location/Privacy (GEOPRIV): This working group is listed as a "concluded" working group as of November 2014. The IETF has recognized that many applications are emerging that require geographic and civic location information about resources and entities, and that the representation and transmission of that information has significant privacy and security implications. It has created a suite of protocols that allows such applications to represent and transmit such location objects and to allow users to express policies on how these representations are exposed and used. The GEOPRIV working group is chartered to continue to develop and refine representations of location in Internet protocols and to analyze the authorization, integrity, and privacy requirements that must be met when these representations of location are created, stored, and used. The group will create and refine mechanisms for the transmission of these representations that address the requirements that have been identified.[103]

Standards

- IETF RFC 3261: *SIP: Session Initiation Protocol*
- IETF RFC 3856: *A Presence Event Package for the Session Initiation Protocol (SIP)*
- IETF RFC 3966: *The tel URI for Telephone Numbers*

[101] IETF, *Mission Statement.* Available at: http://www.ietf.org/about/mission.html (last accessedFebruary 26, 2015).
[102] IETF, *Emergency Context Resolution with Internet Technology (ECRIT).* Available at: http://datatracker.ietf.org/wg/ecrit/charter/ (last accessedFebruary 26, 2015).
[103] IETF, *Geographic Location / Privacy (geopriv).* Available at: http://datatracker.ietf.org/wg/geopriv/charter/ (last accessedFebruary 26, 2015).

- IETF RFC 3986: *Uniform Resource Identifiers (URI): Generic Syntax*
- IETF RFC 4079: *A Presence Architecture for the Distribution of GEOPRIV Location Objects*
- IETF RFC 4119*: A Presence-based GEOPRIV Location Object Format*
- RFC 5069: *Security Threats and Requirements for Emergency Call Marking and Mapping*
- IETF RFC 5139: *Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)*
- IETF RFC 5222: *LoST: A Location-to-Service Translation Protocol (updated by RFC 6848)*
- IETF RFC 5223: *Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Configuration Protocol (DHCP)*
- IETF RFC 5491: *GEOPRIV Presence Information Data Format (PIDF-LO) Usage Clarification, Considerations, and Recommendations*
- IETF RFC 5985: *HTTP Enabled Location Delivery (HELD)*
- IETF RFC 6155: *Use of Device Identity in HTTP-Enabled Location Delivery (HELD)*
- IETF RFC 6442: *Location Conveyance for the Session Initiation Protocol*
- RFC 6753: *A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)*
- RFC 6772: *Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information*
- RFC 6739: *Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol*
- RFC 6848: *Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)*
- RFC 6881: *Best Current Practice for Communications Services in Support of Emergency Calling*
- RFC 6915: *Flow Identity Extension for HTTP-Enabled Location Delivery (HELD)*
- RFC 7035: *Relative Location Representation*
- RFC 7090: *Public Safety Answering Point (PSAP) Callback*
- RFC 7105: *Using Device-Provided Location-Related Measurements in Location Configuration Protocols*
- RFC 7163: *URN for Country-Specific Emergency Services*
- RFC 7199: *Location Configuration Extensions for Policy Management*
- RFC 7216: *Location Information Server (LIS) Discovery Using IP Addresses and Reverse DNS*
- RFC 7378: *Trustworthy Location*
- RFC 7406: *Extensions to the Emergency Services Architecture for Dealing With Unauthenticated and Unauthorized Devices*
- IETF Internet Draft: *Additional Data related to an Emergency Call*
- IETF Internet Draft: *Data Only Emergency Calls*
- IETF Internet Draft: *A Routing Request Extension for the HELD Protocol*
- IETF Internet Draft: *A LoST extension to return complete and similar location info*
- IETF Internet Draft: *Representation of Uncertainty and Confidence in PIDF-LO*

Coordinated Activities

- ETSI EMTEL
- NENA

Effects on NG911

- Develops standards that enable text and multimedia transmission from the caller to the NG911 system (transport of data).

Website http://www.ietf.org/

International Academies of Emergency Dispatch (IAED)

Name	International Academies of Emergency Dispatch (IAED)
Type	Professional Organization
Summary	The mission of the IAED is to advance and support the public safety emergency telecommunications professional and ensure that citizens in need of emergency, health, and social services are matched safely, quickly, and effectively with the most appropriate resource.[104]
Certifications	• ETC: Emergency Telecommunicator Certification
Effect on NG911	• May drive requirements based on call-handling protocols.
Website	http://www.emergencydispatch.org/

[104] IAED, *Organization.* Available at: http://www.emergencydispatch.org/Organization (last accessed February 26, 2014).

International Organization of Standardization (ISO)

Name International Organization of Standardization (ISO)

Type International Standards Organization

Summary ISO is the world's largest developer and publisher of international standards. ISO is a network of the national standards institutes of 162 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a non-governmental organization that forms a bridge between the public and private sectors. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. On the other hand, other members have their roots uniquely in the private sector, having been set up by national partnerships of industry associations. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.[105]

[105] International Organization of Standards (ISO), *About ISO*. Available at: http://www.iso.org/iso/about.htm (last accessedFebruary 26, 2015).

Standards

- ISO/IEC 20000-1: *Information Technology—Service Management—Part 1: Service Management System Requirements*
- The ISO 27000 family is a series of standards related to information security. Below is a selection of standards that can be applied to NG911 networks and operations. Please note that other standards in the ISO 27000 family also may be applicable to NG911 networks and operations.
    - ISO/IEC 27000: *Information Security Management Systems—Overview and Vocabulary*
    - ISO/IEC 27001: *Information Security Management Systems—Requirements*
    - ISO/IEC 27002: *Code of Practice for Information Security Controls*
    - ISO/IEC 27003: *Information Security Management System Implementation Guidance*
    - ISO/IEC 27004: *Information Security Management—Measurement*
    - ISO/IEC 27005: *Information Security Risk Management*
    - ISO/IEC 27011: *Information Security Management Guidelines for Telecommunications Organizations Based on ISO/IEC 27002*
    - ISO/IEC 27031: *Guidelines for Information and Communication Technology Readiness for Business Continuity*
    - ISO/IEC 27033-1: *Network Security Part 1—Overview and Concepts*
    - ISO/IEC 27033-2: *Network Security Part 2—Guidelines for the Design and Implementation of Network Security*
    - ISO/IEC 27033-3: *Network Security Part 3—Reference Networking Scenarios-Threats, Design Techniques and Control Issues*
    - ISO/IEC 27033-4: *Network Security Part 4—Securing Communications Between Networks Using Security Gateways*
    - ISO/IEC 27033-5: *Network Security Part 5—Securing Communications Across Networks using Virtual Private Networks (VPNs)*
    - ISO/IEC 27035: *Information Security Incident Management*
    - ISO/IEC 27037: *Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence*

Website http://www.iso.org/

International Telecommunication Union (ITU)

Name International Telecommunication Union (ITU) Telecommunication Standardization Section (ITU-T)

Type International Standards Organization

Summary Through its work on standardization, ITU develops technical standards (known as Recommendations) that facilitate the use of public telecommunication services and systems for communications during emergency, disaster relief, and mitigation operations. In such circumstances, technical features need to be in place to ensure that users who must communicate at a time of disaster have the communication channels they need, with appropriate security and with the best possible quality of service.[106]

Relevant Study Groups

- Study Group 2: Study Group 2 is responsible for the numbering standard ITU-T Recommendation, E.164, which has played a key role in shaping the telecommunications networks of today. E.164 provides the structure and functionality for telephone numbers; without it, individuals would not be able to communicate internationally. In recent years, Study Group 2 has worked on E.164 Number Mapping (ENUM), an IETF protocol for entering E.164 numbers into the Internet domain name system (DNS). A less well-known, but equally important product of Study Group 2 is E.212, which describes a system to identify mobile devices as they move from network to network. International mobile subscriber identity (IMSI) is a critical part of the modern mobile telecoms system, allowing a roaming mobile terminal to be identified in another network and subsequently for querying of the home network for subscription and billing information to take place.[107]
- Study Group 11: Study Group 11 is the "signaling" group within ITU-T; it produces ITU-T Recommendations that define how telephone calls and other calls such as data calls are handled in the network. Previously, this occurred primarily in the PSTN and the Integrated Services Digital Network (ISDN). Now, as operators look to align this circuit-switch-based environment with the rapidly emerging Internet technologies, Study Group 11's work is shifting toward IP-based networks or NGNs.[108]
- Study Group 13: Study Group 13 leads ITU's work on standards for NGNs. Broadly speaking, the term NGN refers to the move from circuit-switched to packet-based networks that many operators worldwide will undertake in the next few years. It will mean reduced costs for service providers who, in turn, will be able to offer a richer variety of services.[109]

[106] ITU, *Emergency Telecoms.* Available at: http://www.itu.int/en/ITU-T/emergencytelecoms/Pages/default.aspx (last accessedFebruary 26, 2015).
[107] ITU, *Study Group 2 at a Glance.* Available at: http://www.itu.int/net/ITU-T/info/sg02.aspx (last accessedFebruary 26, 2015).
[108] ITU, *Study Group 11 at a Glance.* Available at: http://www.itu.int/net/ITU-T/info/sg11.aspx (last accessedFebruary 26, 2015).
[109] ITU, *Study Group 13 at a Glance.* Available at: http:/www.itu.int/net/ITU-T/info/sg13.aspx (last accessedFebruary 26, 2015).

Coordinated Activities

- IETF: In recent years, Study Group 2 has worked on ENUM, an IETF protocol for entering E.164 numbers into the Internet DNS.[110]

Standards

- ITU-T Y.1271: *Framework(s) on Network Requirements and Capabilities to Support Emergency Telecommunications over Evolving Circuit-Switched and Packet-Switched Networks*
- ITU-T Y.2705: *Minimum Security Requirements for the Interconnection of Emergency Telecommunications Service (ETS)*

Website http://www.itu.int/

[110] ITU, *ENUM.* Available at: http://www.itu.int/osg/spu/enum/ (last accessedFebruary 26, 2015).

National Emergency Number Association (NENA)

Name National Emergency Number Association (NENA)

Type National Standards Organization (ANSI Accredited)

Summary NENA serves its members and the greater public safety community as the only professional organization solely focused on 911 policy, technology, operations, and education issues. With more than 7,000 members in 48 chapters across the United States and around the globe, NENA promotes implementation and awareness of 911, as well as international three-digit emergency communications systems. NENA is an ANSI-accredited standards developer.

NENA works with 911 professionals nationwide, public policy leaders, emergency services and telecommunications industry partners, like-minded public safety associations, and other stakeholder groups to develop and carry out critical programs and initiatives; to facilitate the creation of an IP-based NG911 system; and to establish industry-leading standards, training, and certifications. Through the association's efforts to provide effective and efficient public safety solutions, NENA strives to protect human life, preserve property, and maintain the security of our communities.

NENA began work on what is now termed NG911 in 2000 with discussion and then production of the NENA Future Path Plan for a technologically updated and more feature-rich replacement for Enhanced 911 (E911). In 2003, NENA established a committee to develop the technical nature and architecture of NG911, recognizing that this would also require various other work efforts over time to define databases management, system operations and administration, and PSAP operations requirements and standards, as well as transition plans. The NENA NG911 Project was formed to tie all aspects together and is currently made up of the organizational components listed below.

Relevant Committees The NENA NG911 Project encompasses and coordinates many actions aimed to accomplish the capabilities for IP-based NG911:

- Technical development
- PSAP operations development
- NG911 system operations development
- Policy change needs and methods development (NG Partner Program [NGPP])
- Transition plan development
- Education Steering Committee
- Interoperability testing (Industry Collaboration Events [ICE]).

There are also plans to conduct a distributed Pilot Testing process to result in national testing recommendations.

Standards **Data and Network Standards:**

- NENA 02-010 v9: *Standard Data Formats For ALI Related Data Exchange, MSAG & GIS*
- NENA 02-014: *GIS Data Collection and Maintenance Standards*
- NENA TBD*: GIS Data Model for NG9-1-1*
- NENA 02-015: *Technical Standard for Reporting and Resolving ANI/ALI Discrepancies and No Records Found for Wireline, Wireless and VoIP Technologies*
- NENA 03-509: *Femtocell and Universal Mobile Access (UMA) Information Document*

- NENA 06-750: *Model Legislation, Enhanced 911 for Multi-Line Telephone Systems*
- NENA 08-001: *Interim VoIP Architecture for E911 Services (i2)*
- NENA 08-503: *VoIP Characteristics*
- NENA 08-505: *Recommended Method(s) for Location Determination to Support IP-Based Emergency Services*
- NENA 08-752: *Location Information to Support IP-Based Emergency Services*
- NENA 71-001: *NENA Standard for NG911 Additional Data*
- NENA 71-501*: Synchronizing GIS System Databases with MSAG & ALI*
- NENA-STA-004.1-2014: *Next Generation 911 (NG911) Civic Location Data Exchange Format (CLDXF)*
- NENA-INF-009.1-2014: *Requirements for a National Forest Guide*
- NENA/APCO-INF-005*: Emergency Incident Data Document (EIDD) Information*
- NENA 70-DRAFT: *Standards for the Provisioning and Maintenance of GIS data to ECRF/LVF*
- NENA TBD: *NG911 Data/Database Management*
- NENA TBD: *Location Information Service (LIS) Standard*

Policy Routing Standards:

- NENA 71-502: *Overview of Policy Rules for Call Routing and Handling in NG911*
- NENA *STA-003: NG911 Policy Routing Rules*
- NENA-INF-011.1-2014*: NG9-1-1 Policy Routing Rules Operations Guide*

Security Standards:

- NENA 75-001: *NENA Security for Next-Generation 911 Standard (NG-SEC)*
- NENA 75-502: *NG-SEC Audit Checklist*

NG911 Architecture Standards:

- NENA 07-503: *Network Interfaces for 911 and Emergency Technologies*
- NENA 08-002: *NENA Functional and Interface Standards for Next Generation 911*
- NENA 08-003: *Detailed Functional and Interface Specification for the NENA i3 Solution*
- NENA 08-501: *Network Interface to IP Capable PSAP*
- NENA 08-506: *Emergency Services IP Network Design for NG911*
- NENA 08-751: *NENA i3 Requirements (Long Term Definition)*
- NENA 53-507: *Virtual PSAP Management*
- NENA 73-501: *Use Cases & Suggested Requirements for Non-Voice-Centric (NVC) Emergency Services*
- NENA-INF-003.1-2013: *Potential Points of Demarcation in NG911 Networks*

PSAP Operations, Training and Public Education Standards:

- NENA 54-750: *Human Machine Interface & PSAP Display Requirements*
- NENA 57-750: *NG911 System & PSAP Operational Features & Capabilities*
- NENA-INF-007.1-2013*: Handling Text-to-9-1-1 in the PSAP*
- NENA TBD: *NG911 Operations Management for 911 Authorities*
- NENA/APCO TBD*: NG-PSAP Requirements*
- NENA REF Not Numbered*: SMS Text-to 9-1-1 Resources*
- NENA REF Not Numbered*: NG9-1-1 Public Education Plan for Elected Officials and Decision Makers*

(Management of) NG911 System Operations:

- NENA TBD: *ESInet Management*
- NENA-STA-008.2-2014*: NENA Registry System*
- NENA TBD: *NG911 System Management*
- NENA TBD: *NG911 Systems Operations*

Transition Standards:

- NENA-INF-006: *NG911 Planning Guidelines*

- NENA-INF-007: *Handling Text Message Calls to 911*
- NENA-INF-008.2-2014: *NG911 Transition Plan Considerations*
- *NENA-INF-006.1-2014: NG9-1-1 Planning Guidelines*
- NENA Not Numbered: *Next Generation 911 Transition Policy Implementation Handbook: A Guide for Identifying and Implementing Policies to Enable NG911*

Reference Standards:

- NENA-ADM-000.18-2014: *Master Glossary of 911 Terminology*

Coordinated Activities

- USDOT NG911 Initiative
- Integrated Justice Information Systems (IJIS)
- NGPP coordinates with various industry vendors and public safety groups.
- NG911 ICE coordinates with industry vendors on interoperability and standards compliance
- ATIS ESIF regarding emergency services interconnection issues
- N11 consortium for coordinating interactions between NG911 and N11 services
- Coalition of Geospatial Organizations (COGO)
- Urban and Regional Information Systems Association (URISA)
- National Center for Missing and Exploited Children (NCMEC)
- FCC CSRIC
- Implementation and Coordination Office (ICO) 911 Resource Center

Effects on NG911

- Defines ESInet (transport and connectivity) requirements and characteristics, beyond generic IP networking standards
- Defines NG911 IP Functions and Interfaces standards for NG911 core architecture
- Defines NG911 databases used to control call-routing processes
- Supports location requirements and standards
- Defines NG911 interface options for originating service provider entry to the system
- Defines emergency entity functionality in coordination with NG911 system functions
- Defines PSAP functional entity downstream interfaces
- Defines mechanisms for acquisition of additional data from beyond the NG911 system
- Addresses PSAP operations

Website

http://www.nena.org/
http://www.nena.org/?page=Standards

National Fire Protection Association (NFPA)

Name	National Fire Protection Association (NFPA)
Type	National Standards Organization (ANSI Accredited)
Summary	NFPA is the world's leading advocate of fire prevention and an authoritative source on public safety. It develops, publishes, and disseminates more than 300 consensus codes and standards intended to minimize the possibility and effects of fire and other risks.[111]
Standards	• NFPA 72: *National Fire Alarm Code (Mass Notification Requirements)* • NFPA 1061: *Professional Qualifications for Public Safety Telecommunications Personnel* • NFPA 1201: *Standard for Providing Fire and Emergency Services to the Public* • NFPA 1221: *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems* • NFPA 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs (2010 Edition)*
Coordinated Activities	• ANSI: NFPA is an ANSI-accredited SDO[112]
Website	http://www.nfpa.org/

[111] NFPA, *About NFPA.* Available at: http://www.nfpa.org/about-nfpa (last accessed February 26, 2015).
[112] NFPA, *Overview.* Available at: http://www.nfpa.org/about-nfpa/nfpa-overview (last accessed February 26, 2015).

North American Electric Reliability Corporation (NERC)

Name North American Electric Reliability Corporation (NERC)

Type Professional Organization

Summary The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. 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. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people.[113]

NERC has eight standards that are subject to enforcement by NERC. There are additionally 11 standards subject to future enforcement and 11 pending regulatory filings.[114]

Relevant Committees

- Standards Committee (SC)
- Critical Infrastructure Protection Committee (CIPC)

Standards

- CIP-002-3: *Cyber Security—Critical Cyber Asset Identification*
- CIP-003-3: *Cyber Security—Security Management Controls*
- CIP-004-3a: *Cyber Security—Personnel & Training*
- CIP-005-3a: *Cyber Security—Electronic Security Perimeter(s)*
- CIP-006-3c: *Cyber Security—Physical Security of Critical Cyber Assets*
- CIP-007-3a: *Cyber Security—Systems Security Management*
- CIP-008-3: *Cyber Security—Incident Reporting and Response Planning*
- CIP-009-3: *Cyber Security—Recovery Plans for Critical Cyber Assets*

Effect on NG911

- These standards apply to the electrical critical infrastructure and will not have direct impact on NG911. This level of cyber security for critical infrastructure is in line with what is needed for NG911.

Website http://www.nerc.com/

[113] North American Electric Reliability Corporation website. At http://www.nerc.com/Pages/default.aspx Last viewed February 26, 2015).
[114] North American Electric Reliability Corporation website. At http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx (Last viewedFebruary 26, 2015).

Organization for the Advancement of Structured Information Standards (OASIS)

Name	Organization for the Advancement of Structured Information Standards (OASIS)
Type	Standards Setting Organization (Community)
Summary	OASIS is a not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society.[115]
Relevant Committees	• OASIS Emergency Management Technical Committee (EM-TC): The mission of the EM-TC is to create incident- and emergency-related standards for data interoperability. The EM-TC welcomes participation from members of the emergency management community, developers and implementers, and members of the public concerned with disaster management and response.[116]
Standards	• OASIS CAP: *Common Alerting Protocol (CAP)* • OASIS EDXL-DE: *Emergency Data Exchange Language Distribution Element (EDXL-DE)* • OASIS EDXL-RM: *EDXL Resource Messaging (EDXL-RM)* • OASIS EDXL-TEC*: EDXL—Tracking of Emergency Clients (EDXL-TEC)* • OASIS EDXL-HAVE*: EDXL Hospital Availability Exchange* • OASIS EDXL-SitRep 1.0*: EDXL Situation Reporting*
Effect on NG911	• Develops standards related to handling emergency data sets
Website	http://www.oasis-open.org/

[115] OASIS, *About OASIS.* Available at: http://www.oasis-open.org/org (last accessed February 26, 2015).
[116] OASIS, *OASIS Emergency Management TC.* Available at: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency (last accessed February 26, 2015).

Open Geospatial Consortium (OGC)

Name	Open Geospatial Consortium (OGC)
Type	Standards Setting Organization (Community)
Summary	The OGC is an international industry consortium of 507 companies, government agencies, and universities participating in a consensus process to develop publicly available interface standards. OGC® Standards support interoperable solutions that "geo-enable" the Web, wireless and location-based services, and mainstream IT. The standards empower technology developers to make complex spatial information and services accessible and useful with all kinds of applications.[117]
Mission	To advance the development and use of international standards and supporting services that promote geospatial interoperability. To accomplish this mission, OGC serves as the global forum for the collaboration of geospatial data/solution providers and users.
Standards	• OGC 06-042: *OpenGIS Web Map Service (WMS) Implementation* • OGC 06-121r9*: OGC Web Services Common Standard* • OGC 07-006r1: *OpenGIS Catalogue Service Implementation* • OGC 07-074: *OpenGIS Location Service (OpenLS) Implementation Core Services.* • OGC 08-007r1: *OpenGIS City Geography Markup Language (CityGML) Encoding Standard* • OGC 07-147r2: *OGC KML (formally Keyhole Markup Language)* • OGC 09-025r1: *OpenGIS Web Feature Service Interface Standard* • OGC 09-083r3: *GeoAPI 3.0 Implementation Standard* • OGC 10-129r: *Geography Markup Language (GML)* • OGC 11030R1: *OGC Open GeoSMS Standard-Core* • OGC 12-019: *OGC City Geography Markup Language (CityGML) Encoding Standard*
Alliance Partners/ Coordinated Activities[118]	• IEEE • IETF GeoPRIV Working Group • ISO • OASIS • OMA
Effect on NG911	• Supports geospatial data standards for data sharing, implementation and interoperability
Website	http://www.opengeospatial.org/

[117] OGC, *OGC Vision, Mission, & Goals.* Available at: http://www.opengeospatial.org/ogc/vision (last accessed February 26, 2015).

[118] OGC, *OGC Alliance Partners.* Available at: http://www.opengeospatial.org/ogc/alliancepartners (last accessed February 26, 2015).

Open Mobile Alliance (OMA)

Name Open Mobile Alliance (OMA)

Type International Standards Organization

Summary OMA is the focal point for the development of mobile service enabler specifications, which support the creation of interoperable end-to-end mobile services. OMA drives service enabler architectures and open enabler interfaces that are independent of the underlying wireless networks and platforms. OMA creates interoperable mobile data service enablers that work across devices, service providers, operators, networks, and geographies. Toward that end, OMA will develop test specifications, encourage third-party tool development, and conduct test activities that allow vendors to test their implementations.[119]

Goals

- Deliver high quality, open technical specifications based upon market requirements that drive modularity, extensibility, and consistency amongst enablers to reduce industry implementation efforts.
- Ensure OMA service enabler specifications provide interoperability across different devices, geographies, service providers, operators, and networks; facilitate interoperability of the resulting product implementations.
- Be the catalyst for the consolidation of standards activity within the mobile data service industry; work in conjunction with other existing standards organizations and industry fora to improve interoperability and decrease operational costs for all involved.
- Provide value and benefits to members in OMA from all parts of the value chain including content and service providers, information technology providers, mobile operators and wireless vendors, such that they elect to actively participate in the organization.[120]

Relevant Working Groups

- Location Working Group: The OMA Location Working Group develops specifications to ensure interoperability of location services on an end-to-end basis, as well as to provide technical expertise and consultancy on location services for other groups within OMA.[121]
- Device Management Working Group: The goal of the Device Management Working Group is to specify protocols and mechanisms that achieve management of mobile devices, including the necessary configuration to access services and management of the software on mobile devices.[122]

[119] OMA, *About OMA.* Available at: http://www.openmobilealliance.org/AboutOMA/Default.aspx (last accessed:March 2, 2015).
[120] OMA, *Collaborating with OMA.* Available at: http://openmobilealliance.org/about-oma/collaborating-with-oma/ (last accessedMarch 2, 2015).
[121] OMA, *Location Working Group.* Available at: http://www.openmobilealliance.org/Technical/LOC.aspx (last accessedMarch 2, 2015).
[122] OMA, *Device Management Working Group.* Available at: http://openmobilealliance.org/Technical/DM.aspx (last accessedMarch 2, 2015).

Standards	• OMA-ERELD-SUPL-V3_O-20110308-D: *Enabler Release Definition for Secure User Plan Location (SUPL)* • OMA-ERELD-LPPe-V1_0-20101012-C: *Enabler Release Definition for LPP Extensions (LPPe)* • OMA-TS-MLP-V3_3-20080627-C: *Mobile Location Protocol (MLP) 3.3* • OMA-ERELD-LOCSIP-V1_0-20100803-C: *Enabler Release Definition for Location in SIP/IP core*
Coordinated Activities[123]	• 3GPP: Based on the OMA-3GPP Standardization Collaboration, OMA and 3GPP work to update on a regular basis the list of dependencies between each organization's specifications and work in progress[124] • 3GPP2: Based on the OMA-3GPP2 Standardization Collaboration, OMA and 3GPP2 work to update on a regular basis the list of dependencies between each organization's specifications and work in progress [125] • IETF: Based on the OMA-IETF Standardization Collaboration, OMA and IETF work to update on a regular basis the list of dependencies between each organization's specifications and work in progress[126]
Effect on NG911	• Develops standards that enable text and multimedia transmission from the caller to the NG911 system (transport of data) • Supports location requirements and/or specifies standards
Website	http://www.openmobilealliance.org/

[123] OMA, *Collaborating with OMA.* Available at: http://openmobilealliance.org/about-oma/collaborating-with-oma/ (last accessedMarch 2, 2015).
[124] OMA, *3GPP Dependencies.* Available at: http://technical.openmobilealliance.org/Technical/3GPP.aspx (last accessedMarch 2, 2015).
[125] OMA, *3GPP2 Dependencies.* Available at: http://technical.openmobilealliance.org/Technical/3GPP2.aspx (last accessedMarch 2, 2015).
[126] OMA, *IETF Dependencies.* Available at: http://technical.openmobilealliance.org/Technical/IETF.aspx (last accessedMarch 2, 2015).

Society of Cable Telecommunications Engineers (SCTE)

Name	Society of Cable Telecommunications Engineers (SCTE)
Type	Standards Setting Organization—Industry (Cable Telecommunications)
Summary	SCTE is a non-profit professional association that provides technical leadership for the telecommunications industry and serves its members through professional development, standards, certification, and information.[127]
Mission	Providing technical leadership for the telecommunications industry and serving its members through excellence in professional development, standards, certification, and information.
Coordinated Activities	• ANSI: The SCTE Standards Program provides an ANSI-accredited forum for development of technical specifications supporting the cable telecommunications industry.[128]
Standards	• ANSI/SCTE 24-1 2009 IPCablecom 1.0 Part 1: *Architectural Framework for the Delivery of Time Critical Services Over Cable Television Networks Using Cable Modems* • ANSI/SCTE 24-2 2009 IPCablecom 1.0 Part 2: *Audio Code Requirements for the Provision of Bi-directional Audio Service Over Cable Television Networks Using Cable Modems* • ANSI/SCTE 24-3 IPCablecom Part 3: *Network Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems* • ANSI/SCTE 24-4: *Dynamic Quality of Service for the Provision of Real-time Services over Cable Television Networks using Cable Modems* • ANSI/SCTE 24-21 2012 BV16: *Speech Codec Specification for Voice over IP Applications in Cable Telephony* • ANSI/SCTE 24-22 2013 iLBCv2.0: *Speech Codec Specification for Voice over IP Applications in Cable Telephony* • ANSI/SCTE 24-23 2012 BV32: *Speech Codec Specification for Voice over IP Applications in Cable Telephony* • ANSI/SCTE 165-12 2009 IPCablecom: *PSTN Gateway Call Signaling Protocol*
Website	http://www.scte.org/

[127] Society of Cable Telecommunications Engineers, *About SCTE.* Available at: http://www.scte.org/about_us/default.aspx (last accessedMarch 2, 2015).
[128] Society of Cable Telecommunications Engineers, *About SCTE.* Available at: http://www.scte.org/about_us/default.aspx (last accessedMarch 2, 2015).

Telecommunications Industry Association (TIA)

Name Telecommunications Industry Association (TIA)

Type National Standards Organization—Industry (Telecommunications)

Summary TIA is a trade association representing the global information and communications technology industries through standards development and other activities for companies involved in telecommunications, broadband, mobile wireless, information technology, networks, cable, satellite, unified communications, emergency communications, and the greening of technology. Within the association, each area is represented by engineering committees and subcommittees that formulate standards to serve the industry and users.[129]

Relevant Engineering Committees

- TR-8 Mobile and Personal Private Radio Standards: Engineering Committee TR-8 formulates and maintains standards for private radio communications systems and equipment for both voice and data applications. TR-8 addresses all technical matters for systems and services, including definitions, interoperability, compatibility, and compliance requirements. The types of systems addressed by these standards include business and industrial dispatch applications, as well as public safety (such as police, ambulance and firefighting) applications.[130]
- TR-45 Mobile and Personal Communications Systems Standards: Engineering Committee TR-45 develops performance, compatibility, interoperability, and service standards for mobile and personal communications systems. These standards pertain to, but are not restricted to, service information, wireless terminal equipment, wireless base station equipment, wireless switching office equipment, ancillary apparatus, auxiliary applications, inter-network and intersystem operations, interfaces, and wireless packet data technologies.[131]
- TR-48 Vehicular Telematics: Engineering Committee TR-48 is responsible for development and maintenance of standards relating to vehicular telematics equipment and services. TR-48 works with other TIA committees, national and international standards organizations, and other relevant entities to ensure work items are necessary and not duplicative.[132]
- TR-50 Smart Device Communications Standards: This committee is responsible for the development and maintenance of access agnostic interface standards for the monitoring and bi-directional communication of events and information between machine-to-machine (M2M) systems and smart devices, applications or networks. These standards development efforts pertain to, but are not limited to, the functional areas as noted: Reference Architecture, Informational Models and Standard Objects, Protocol Aspects, Software Aspects, Conformance and Testing, and Security.[133]

[129] TIA, *About TIA.* Available at: http://www.tiaonline.org/about/ (last accessed January 8, 2014).
[130] TIA, *TR-8 Mobile and Personal Private Radio Standards.* Available at: http://www.tiaonline.org/all-standards/committees/tr-8 (last accessedMarch 2, 2015).
[131] TIA, *TR-45 Mobile and Personal Communications Systems Standards.* Available at: http://www.tiaonline.org/all-standards/committees/tr-45 (last accessed March 2, 2015).
[132] TIA, *TR-48 Vehicular Telematics.* Available at: http://www.tiaonline.org/all-standards/committees/tr-48 (last accessed March 2, 2015).

Standards

- TIA-1057: *Telecommunications IP Telephony Infrastructure Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)*
- TIA-TSB-146: *Telecommunications—IP Telephony Infrastructures—IP Telephony Support for Emergency Calling Service*
- TIA/EIA/IS-834: *G3G CDMA-DS to ANSI/TIA/EIA-41*
- TIA-102: *Project 25—Data Overview*
- TIA-102.BAED: Project 25 – *Packet Data Logical Link Control Procedures Standard*
- J-STD-110: *Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification*
- J-STD-110.01: *Joint ATIS/TIA Implementation Guide for J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification*
- J-STF-110.a: *Joint ATIS/TIA Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification*

Strategic Initiatives

The initiatives listed below are of high interest to the telecommunications community and are areas in which TIA has developed standards or closely monitors for future standards development needs:

- Project 25
- CALEA
- 3GPP2
- ITU [134]

Coordinated Activities[135]

- 3GPP
- 3GPP2
- APCO International
- ATIS
- ETSI
- ITU
- ANSI: TIA is an ANSI-accredited SDO[136]

Effect on NG911

- Develops standards adhered to by originating service providers' (OSP) network and applications services for emergency calling.

Website

http://www.tiaonline.org/

[133]TIA, TR-50 Smart Device Communications Standards Available at: https://global.ihs.com/landing_page_tia.cfm?&rid=TIA&seg_code=TR-50&org_code=TIA (last accessed March 2, 2015)
[134] TIA, *Strategic Initiatives.* Available at: http://www.tiaonline.org/standards/strategic-initiatives (last accessed January 11, 2015).
[135]OMA, *Collaborating with OMA,* Available at: http://openmobilealliance.org/about-oma/collaborating-with-oma/ (last accessed March 2, 2015).
[136] TIA, *TIA Homepage.* Available at: http://www.tiaonline.org/ (last accessed March 2, 2015).

Wi-Fi Alliance

Name	Wi-Fi Alliance
Type	Standards Organization
Summary	The Wi-Fi Alliance is a global non-profit organization with the goal of driving adoption of a single worldwide standard for high-speed wireless local area networking.
Mission	The Wi-Fi Alliance mission is to: • Foster highly effective collaboration among stakeholders • Deliver excellent connectivity experiences through interoperability • Embrace technology innovation • Promote the adoption of our technologies worldwide • Advocate for fair worldwide spectrum rules • Lead, develop and embrace industry-agreed standards[137]
Related Activities	• ITU
Website	http://www.wi-fi.org/

[137] Wi-Fi Alliance, *Organization.* Available at: http://www.wi-fi.org/who-we-are (last accessed March 2, 2015).

WiMAX Forum

Name	WiMAX Forum
Type	Industry Organization (WiMAX)
Summary	The WiMAX Forum is an industry-led, not-for-profit organization formed to certify and promote the compatibility and interoperability of broadband wireless products based upon the harmonized IEEE 802.16/ETSI HiperMAN standard.[138]
Mission	The WiMAX Forum is the worldwide consortium focused on global adoption of WiMAX and chartered to establish certification processes that achieve interoperability, publish technical specifications based on recognized standards, promote the technology, and pursue a favorable regulatory environment.
Related Activities	• ITU
Website	http://www.wimaxforum.org/

[138] WiMAX Forum, *About the WiMAX Forum.* Available at: http://www.wimaxforum.org/about (last accessed March 2, 2015).

Moving Forward

It is important for NG911 stakeholders to be mindful of how the un-standardized, 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 national activities (e.g., state oversight, state/regional compliant designs, and federal coordination working groups) should be considered to ensure that a complete set of NG911 open standards are accepted and adopted by all relevant stakeholders. This should include active participation by the stakeholders. Additionally, increased national collaboration could be utilized to monitor progress on the following options to address standards and technology barriers and issues identified in the *National Plan for Migration to IP-enabled Systems*:

- Strive for IP-enabled 911 open standards and understand future technology trends to encourage system interoperability and emergency data sharing
- Establish routing and prioritization 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 911 system of systems
- Develop a certification and authentication process to ensure service providers and 911 authorities meet security and system access requirements[139]

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 carriers to the 911 system—are unlikely to be fully realized.

A significant number and variety of standards potentially will have a key 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 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.

[139] National 911 Program, *National Plan for Migration to IP-enabled Systems.* Available at: http://911.gov/911-issues/standards.html (last accessed March 2, 2015).

Acronym List

ACRONYM	DESCRIPTION
3G	Third Generation
3GPP	3rd Generation Partnership Project
AACN	Advanced Automatic Collision Notification
AES	Advanced Encryption Standard
ANS	American National Standard
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communication Officials
ARIB	Association of Radio Industries and Businesses
ASD	ANSI-accredited Standards Developer
ATIS	Alliance for Telecommunications Industry Solutions
BBF	Broadband Forum
BNG	Broadband Network Gateway
CAD	Computer Aided Dispatch
CALEA	Commission on Accreditation for Law Enforcement Agencies
CAP	Common Alerting Protocol
CESE	Conforming Emergency Services Entity
CDMA	Code Division Multiple Access
CCSA	China Communications Standards Association
CID	Command, Control, and Interoperability Division
CMSP	Commercial Mobile Service Providers
COGO	Coalition of Geospatial Organizations
CS&C	DHS Office of Cybersecurity and Communications

ACRONYM	DESCRIPTION
CSRIC	FCC Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security
DNS	Domain Name System
DOC	Department of Commerce
DSL	Digital Subscriber Line
E-CSCF	Emergency Call Session Control Function
EAS	Emergency Alert System
ECES	Entities Consuming Emergency Services
ECRIT	Emergency Context Resolution with Internet Technologies
EDGE	Enhanced Data rates for GSM Evolution
EDXL	Emergency Data Exchange Language
EDXL-DE	EDXL-Distribution Element
EDXL-RM	EDXL-Resource Messages
EEEL	Electronics and Electrical Engineering Laboratory
EGEA	Expert Group on Emergency Access (see EU)
eHRPD	Evolved High Rate Packet Data
EIC	Emergency Interoperability Consortium
EIDD	Emergency Information Data Document
EIS	Emergency Information Service
EISI	Emergency Information Services Interface
EMTEL	Emergency Telecommunications

ACRONYM	DESCRIPTION
EPES	Entities Providing Emergency Services
ERIC	Emergency Response Interoperability Center
ESIF	Emergency Services Interconnection Forum
ESINet	Emergency Services IP Network
ESMI	Emergency Services Messaging Interface
ESW	Emergency Services Coordination Workshop
ETC	Emergency Telecommunicator Certification
ETSI	European Telecommunications Standards Institute
EU	European Union
FDD	Frequency Division Duplex
FIPS PUB	Federal Information Processing Standard Publication
GEOPRIV	Geographic Location/Privacy
GIS	Geographic Information System
GML	Geography Markup Language
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HAVE	Hospital Availability Exchange
HELD	HTTP Enabled Location Delivery
HRPD	High Rate Packet Data (3GPP2 access technology)
HSGW	High Rate Packet Data Serving Gateway
HSPA+	Evolved High Speed Packet Access
HSSP	Homeland Security Standards Panel
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure

ACRONYM	DESCRIPTION
I-WLAN	Intelligent Wireless Local Area Networking
IACP	International Association of Chiefs of Police
ICO	Implementation and Coordination Office
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IJIS	Integrated Justice Information Systems
IM	IP Multimedia
IMT-2000	International Mobile Telecommunications-2000
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	Internet Protocol Connectivity Access Network
IPAWS	Integrated Public Alert Warning System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
ITS	Intelligent Transportation Systems
ITU	International Telecommunication Union
ITU-R	ITU—Radio Communications Sector

ACRONYM	DESCRIPTION
ITU-T	ITU—Standardization Sector
L7 LCP	Layer 7 Location Control Protocol
LAN	Local Area Network
LCP	Location Configuration Protocol
LEITSC	Law Enforcement Information Technology Standards Council
LIS	Location Information Server
LLDP-MED	Link Layer Discovery Protocol-Media Endpoint Discover
LoST	Location-to-Service Translation (protocol)
LRF	Location Retrieval Function
LTE	Long-Term Evolution
MAN	Metropolitan Area Network
MHz	Megahertz
MIH	Media Independent Handover
MLS	Mobile Location Services (see OMA)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPC	Mobile Positioning Center
MSC	Mobile Switching Center
NAED	National Academies of Emergency Dispatch
NENA	National Emergency Number Association
NG911	Next Generation 911
NGES	Next Generation Emergency Services Subcommittee
NGN	Next Generation Networking
NHTSA	National Highway Traffic Safety Administration
NG-SEC	Security for Next Generation 911 Standard
NGPP	Next Generation Partner Program
NIEM	National Information Exchange Model

ACRONYM	DESCRIPTION
NIST	National Institute of Standards and Technology
NOBLE	National Organization of Black Law Enforcement Executives
NPSBN	Nationwide Public Safety Broadband Network
NSA	National Sheriffs' Association
NTIA	National Telecommunications and Information Administration
OASIS	Organization for the Advancement of Structured Information Standards
OEC	Office of Emergency Communications
OIC	Office of Interoperability and Compatibility
OJP	Office of Justice Programs
OLES	Office of Law Enforcement Standards
OMA	Open Mobile Alliance
OSP	Originating Service Provider
PERF	Police Executive Research Forum
PIDF-LO	Presence Information Data Format-Location Object
PS SoR	Public Safety Statement of Requirements
PSAP	Public Safety Answering Point
PSHSB	Public Safety and Homeland Security Bureau
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
QoS	Quality of Service
RFAI	Request for Assistance Interface
RG	Residential Gateway
RITA	Research and Innovative Technology Administration
RM	Reference Material
RSVP	Resource ReSerVation Protocol

ACRONYM	DESCRIPTION
S&T	Science & Technology Directorate
SAFECOM	Wireless Public Safety Interoperable Communications Program
SDO	Standards Development Organization
SDP	Session Description Protocol
SHS	Secure Hash Standard
SITREP	Situation Report
SIP	Session Initiated Protocol
SMS	Short Message Service
SOP	Standard Operating Procedure
SR	Selective Router
SRDB	Selective Routing Database
SRIC	Standards Review and Interpretation Committee
SRM	Standard Reference Materials
SSO	Standards Setting Organization
SUPL	Secure User Plane for Location (see OMA)
SWG	Software Working Group
TCC	Text Control Center
TDD	Time Division Duplex
TISPAN	Telecommunications & Internet converged Services & Protocols for Advanced Networks
TS	Technical Specifications
TSG CT	Technical Specification Group Core Network and Terminals
TSG-X	Technical Specification Group Networks
TSP	Telematics Service Provider
TTA	Telecommunications Technology Association
TTC	Telecommunications Technology Committee
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

ACRONYM	DESCRIPTION
USDOT	Department of Transportation
UTMS	Universal Mobile Telecommunications System
UTRA	UTMS Terrestrial Radio Access
VEDS	Vehicular Emergency Data Set
VoDSL	Voice over Digital Subscriber Line
VOP	Voice over Packet
VoIP	Voice over Internet Protocol
WAVE	Wireless Access for the Vehicular Environment (802.11p)
WG	Working Group
WLAN	Wireless Local Area Network
WTSC	Wireless Technologies and Systems Committee
xDSL	Example Digital Subscriber Line (see DSL)
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

Appendix A: Standards and Best Practices

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
3GPP	3GPP TS 23.167 (Free)	3GPP; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) emergency sessions	Defines the service description (Stage 2) for emergency services in the IMS, including the elements necessary to support SIP Multimedia emergency services.	ETSI TS 123 167	Version 12.0.0 September 22, 2014	Technical Standard (Product/ Design)		X	X		
	3GPP TS 23.228 (Free)	IP Multimedia Subsystem (IMS); Stage 2	Defines the Stage 2 service description for the IMS, which includes the elements necessary to support IP Multimedia (IM) services.		Version 13.1.0 December 17, 2014	Technical Standard		X	X		
	3GPP TS 23.517 (Free)	3GPP; 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.	ETSI ES 282 007	Version 8.0.0 December 2007	Technical Standard (Interface/ Design)		X	X		
	3GPP TS 24.229 (Free)	IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3	Defines a call control protocol for use in the IM Core Network (CN) subsystem based on the SIP, and the associated SDP.		Version 13.0.0 December 21, 2014	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
3GPP	3GPP TS 29.010 (Free)	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 a detailed specification 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 and to provide a detailed specification 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 12.0.0 September 30, 2014	Technical Standard		X	X		
	3GPP TSG SA Release 12 (Free)	Release 12	Exploits new business opportunities such as Public safety and Critical Communications, explores Wi-Fi integration and system capacity and stability.		In progress Planned release March 2015	Technical Standard					
3GPP2	3GPP2 S.R0006-529-A (Free)	Wireless Features Description: Emergency Services	Describes the wireless Emergency Services (i.e., 911) feature that permits a subscriber to dial 911 and be connected to a PSAP (appropriate to the calling subscriber's current location) to request an emergency response from the appropriate agency (e.g., fire, police, ambulance).		Version 1.0 June 2007	Technical Standard (Product/ Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
3GPP2	3GPP2 X.S0049-0 (Free)	All-IP Network Emergency Call Support	Describes the service and procedures in the IMS, including the elements necessary to support emergency services in IMS.		Version 1.0 February 2008	Technical Standard (Interface/ Design)		X	X		
	3GPP2 X.S0057-A (Free)	E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects	Provides a specification of the functions and interfaces of the evolved High Rate Packet Data (eHRPD) Serving Gateway (HSGW) and the IP level interfaces of the eHRPD user equipment (UE).		Version 2.0 October 2012	Technical Standard		X	X		
	3GPP2 X.S0060-0 (Free)	HRPD Support for Emergency Services	Describes the characteristics for the provisioning of IMS emergency services using the High Rate Packet Data (HRPD) network.		Version 1.0 July 2008	Technical Standard (Product/ Design)		X	X		
APCO	APCO ANS 1.101.2-2010 (Free)	Standard for Public Safety Telecommunicators When Responding to Calls of Missing, Abducted, and Sexually Exploited Children	Presents the missing, abducted, and/or sexually exploited child response process for public safety telecommunicators. The standard includes the process from first response through ongoing incident and case support.		Version 2 July 2010	Operational Standard					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
APCO	APCO/NENA ANS 1.102.2-2010 (Free)	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. The assessment tool objectively assesses the capabilities of the PSAP against models representing the best level of preparedness, survivability, and sustainability amidst a wide range of natural and man-made events.		Version 2 July 2010	Operational Standard					X
	APCO ANS 3.103.2-2013 (Free)	Wireless 9-1-1 Deployment and Management Effective Practices Guide	Provides Effective Practices (EPs) to increase the Public Safety Answering Point (PSAP) Managers' understanding of the technology application and the ability to better manage wireless calls, as well as public and responder expectations.		Version 2 September 2013	Operational Standard					X
	APCO/NENA ANS 1.105.1-2009 (Free)	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 1 May 2009 (Version 2 in Development)	Operational Standard					X
	APCO/NENA 1.107.1-201x (Free)	Quality Assurance/Quality Improvement	Provides quality assurance and improvement guidelines.		In Development						X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
APCO	APCO 1.108.1-201x (Free)	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.		In Development	Operational Standard					X
	APCO 1.110.1-201x (Free)	Unified Computer Aided Dispatch Functional Requirements (UCADFR)	Defines unified CAD functional requirements.		In Development	Operational Standard					X
	APCO ANS 1.111.1-2013 (Free)	Public Safety Communications Common Disposition Codes for Data Exchange	Provides a standardized list of disposition codes facilitate effective incident exchange between NG911 PSAPs and other authorized agencies,		Version 1 December 2013	Operational Standard					X
	APCO ANS 1.112.1-2014 (Free)	Best Practices for the Use of Social Media in Public Safety Communications	The purpose of this standard is to provide a consistent foundation for agencies to develop specific operational procedures and competencies. This standard recognizes the need for each agency to customize specific procedures to their local environment.		Version 1 2014	Operational Standard					X
	APCO 1.114.1-201x (Free)	Vehicle Telematics Best Practices	Provides best practices for vehicle telematics in the PSAP.		In Development	Operational Standard					X
	APCO 1.115.1-201x (Free)	Core Competencies, Operational Factors, and Training for Next Generation Technologies in Public Safety Communications			In Development	Operational Standard					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
APCO	APCO/CSAA ANS 2.101.2-2014 (Free)	Alarm Monitoring Company to Public Safety Answering Point (PSAP) Computer-Aided Dispatch (CAD) Automated Secure Alarm Protocol (ASAP)	Provides detailed technical data to software providers who support CAD Systems or alarm monitoring applications concerning the common data elements and structure that shall be utilized when electronically transmitting a new alarm event from an alarm monitoring company to a PSAP.		Version 2 August 2014	Technical Standard					X
	APCO 2.102.1.201x (Free)	Advanced Automatic Collision Notification (AACN) Data Set	Describes and outlines the AACN data set.		In Development	Technical Standard				X	X
	APCO ANS 2.103.1-2012 (Free)	Public Safety Communications Common Incident Types For Data Exchange	Defines and outlines public safety communications common incident types for data exchange.		Version 1 November 2012	Technical Standard				X	X
	APCO/NENA 2.105.1-201X (Free)	NG9-1-1 Emergency Incident Data Document (EIDD)	Provides format for sharing emergency incident information.		In Development	Technical Standard				X	X
	APCO ANS 3.101.2-2013 (Free)	Core Competencies and Minimum Training Standards for Public Safety Communication Training Officers (CTO)	Addresses the minimum training requirements, in general, necessary to foster levels of consistency for all personnel in an emergency communications environment assigned to providing on-the-job training to active 911 professionals and telecommunicators, as well as to promote the leadership role of the CTO.		Version 2 January 2013	Training Standard					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
APCO	APCO ANS 3.102.1-2012 (Free)	Core Competencies and Minimum Training Standards for Public Safety Communications Supervisor	Identifies the core competencies and minimum training requirements for Public Safety Communications Supervisors relating to managing daily operations, performing administrative duties and maintaining employee relations.		Version 1 December 2012	Training Standard					X
	APCO ANS 3.103.1-2010 (Free)	Minimum Training Standards for Public Safety Telecommunicators	Identifies the minimum training requirements for public safety telecommunicators, which typically includes with receiving, processing, transmitting, and conveying public safety information to dispatchers, first responders (police, fire, EMS), and emergency management personnel.		Version 1 February 2011 (Version 2 in Development)	Training Standard					X
	APCO ANS 3.104.1.2012 (Free)	Core Competencies and Minimum Training Standards for Public Safety Communications Training Coordinator	Defines the minimum training standards for PSAP Training Coordinators.		Version 1 December 2012	Training Standard					X
	APCO 3.105.1.201x (Free)	Minimum Training Standard for TTY/TDD Use in the Public Safety Communications Center	Defines the minimum training standards for TTY/TDD use in Public Safety Communications Centers.		In Development	Training Standard					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
APCO	APCO ANS 3.106.1-2013 (Free)	Core Competencies and Minimum Training Standards for Public Safety Communications Quality Assurance Evaluators (QAE)	Defines the minimum training standards for PSAP Quality Assurance Evaluators.		Version 1 April 2013	Training Standard					X
	APCO 3.107.1.201x (Free)	Core Competencies and Minimum Training Standards for Public Safety Communications Technician	Defines the minimum training standards for PSAP Communications Technicians.		In Development	Training Standard					X
	APCO ANS 3.108.1.2014 (Free)	Core Competencies and Minimum Training Standards for Public Safety Communications Instructor	Defines the minimum training standards for PSAP Instructors.		Version 1 February 2014	Training Standard					X
ATIS	ATIS-0500002.2008(R2013) (Fee/Charge)	Emergency Services Messaging Interface (ESMI)	Contains standards for an Emergency Services Interface to the Emergency Services Network (ESNet). It specifies protocols and message sets for use in the Emergency Services Messaging Interface (ESMI). ESMI is the evolution of ESNet that provides sophisticated and robust services to the PSAP and other authorized agencies.		July 2008	Technical Standard (Interface/ Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-0500003 (Fee/Charge)	Routing Number Authority (RNA) for pseudo Automatic Number Identification Codes (pANIs) Used for Routing Emergency Calls: pANI Assignment Guidelines and Procedures	This document 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 (USA & Canada).		July 2005	Technical Standard		X	X		
	ATIS-0500005 (Fee/Charge)	Standard Wireless Text Message Case Matrix	This document was generated to address the need for standard wireless text messages. Currently, some Public Safety Answering Point (PSAP) screen formats provide space for Automatic Location Identification (ALI) text messages and the text messages are used to alert the call taker of a unique condition.		September 2005	Technical Standard		X	X		X
	ATIS-0500006.2008(R2013) (Fee/Charge)	Emergency Information Services Interfaces (EISI) ALI Service	Defines/describes the protocols and message sets used within the Emergency Services Network to communicate between Entities Consuming Emergency Services (ECES) and Entities Providing Emergency Services (EPES).		August 2008	Technical Standard (Interface-Data/Design)		X	X		
	ATIS-0500007.2008(R2013) (Fee/Charge)	Emergency Information Services Interface (EISI) Implemented with Web Services	Defines/describes the protocols and message sets used within the Emergency Services Network to communicate (through the use of web services) between ECES and EPES.		January 2008	Technical Standard (Interface-Data/Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-0500013 (Fee/Charge)	Approaches to Wireless E9-1-1 Indoor Location Performance Testing	Indoor use is becoming very common with the wireless consumer; therefore, a recommendations needs to be made for indoor testing methodologies and evaluations for determining when indoor testing is valid.		February 2010	Technical Standard		X			X
	ATIS-0500015.2010 (Fee/Charge)	Flexible LDF-AMF (Location Determination Function – Access Measurement Function) Protocol (FLAP) Specification	Provide a framework and associated protocol(s) to allow a location determination function to obtain the value of relevant network parameters associated with an end device, and from which the location of that end device may be determined. This standard provides the detailed functional description and protocol specifications for this framework.		August 2010	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-0500017 (Fee/Charge)	Considerations for an Emergency Services Next Generation Network (ES-NGN)	This Technical Report uses the term Emergency Services Next Generation Network (ES-NGN) to define an emergency services architecture based upon the ATIS definition of NGN. This Technical Report identifies standards and standards activities that are relevant to the evolution of emergency services networks in the context of next generation telecommunications networks. In addition it identifies potential gaps where standards need to be developed in order to complete the definition of emergency services in next generation networks. The focus of this Technical Report is the interconnection between the ES-NGN and networks that originate emergency calls. It also discusses connectivity to PSAPs and legacy emergency services networks.		June 2009	Technical Report		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-0500018 (Fee/Charge)	P-ANI Allocation Tables for ESQKs, ESRKs, and ESRDs	This document contains ESQK, ESRK, and ESRD allocation tables and capacities. The content of this standard is intended to assist Wireless Service Providers (WSPs) and Mobile Positioning Centers (MPCs) in improving the efficacy of the p-ANI number use and administration, and complement number preservation and utilization of limited p-ANI number resources.		August 2014	Technical Standard		X	X		
	ATIS-0500019.2010 (Fee/Charge)	Request for Assistance Interface (RFAI) Specification	Defines/describes the Request for Assistance Interface (RFAI) between the Emergency Services Next Generation Network (ES-NGN) and a PSAP.		September 2010	Technical Standard				X	X
	ATIS-0500023 (Fee/Charge)	Applying Common IMS to NG9-1-1 Networks	Defines an IMS counterpart to the NENA i3 specification.		April 2013	Technical Issue Documentation		X	X	X	
	ATIS-0500024 (Fee/Charge)	Comparison of SIP Profiles	This Technical Report compares SIP profiles defined by ATIS, 3GPP, and NENA as they relate to emergency services.		April 2013	Technical Report		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-0500026 (Fee/Charge)	Operational Impacts on Public Safety of ATIS-0700015, Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination	Supplemental document that explains, in plain language, the IP to NG911 interfaces, without overdependence on technical terms and acronyms, to assist Public Safety in understanding the operational impact of the new standard. This document explains the operational impacts of the ATIS-0700015 standard compared to existing network functionality in today's non-Internet Protocol Multimedia Subsystem (IMS) originating networks. It provides Public Safety the needed insight and overview of what to expect from future IMS originated emergency calls. This document is not a specification but is intended to be informative only.		September 2014	Technical Standard		X	X	X	X
	ATIS-0700015.v002 (Fee/Charge)	ATIS Standard for Implementation of 3GPP Common IMS Emergency Procedures for IMS Origination and ESInet/Legacy Selective Router Termination	This document describes North American emergency call handling procedures in an IMS-based origination network (including steps taken by the originating device and network elements) and routing of such calls to a terminating ESInet or to a legacy Selective Router.		March 2014	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS	ATIS-1000026 .2008(R2013) (Fee/Charge)	Session Border Controller Functions and Requirements	Defines the Session Border Controller (SBC) functions and requirements that reside within a service provider's network.		April 2008	Technical Standard		X	X		
ATIS	ESIF Issue 76 (Fee/Charge)	Analysis of Unwanted User Service Interactions with NG9-1-1 Capabilities	Defines multiple types of originating service calls and their corresponding service interactions with NG911 capabilities.		In Development	Technical Issue Documentation		X	X	X	X
	ESIF Issue 81 (Fee/Charge)	Applying Common IMS to NG911 Networks (Stage 2 and 3) Specification	Defines call processing, transport, or delivery of Emergency Service calls within the NG911 network to the appropriate PSAP.		In Development	Technical Issue Documentation		X	X	X	X
	ESIF Issue 82 (Fee/Charge)	IMS-based Next Generation Emergency Services Network Interconnection			In Development	Technical Issue Documentation					
	ESIF Issue 85 (Fee/Charge)	Supplemental Guide to ATIS-0700015 for Public Safety		ATIS-0700015	In Development	Technical Issue Documentation					
ATIS/TIA	ANSI/J-STD-036-B (R2013) (Fee/Charge)	Enhanced Wireless 9-1-1 Phase II (Joint TIA/ATIS ANS)	Provides a solution for handling of Wireless Enhanced Emergency Calls for the FCC E911 Phase II Mandate.		May 2007	Technical Standard		X	X		X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ATIS/TIA	J-STD-110 including J-STD-110.a & J-STD-110.01 (Fee/Charge)	Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification	Defines the requirements, architecture and procedures for text messaging to 911 emergency services using native wireless operator SMS capabilities for the existing generation and next generation (NG911) Public Safety Answering Points.	J-STD-110.01	March 2013	Joint Standard					X
	J-STD-110.01 (Fee/Chargee)	Joint ATIS/TIA Implementation Guideline for J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification	These implementation guidelines address Commercial Mobile Service Providers (CMSPs) and Text Control Center (TCC) provider deployment considerations of J-STD-110.	J-STD-110	November 2013	Joint Standard					X
	J-STD-110.a (Fee/Charge)	Joint ATIS/TIA Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification	The purpose of this Supplement is to provide errata and clarifications to J-STD-110, Joint ATIS/TIA Native SMS to 911 Requirements and Architecture Specification.	J-STD-110	November 2013	Joint Standard					X
CALEA	Standards for Law Enforcement Agencies (Fee/Charge)	81.0 Communications	Defines what law enforcement organizations should be doing in regard to all aspects of communications.		November 2010	Operational Standard					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
CALEA	Standards for Public Safety Communications Agencies (Fee/Charge)	Public Safety Communications Standards Manual	Contains standards organized into seven chapters or topic areas, including Organization; Direction and Supervision; Human Resources; Recruitment, Selection, and Promotion; Training; Operations; and Critical Incidents, Special Operations, and Homeland Security.		September 2011	Operational Standard					X
DOC	FIPS-PUB-140-2 (Free)	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.	ISO/IEC JTC 1/SC 27	December 2002 (FIPS-PUB-140-3 has a revised draft)	Technical Standard		X	X		
	FIPS-PUB-180-4 (Free)	Secure Hash Standard (SHS)	Specifies five secure hash algorithms for computing a condensed representation of electronic data (message).		March 2012	Technical Standard		X	X		
	FIPS-PUB-197 (Free)	Advanced Encryption Standard (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 2001	Technical Standard (Data/ Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
DOC	NIST Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity	The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.		February 12, 2014			X	X	X	X
DHS/ DOC	NIEM	National Information Exchange Model (NIEM)	Designed to develop, disseminate and support 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.	EDXL; CAP							
ETSI	ETSI TS 101 470 (Free)	Emergency Communications (EMTEL); Total Conversation Access to Emergency Services	Define requirements based on the background described in TR 103 170, for using Total Conversation for emergency services and make access of emergency services possible to people with disabilities.		Version 1.1.1 November 2013	Technical Standard	X				X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ETSI	ETSI TS 102 164 (Free)	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.	OMA-TS-MLP-V3_2-20051124-C	Version 1.3.1 September 2006	Technical Standard					
	ETSI TS 102 424 (Free)	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 a NGN to support emergency communications (EMTEL) from citizen to authority.		Version 1.1.1 September 2005	Technical Standard					
	ETSI TS 123 167 (Free)	Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS) emergency sessions	Defines the stage 2 service description for emergency services in the IMS, including the elements necessary to support IM emergency services.	3GPP TS 23.167 Version 12.0.0 Release 12	Version 12.0.0 September 2014	Technical Standard (Product-Interface/ Design)		X	X		
	ETSI TS 182 009 (Free)	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.	3GPP TS 23. 09 (Release 7) 3GPP TS 23.167, (Release 7)	Version2.1.1 October 2008	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ETSI	ETSI ES 203 178 (Free)	Functional architecture to support European requirements on emergency caller location determination and transport	Considering TS 102 650 and architectures from other standardization organizations, a single functional architecture to support European requirements on emergency caller location determination and transport needs to be developed 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.		In Progress Draft December 2014	Version1..0.0 Final Draft April 2004	X	X	X	X	
	ETSI ES 282 007 (Free)	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional Architecture	Presents the IMS core component of the TISPAN NGN functional architecture and its relationship to other subsystems and components.	3GPP TS 23.517 (Release 8)	Version 2.1.1 November 2008	Technical Standard (Interface/ Design)		X	X		
FGDC	FGDC-STD-001-1998 (Free)	Content Standard for Digital Geospatial Metadata	This standard is intended to support the collection and processing of geospatial metadata. It is intended to be useable by all levels of government and the private sector.		Version 2.0 1998						

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
FGDC	FGDC-STD-016-2011 (Free)	United States Thoroughfare, Landmark, and Postal Address Data Standard	Supports seamless exchange of address information, and foster consistent implementation of this standard, by defining XML models for every address element, attribute, and class, integrated into a single XML Schema Document.		Version 2.0 February 2011						
IEEE	IEEE 802.1AB-2009_Cor1-2013 (Free)	Station and Media Access Control Connectivity Discovery	Defines and describes the protocol and set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802 LANs.		Corrigendum 1: Technical & Editorial Corrections June 14, 2013	Technical Standard	X	X	X		
	IEEE 802.1AC-2012 (Free)	Media Access Control (MAC) Services Definition	Defines the MAC found in LANs and MANs, and the Internal Sublayer Service and External Internal Sublayer Service provided within MAC Bridges, in abstract terms of a) their semantics, primitive actions and events, b) the parameters of, interrelationship between, and valid sequences of, these actions and events.		September 14, 2012	Technical Standard		X	X		
	IEEE 802.11-2012 (Free)	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications	Defines and describes the characteristics associated with WLANs.		March 29, 2012	Technical Standard (Product/ Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IEEE	IEEE 802.16 (Free)	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.	ETSI HiperMAN	August 17, 2012	Technical Standard (Product/ Design)		X	X		
	IEEE 802.23 (Fee/Charge)	Emergency Services for Internet Protocol (IP) Based Citizen to Authority Communications	Defines and describes the characteristics associated with voice, data, and multi-media requests across IEEE 802 networks and provides a uniform approach for transferring required data for emergency services requests.		Working Group Disbanded in June 2011	Technical Standard (Product-Interface/ Design)		X	X	X	
	IEEE 1512 (Fee/Charge)	Standard for Common Incident Management Message Sets for Use by Emergency Management Centers	Addresses the exchange of vital data about public safety and emergency management issues involved in transportation-related events, through common incident management sets.	IEEE Std-2000; IEEE Std 1512.1-2003; IEEE Std 1512.3-2002	July 7 2000	Technical Standard					
	IEEE 1903 (Fee/Charge)	Standard for the Functional Architecture of Next Generation Service Overlay Networks	Specifies a functional architecture for Next Generation Service Overlay Network, consisting of a set of functional entities (FEs), their functions, reference points and information flows to illustrate service interaction and media delivery among FEs and external components.		October 7, 2011	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IEEE	IEEE 446-1995 (Fee/Charge)	Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications	This Recommended Practice addresses the uses, power sources, design, and maintenance of emergency and standby power systems. Including recommendations for protecting both power sources and switching equipment during fault conditions. and the design of system grounding, and reliability objectives		July 3, 1996	Best Practice				X	X
IETF	RFC 3261 (Free)	SIP: Session Initiation Protocol	Describes the Session Initiation Protocol (SIP), an application-layer control (signaling) protocol for creating, modifying, and terminating sessions (include Internet telephone calls, multimedia distribution, and multimedia conferences) with one or more participants.		July 2002	Proposed Technical Standard (Interface/ Design)		X	X		
	RFC 3856 (Free)	A Presence Event Package for the Session Initiation Protocol (SIP)	Describes the usage of the SIP for subscriptions and notifications of presence.		August 2004	Proposed Technical Standard		X	X		
	RFC 3966 (Free)	The tel URI for Telephone Numbers	Specifies the URI (Uniform Resource Identifier) scheme “tel”. The “tel” URI describes resources identified by telephone numbers.		December 2004	Proposed Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 3986 (Free)	Uniform Resource Identifiers (URI): Generic Syntax	Defines the generic URI syntax and a process for resolving URI references that might be in relative form, along with guidelines and security considerations for the use of URIs on the Internet.		January 2005	Technical Standard		X	X		
	RFC 4079 (Free)	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 moreover demonstrates that tools already developed for presence could be reused to simplify the standardization and implementation of GEOPRIV.		July 2005	Technical Information Document		X	X		
	RFC 4119 (Free)	A Presence-based GEOPRIV Location Object Format	Defines and describes an object format, which is an extension of the privacy-sensitive Presence Information Data Format (PDIF), for carrying geographical information (physical position) on the Internet.		December 2005	Proposed Technical Standard (Data/Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 5069 (Free)	Security Threats and Requirements for Emergency Call Marking and Mapping	This document reviews the security threats associated with the marking of signalling messages to indicate that they are related to an emergency, and with the process of mapping locations to Universal Resource Identifiers (URIs) that point to Public Safety Answering Points (PSAPs).		January 2008	Informational Document		X	X		
	RFC 5139 (Free)	Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)	Defines an XML format for the representation of civic location.		February 2008	Proposed Technical Standard		X	X		
	RFC 5222 (Free)	LoST: A Location-to-Service Translation Protocol	Defines and describes an XML-based protocol for mapping service identifiers and geodetic or civic location information to service contact URIs. In particular, it can be used to determine the location-appropriate PSAP for emergency services.		August 2008	Proposed Technical Standard (Interface/ Design)		X	X		
	RFC 5223 (Free)	Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Configuration Protocol (DHCP)	Describes how a LoST client can discover a LoST server using the Dynamic Host Configuration Protocol (DHCP).		August 2008	Proposed Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 5491 (Free)	GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations	Makes recommendations on how to constrain, represent, and interpret locations in a PIDF-LO.		March 2009	Proposed Technical Standard		X	X		
	RFC 5985 (Free)	HTTP Enabled Location Delivery (HELD)	Defines and describes a XML-based protocol that can be used to acquire device location information from a Location Information Server (LIS) within access networks employing both wired technology (e.g., DSL, cable)and wireless technology (e.g., WiMAX).		September 2010	Proposed Technical Standard (Interface/ Design)		X	X		
	RFC 6155 (Free)	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 describe the conditions where requests containing identifiers are permitted.		March 2011	Proposed Technical Standard		X	X		
	RFC 6442 (Free)	Location Conveyance for the Session Initiation Protocol	Defines an extension to the SIP to convey geographic location information from one SIP entity to another SIP entity.		December 2011	Proposed Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 6753 (Free)	A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD)	Describes how to use HTTP over Transport Layer Security (TLS) as a dereferencing protocol to resolve a reference to a Presence Information Data Format Location Object (PIDF-LO).		October 2012	Proposed Technical Standard		X	X		
	RFC 6772 (Free)	Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information	This document defines an authorization policy language for controlling access to location information. It extends the Common Policy authorization framework to provide location-specific access control.		January 2013	Proposed Technical Standard	X	X			
	RFC 6739 (Free)	Synchronizing Service Boundaries and <mapping> Elements Based on the Location-to-Service Translation (LoST) Protocol	Defines an XML protocol to exchange mappings between two nodes		October 2012	Experimental Technical Standard		X	X		
	RFC 6848 (Free)	Specifying Civic Address Extensions in the Presence Information Data Format Location Object (PIDF-LO)	Describes a backward-compatible mechanism for adding civic address elements to the GEOPRIV civic address format.		January 2013	Proposed Technical Standard		X	X		
	RFC 6881 (Free)	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	Best Current Practice		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 6915 (Free)	Flow Identity Extension for HTTP-Enabled Location Delivery (HELD)	RFC 6155 specifies an extension for the HTTP-Enabled Location Delivery (HELD) protocol, allowing the use of an IP address and port number to request a Device location based on an individual packet flow.		April 2013	Proposed Technical Standard		X	X		
	RFC 7035 (Free)	Relative Location Representation	This document defines an extension to the Presence Information Data Format Location Object (PIDF-LO) (RFC 4119) for the expression of location information that is defined relative to a reference point.		October 2013	Proposed Technical Standard		X	X		
	RFC 7090 (Free)	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	Proposed Technical Standard		X	X		
	RFC 7105 (Free)	Using Device-Provided Location-Related Measurements in Location Configuration Protocols	This document describes a protocol for a Device to provide location-related measurement data to a Location Information Server (LIS) within a request for location information.		January 2014	Proposed Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 7163 (Free)	URN for Country-Specific Emergency Services	This document 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". This document updates those instructions to allow such registrations when, at the time of registration, those services are offered in only one country.		March 2014	Proposed Technical Standard		X	X		
	RFC 7199 (Free)	Location Configuration Extensions for Policy Management	This document 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	Proposed Technical Standard		X	X		
	RFC 7216 (Free)	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	Proposed Technical Standard		X	X		
	RFC 7378 (Free)	Trustworthy Location Information	Outlines potential threats to trustworthy location and analyzes the operational issues with potential solutions.		December 2014	Informational Document					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	RFC 7406 (Free)	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	Informational Document					
IETF	Internet Draft (draft-ietf-ecrit-additional-data-28) (Free)	Additional Data related to an Emergency Call	When an emergency call is sent to a Public Safety Answering Point (PSAP), the device that sends it, as well as any service provider in the path of the call, or access network may have information about the call which the PSAP may be able to use. This document describes an XML data structure that contains this kind of information in a standardized form.		February 4, 2015(Draft Status expires June 2015)	Draft Technical Standard		X	X		
	Internet Draft (draft-ietf-ecrit-data-only-ea-09) (Free)	Data Only Emergency Calls	Defines protocols for calls made to PSAPs from data only providers (e.g., temperature sensors issuing alerts, vehicles sending crash data).		October 2014 (Draft Status expires April 2015)	Draft Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	Internet Draft (draft-ietf-ecrit-held-routing-00) (Free)	A Routing Request Extension for the HELD Protocol	This document describes a solution where by the routing information may be obtained from a location server using a simple extension to the HELD protocol, in circumstances where public LoST servers or a distributed network of forest guides linking public LoST servers is not available.		December 2014 (Draft status Expires June 2015)	Draft Technical Standard		X	X		
	Internet Draft (draft-ietf-ecrit-similar-location-00) (Free)	A LoST extension to return complete and similar location info	This document introduces a new way to provide returned location information in LoST responses that is either of a 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.		October 2014 (Draft status Expires April 2015)	Draft Technical Standard		X	X		
	Internet Draft (draft-ietf-geopriv-uncertainty-04) (Free)	Representation of Uncertainty and Confidence in PIDF-LO	This document defines key concepts of uncertainty and confidence as they pertain to location information. Methods for the manipulation of location estimates that include uncertainty information are outlined.		October 2014 (Draft status Expires April 2015)	Draft Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
IETF	Internet Draft (draft-ietf-ecrit-car-crash-01) (Free)	Next-Generation Vehicle-Initiated Emergency Calls	This document describes how to use IP-based emergency services mechanisms to support the next generation of emergency calls placed by vehicles and conveying vehicle, sensor, and location data related to the crash or incident.		October 2014 (Draft status Expires April 2015)	Draft Informational Document	X	X	X		
ISO	ISO/IEC 20000-1:2011 (Charge)	Service Management Part 1: Service Management System Requirements	ISO/IEC 20000-1:2011 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil agreed service requirements.	ISO 20000 Family	2011	Operational Standard	X	X	X	X	X
	ISO/IEC 27000:2014 (Charge)	Information Security Management Systems – Overview and Vocabulary	ISO/IEC 27000:2014 provides the overview of information security management systems (ISMS), and terms and definitions commonly used in the ISMS family of standards.	ISO 27000 Family	2014	Operational Standard	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27001:2013 (Charge)	Information Security Management Systems – Requirements	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.	ISO 27000 Family	2013	Operational Requirements	X	X	X	X	X
	ISO/IEC 27002:2013 (Charge)	Code of Practice for Information Security Controls	ISO/IEC 27002:2013 gives 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).	ISO 27000 Family	2013	Guidelines	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27003:2010 (Charge)	Information Security Management System Implementation Guidance	ISO/IEC 27003:2010 focuses on the critical aspects needed for successful design and implementation of an Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2005. It describes the process of ISMS specification and design from inception to the production of implementation plans. It describes the process of obtaining management approval to implement an ISMS, defines a project to implement an ISMS (referred to in ISO/IEC 27003:2010 as the ISMS project), and provides guidance on how to plan the ISMS project, resulting in a final ISMS project implementation plan.	ISO 27000 Family	2010	Design Operational	X	X	X	X	X
	ISO/IEC 27004:2009 (Charge)	Information Security Management - Measurement	ISO/IEC 27004:2009 provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.	ISO 27000 Family	2009	Design Operational	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27005:2011 (Charge)	Information Security Risk Management	ISO/IEC 27005:2011 provides guidelines for information security risk management.	ISO 27000 Family	2011	Guidelines Operational	X	X	X	X	X
	ISO/IEC 27011:2008 (Charge)	Information Security Management Guidelines for Telecommunications Organizations based on ISO/IEC 27002	The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security management in telecommunications organizations. The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.	ISO 27000 Family	2008	Guidelines Operational		X	X	X	X
	ISO/IEC 27031:2011 (Charge)	Guidelines for Information and Communication Technology Readiness for Business Continuity	ISO/IEC 27031:2011 describes the concepts and principles of information and communications technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity	ISO 27000 Family	2011	Guidelines Operational	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27033-1:2009 (Charge)	Network Security—Part 1: Overview and Concepts	ISO/IEC 27033-1:2009 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security.	ISO 27000 Family	2009	Definitions	X	X	X	X	X
	ISO/IEC 27033-2:2012 (Charge)	Network Security—Part 2: Guidelines for the Design and Implementation of Network Security	ISO/IEC 27033-2:2012 gives guidelines for organizations to plan, design, implement and document network security.	ISO 27000 Family	2012	Guidelines	X	X	X	X	X
	ISO/IEC 27033-3:2010 (Charge)	Network Security—Part 3: Reference Networking Scenarios – Threats, Design Techniques and Control Issues	ISO/IEC 27033-3:2010 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents.	ISO 27000 Family	2010	Guidelines	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27033-4:2014 (Charge)	Network Security—Part 4: Securing Communications between Networks Using Security Gateways	ISO/IEC 27033-4:2014 gives guidance for securing communications between networks using security gateways (firewall, application firewall, intrusion protection system, etc.) in accordance with a documented information security policy of the security gateways.	ISO 27000 Family	2014	Guidelines	X	X	X	X	X
	ISO/IEC 27033-5:2013 (Charge)	Network Security – Part 5: Securing Communications Across Networks Using Virtual Private Networks (VPNs)	ISO/IEC 27033-5:2013 gives guidelines for the selection, implementation, and monitoring of the technical controls necessary to provide network security using virtual private network (VPN) connections to interconnect networks and connect remote users to networks.	ISO 27000 Family	2013	Guidelines	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ISO	ISO/IEC 27035:2011 (Charge)	Information Security Incident Management	ISO/IEC 27035:2011 provides a structured and planned approach to: detect, report and assess information security incidents; respond to and manage information security incidents; detect, assess and manage information security vulnerabilities; and continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.	ISO 27000 Family	2011	Operational	X	X	X	X	X
	ISO/IEC 27037:2012 (Charge)	Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence	ISO/IEC 27037:2012 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.	ISO 27000 Family	2012	Guidelines	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
ITU	ITU-T Y.1271 (Free)	Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks	Many challenges and considerations need to be addressed in defining and establishing the functional capabilities to support emergency telecommunications in evolving circuit- and packet-switched telecommunications networks. This Recommendation presents an overview of the basic requirements, features, and concepts for emergency telecommunications that evolving networks are capable of providing.		July 2014	Technical		X	X	X	X
	ITU-T Y.2705 (Free)	Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS)	Emergency telecommunications service (ETS) is a national service, providing priority communications services to ETS authorized users in times of disaster and emergencies. Recommendation ITU-T Y.2705 provides minimum security requirements for the inter-network interconnection of ETS. This will allow 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 2013	Technical		X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NAED	Emergency Telecommunicator Certification (Fee/Charge)	Emergency Telecommunicator Certification	Designed to train new employees unfamiliar with emergency communication centers, emergency telecommunication technology, interpersonal communication, legal issues, and job stress factors.		October 2011	Operational Certification					X
NENA	NENA ADM-000.18-2014 (Free)	Master Glossary of 911 Terminology	Guide for readers of NENA publications and a tool for members of the NENA committees that prepare them. It defines the terms, acronyms, and definitions associated with the 911 industry. Intended users of this document are any person needing NENA's definition/description of a 911 related term.		Ongoing Revision In Progress	Information Document	X	X	X	X	X
	NENA 02-010 (Free)	Standard Data Formats For 911 Data Exchange & GIS Mapping	Sets forth NENA standard formats for Automatic Location Identification (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.		Version 9.0 March 2011/New Document for NG911 in progress	Technical Standard		X	X	X	

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 02-014 (Free)	GIS Data Collection and Maintenance Standards	This document is the NENA recommended standard for GIS data collection and GIS data maintenance.		Version 1 July 2007	Technical Standard		X	X	X	
	NENA TBD	GIS Data Model for NG9-1-1			In Progress			X	X	X	
	NENA 02-015 (Free)	Technical Standard for Reporting and Resolving ANI/ALI Discrepancies and No Records Found for Wireline, Wireless and VoIP Technologies	This NENA document sets forth standards for PSAP jurisdictions, Access Infrastructure Providers (AIP), Service Providers and Data Base Management System Providers (DBMSPs) in reporting and resolving discrepancies that occurred during a 911 call.		Version 1 June 2009	Technical Standard		X	X	X	X
	NENA 03-509 (Free)	Femtocell and UMA	Describe in technical as well as operational terms the current state of femtocell and UMA deployments with respect to call processing of E911 calls, and to identify the impacts to PSAPs of receiving and processing calls from femtocells.		Version 1 January 2011	Technical Information Document					X
	NENA 06-750 (Free)	Model Legislation, Enhanced 911 for Multi-Line Telephone Systems	Policy document that reflects changes in IP technology; Implementation & Testing; Training and use of building code Fire Zones to facilitate the creation of the Emergency Response Location.		Version 3.0 February 2011	Requirements Document	X				

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 07-503 (Free)	Network Interfaces for E911 and Emerging Technologies	Describes network interfaces for users, manufactures and providers of E911 in Emerging Technologies such as VoP, VoIP, and VoDSL.		Version 1 September 2002	Technical Standard (Interface/ Design)		X	X		
	NENA 07-504 (Free)	Automatic Collision Notification and Vehicle Telematics	Defines/describes communications methodologies and protocols to facilitate emergency communications between Telematics Service Providers (TSP) and PSAPs (existing and NG911).		Version 1 June 2007	Technical Standard (Data/ Design)		X	X		
	NENA 08-001 (Free)	Interim VoIP Architecture for Enhanced 9-1-1 Services (i2)	This document is the NENA recommended standard for the i2 architecture to support the interconnection of VoIP domains with the existing Emergency Services Network infrastructure in support of the migration toward end-to-end emergency calling over the VoIP networks between callers and PSAPs.		Version 2 August 2010	Technical Standard		X	X	X	

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 08-002 (Free)	NENA Functional and Interface Standards for Next Generation 9-1-1 (i3)	Describes the Emergency Services IP network (ESInet), which is designed as an IP-based inter-network (network of networks) shared by all agencies that may be involved in any emergency. The NG911 PSAP is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the i3 standard.		Version 1 December 2007	Technical Standard (Interface/ Design)		X	X		
	NENA 08-003 (Free)	Detailed Functional and Interface Specification for the NENA i3 Solution – Stage 3	Builds upon prior NENA publications including i3 requirements [1] and architecture [101] documents and provides a baseline to other NG911-related specifications.		Version 1 June 2011 (Version 2 pending release)	Technical Standard		X	X	X	
	NENA 08-501 (Free)	Technical Information Document on the Network Interface to IP Capable PSAP	Provides technical information to guide manufacturers of network equipment and PSAP CPE in the development of Internet Protocol based interfaces between the network and PSAP CPE and to assist E911 Network Service Providers and PSAPs in implementing such interfaces.		Version 1 June 2004	Technical Information Document	X	X	X	X	X
	NENA 08-503 (Free)	VoIP Characteristics	The purpose of this document is to procure, create and publish a VoIP primer document to be used by individuals not familiar with VoIP technology.		Version 1 June 2004	Technical Information Document	X	X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 08-505 (Free)	Recommended Method(s) for Location Determination to Support IP-Based Emergency Services	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.		Version 1 December 2006	Technical Information Document		X	X	X	
	NENA 08-506 (Free)	Emergency Services IP Network Design for NG91-1-	The purpose of this document is to provide network architects, consultants, 911 entities, and state authorities with the information that will assist them in developing the requirements for and/or designing ESInets today that will be capable of meeting the requirements of an NG911 system.		Version 1 December 2011	Technical Information Document				X	
	NENA 08-751 (Free)	NENA i3 Technical Requirements Document	Specifies the requirements the i3 (Long Term Definition) Standard should meet.		Version 1 September 2006	Technical Standard	X	X	X	X	X
	NENA 08-752 (Free)	Location Information to Support IP-Based Emergency Services	Provides the NENA requirements for providing information to support emergency calling.		Version 1 December 2006	Technical Standard		X	X	X	

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 53-507 (Free)	Virtual PSAP Management	Guide for PSAP staff and policy makers to evaluate and consider the opportunities and challenges presented with the Next Generation 911 systems as they relate to personnel and PSAP management.		Version 1 May 2009	Operational Information Document					X
	NENA 54-750 (Free)	Human Machine Interface & PSAP Display Requirements	Prescribes the requirements for the human machine interface (HMI) display for NG911.		Version 1 October 2010	Operational Standard					X
	NENA 57-750 (Free)	NG9-1-1 System & PSAP Operational Features & Capabilities Requirements	Contains a list of operational capabilities or features that are expected to be supported in a standards-based NG911 system.		Version 1 June 2011	Operational Standard					X
	NENA STA-008.2-2014 (Free)	NENA Registry System (NRS)	This document describes how registries are created and maintained in NENA.		Version 1 October 2014	Joint Technical (Data) and Operational Standard				X	X
	NENA 71-001 (Free)	NENA Standard for NG9-1-1 Additional Data	Describes the use of additional data available with NG911 (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 Emergency Information Data Document (EIDD) Specification.		Version 1 September 2009 (Version 2 in progress)	Technical Standard (Data/ Design)		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA STA-004.1-2014 (Free)	Next Generation 9-1-1 (NG9-1-1) Civic Location Data Exchange Format (CLDXF)	Supports the exchange of United States civic location address information about 911 calls, both within the U.S. and internationally. Identifies the data elements needed for address data exchange, and provides an XSD for implemented the standard.		Version 1 March 2014	Technical Standard		X	X	X	
	NENA 71-501 (Free)	Information Document for Synchronizing Geographic Information System databases with MSAG & ALI	Provides PSAP management, vendors, and other interested parties the necessary guidelines for synchronizing GIS data with existing 911 databases.		Version 1.1 September 2009	Technical and Operational Standard		X	X	X	
	NENA 71-502 (Free)	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.		Version 1 August 2010	Technical and Operational Information Document					
	NENA 73-501 (Free)	Use Cases & Suggested Requirements for Non-Voice-Centric (NVC) Emergency Services	Identifies suggested requirements for Non-Voice Centric Emergency Service.		Version 1 January 2011	Technical Information Document	X	X	X	X	X
	NENA 75-001 (Free)	Security for Next-Generation 9-1-1 Standard (NG-SEC)	Establishes the minimal guidelines and requirements for the protection of NG911 assets or elements within a changing business environment.		Version 1 February 2010	Technical Standard (Interface/ Design)		X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA 75-502 (Free)	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.		Version 1 December 2011	Technical Information Document					X
	NENA INF-008.2-2014 (Free)	NG9-1-1 Transition Plan Considerations	This Information Document is intended to provide NENA's recommendations for transitioning to NG911.		Version 2 November 2013	Information Document		X	X	X	X
	NENA TBD	Standards for the Provisioning and Maintenance of GIS data to ECRF/LVR	Defines the operational processes and procedures necessary to support the i3 Emergency Call Routing Function (ECRF) and Location Validation Function (LVF) and identifies ECRF/LVF performance and implementation tradeoffs for 911 Authorities' consideration.		Version 1 is currently in review	Technical Standard		X	X	X	X
	NENA-STA-003 (Free)	NG9-1-1 Routing Policy Rules	Defines templates to be used when drafting policy rules to address how and where calls are diverted if the target PSAP is unreachable.		August 2013	Technical Standard				X	X
	NENA INF-003 (Free)	Potential Points of Demarcation in NG9-1-1 Networks	Identifies points of demarcation and the relative merits of different demarcation options from a regulatory or financial perspective.		March 2013	Information Document				X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA/APCO INF-005 (Free)	Emergency Incident Data Document (EIDD) Information	Provides information on data components that will be used in the future EIDD technical standard to share emergency incident information between and among authorized entities and systems		February 2014	Information Document				X	X
	NENA-INF-006.1-2014 (Free)	NG9-1-1 Planning Guidelines	Provides guidance to help 911 Authorities create a smooth, timely and efficient transition plan to accomplish implementation of NG9-1-1.		January 2014	Information Document					X
	NENA-INF-007.1-2013 (Free)	Handling Text-to-9-1-1in the PSAP	Provides a guideline for PSAPs with recommendations for emergency calling to 911 using text messaging.		October 2013	Information Document					X
	NENA-INF-009.1-2014 (Free)	Requirements for a National Forest Guide	The purpose of this information document is to gather a set of requirements for a national, authoritative Forest Guide (FG) in order to allow an entity to procure the technology and services required from this NG9-1-1 functional element.		August 2014	Information Document					X
	NENA-INF-011.1-2014 (Free)	NG9-1-1 Policy Routing Rules Operations Guide	This document is provided to assist 911 Governing Authorities in using Policy Routing Rules (PRRs) during the full life cycle of a NG9-1-1 System.		October 2014	Information Document					X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA TBD	NG9-1-1 Data/Database Management			Working Group currently being established	Technical Standard					
	NENA TBD	ESInet Management	Guide for PSAP staff and policy makers to evaluate and consider the opportunities and challenges presented with the Next Generation 9-1-1 systems as they relate to personnel and PSAP management.		Pending	Technical Standard				X	
	NENA TBD	NG9-1-1 Operations Management for 911 Authorities			Pending	Operational Standard					X
	NENA TBD	NG9-1-1 Systems Operations			Pending	Technical Standard					
	NENA TBD	PSAP Procedural Transition to NG9-1-1			Pending	Technical Standard					X
	NENA/APCO TBD	NG9-1-1 Public Safety Answering Point (PSAP) Requirements	This technical requirements document introduces requirements for a NG9-1-1 Public Safety Answering Point (PSAP) that is capable of receiving IP-based signaling and media for delivery of emergency calls conformant to the latest version of the NENA i3 Architecture document		In Progress	Technical Requirements Document					X
	NENA TBD	NG9-1-1 System Management Guide			Version 1 In Progress	Operational Information Document					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NENA	NENA TBD	Location Information Service (LIS) Standard			Pending	Technical Standard					
	NENA REF Not Numbered	NG9-1-1 Public Education Plan for Elected Officials and Decision Makers	The purpose of this document is to provide guidance when reaching out to local decision makers to educate them on NG9-1-1 basics and the need to address funding, legislative and regulatory issues to enable the transition to NG9-1-1.		September 2013	Information Document					X
	NENA REF Not Numbered	SMS Text-to-9-1-1 Resources for PSAPs & 9-1-1 Authorities	This document provides information and planning guidelines for Public Safety to support their efforts to plan and implement Interim SMS Text for 911 service		May 2014	Information Document					X
	NENA (Not Numbered)	Next Generation 9-1-1 Transition Policy Implementation Handbook	A guide for 911 leaders and government officials responsible for ensuring that federal, state and local 911 laws and regulations effectively enable the implementation of NG9-1-1 systems.		March 2010	Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NFPA	NFPA 72 (Fee/Charge)	National Fire Alarm and Signaling Code (Mass Notification Requirements)	Defines and describes the application, installation, location, performance, inspection, testing, and maintenance of fire alarm systems, supervising station alarm systems, public emergency alarm reporting systems, fire warning equipment and emergency communications systems (ECS), and their components.		2013 Edition (Next Edition released 2016)	Technical Standard					
	NFPA 1061 (Free)	Standard for Professional Qualifications for Public Safety Telecommunications Personnelr	Identifies the minimum job performance requirements for public safety telecommunicators.		2014 Edition (Next Edition released 2018)	Operational Standard					
	NFPA 1221 (Free)	Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems	Defines and describes the installation, performance, operation, and maintenance of public emergency services communications systems and facilities.		2013 Edition (Next Edition released 2016)	Technical Standard					
	NFPA 1600 (Free)	Standard on Disaster/ Emergency Management and Business Continuity Programs	Establishes a common set of criteria for disaster/emergency management and business continuity programs.		2013 Edition (Next Edition released 2016)	Operational Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NRIC	9-9-3215 (Free)	Mobile Switching Center(MSC) Default Route Operational Standard Recommendation	For Network Operators that operate Mobile Switching Centers (MSCs), the MSC should default route 911 calls based on cell sector/tower location to the proper serving Public Safety Answering Point (PSAP) when necessary and where feasible.			Best Practice					
	9-9-3216 (Free)	Default Routing	For Network Operators that cannot default route 911 calls based on cell sector/tower location, switch level defaulted calls should be routed to a fast busy tone or to an appropriate recorded announcement.			Best Practice					
	9-9-3217 (Free)	E9-1-1 Service Provider Contact Information	Network Operators and Service Providers should provide and maintain current 24/7/365 contact information accessible to Public Safety Answering Points (PSAPs) so that PSAPs may obtain additional subscriber information as appropriate.			Best Practice					
	9-9-3218 (Free)	Training on Obtaining E9-1-1 Phase II Data	PSAPs should provide Training to educate PSAP personnel as to the process to obtain E9-1-1 Phase II data.			Best Practice					
NRIC	9-9-3219 (Free)	Training on E9-1-1 Phase II ALI Display	PSAPs should provide training to educate PSAP personnel as to the proper meaning and interpretation of the E9-11 Phase II display parameters.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	9-9-3223 (Free)	Originating Source to E9-1-1 Selective Router Trunking Architecture	Network Operators and Service Providers should implement dedicated trunk groups between the Mobile Switching Center (MSC) end office or similar source and the E9-1-1 Selective Router (SR), based on the geography served by the default Public Safety Answering Points (PSAPs). This should be done rather than aggregating traffic from centralized switching architectures serving wide spread geographic areas onto a single trunk group to the E9-1-1 Selective Router. This should be done in conjunction with the local PSAP jurisdictional authorities to ensure that correct choices are made.			Best Practice					
	9-9-3225 (Free)	Mobile Positioning Center (MPC) Capacity Reserve	Network Operators and Service Providers that deploy geographically diverse 911 Mobile Positioning Centers (MPC) with dual load sharing nodes should ensure that the utilization on either node is less than half of each node's capacity so that if one node fails the other node will absorb the load.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	9-9-3226 (Free)	MPC 911 Network Operations Support	Network Operators and Service Providers operating Mobile Positioning Centers (MPC) should provide 24x7 network operations support			Best Practice					
	9-9-3227 (Free)	911 Voice traffic and Location Data Concurrency	Network Operators, Service Providers and Equipment Suppliers should deploy location solutions such that the E911 related data traffic between the Position Determining Entity (PDE) and the mobile subscriber associated with location determination should not interfere with the voice traffic, when feasible.			Best Practice					
NRIC	9-9-3228 (Free)	Global Positioning System (GPS) Location accuracy for E9-1-1	Network Operators, Service Providers and Equipment Suppliers that use Global Positioning System (GPS)-enabled Phase II location solutions should ensure that the GPS satellite location information (e.g., GPS ephemeris, almanac, etc.) is as current as is feasible to assist the handset in providing improved accuracy of the GPS fix, aiding in the reduction of the time of database responses and reduction of the number of database query rebids.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	9-9-3229 (Free)	911 Performance Statistics and Logging	Network Operators and Service Providers that operate Mobile Positioning Centers (MPC)/ Gateway Mobile Location Centers (GMLC) should maintain local storage of record logs for a minimum of 7 days showing incoming successful requests from Emergency Services Message Entity (ESME) and outgoing responses to ESME.			Best Practice					
NRIC	9-9-3231 (Free)	Satellite Location Identification information Transfer Delay	Network Operators and Service Providers that use Global Positioning System (GPS) enabled Phase II location solutions should ensure that the GPS satellite location identification information (e.g., GPS ephemeris, almanac, etc.) is transmitted to the Phase II Mobile Subscriber or Position Determining Entities (PDE) as soon as is feasible after the E9-1-1 call commences in order to reduce the number of database query rebids.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	9-7-3232 (Free)	Handsets that use a GPS algorithm for E9-1-1	Equipment Suppliers should ensure that the Phase II handsets commence Global Positioning System (GPS) acquisition before the GPS satellite location identification information is received so that GPS acquisition time is minimized and to reduce the number of database query rebids.			Best Practice					
	9-9-3233 (Free)	E9-1-1 Phase II Accuracy Optimization Reporting and Resolution Process	Service Providers deploying wireless Phase II should work to ensure that Phase II accuracy is optimized and the performance trouble resolution process is followed as needed.			Best Practice					
NRIC	9-9-0567 (Free)	Unnamed	Network operators and service providers (of any technology type) should spread 911 access connections across similar equipment to avoid single points of failure.			Best Practice					
	9-9-0569 (Free)	Unnamed	In E9-1-1, the PSTN may be used as a backup to dedicated trunks. Two implementation options exist. This best practice discusses both options.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NRIC	9-9-0574 (Free)	Unnamed	Network operators and service providers (of any technology type) should remotely monitor and manage the 911 network components using network management controls, where available, to quickly restore 911 service and provide priority repair during network failure events.			Best Practice					
	9-9-0900 (Free)	Unnamed	Routing errors are encountered when a VPC or MPC/GMLC operator sends bad shell record data (pseudo automatic number identification [pANI]-to-emergency service number [ESN] relationship) to the E9-1-1 SSP for entry into the routing database. These errors result from an incorrect MSAG-to-ESN-to-PSAP relationship. To avoid such errors, the VPC should follow the recommendations in NENA 56-504, NENA VoIP 911 Deployment and Operational Guidelines (see Testing in Section 5.1.4), to fully test the routing for every pANI placed in service.			Best Practice					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	9-9-3224 (Free)	Unnamed	Network operators and service providers (of any technology type) should use dedicated signaling system 7 (SS7) or multi-frequency (MF) controlled trunk groups for the normal routing of E9-1-1 calls from originating switching entities to E9-1-1 SRs rather than using shared PSTN trunking.			Best Practice					
	CIP-002-3 (Free)	Cyber Security - Critical Cyber Asset Identification	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3 December 2009	Operational Standard		X	X	X	X
NRIC	CIP-003-3 (Free)	Cyber Security - Security Management Controls	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3 November 2013	Operational Standard		X	X	X	X
	CIP-004-3a (Free)	Cyber Security - Personnel & Training	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3a May 2012	Operational Standard		X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NRIC	CIP-005-3a (Free)	Cyber Security - Electronic Security Perimeter(s)	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3a November 2013	Operational Standard		X	X	X	X
	CIP-006-3d (Free)	Cyber Security - Physical Security of Critical Cyber Assets	NERC Standards CIP-002-3 through CIP-009-3 provides a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3d/4d March 2013	Operational Standard		X	X	X	X
	CIP-007-3a (Free)	Cyber Security - Systems Security Management	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3a November 2013	Operational Standard		X	X	X	X
NRIC	CIP-008-3 (Free)	Cyber Security - Incident Reporting and Response Planning	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3 December 2009	Operational Standard		X	X	X	X

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
NERC	CIP-009-3 (Free)	Cyber Security - Recovery Plans for Critical Cyber Assets	NERC Standards CIP-002-3 through CIP-009-3 provides a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.		Version 3 December 2009	Operational Standard		X	X	X	X
	OASIS CAP (Free)	Common Alerting Protocol	Defines and describes CAP, which provides an open, non-proprietary digital message format for all types of alerts and notifications.		Version 1.2 July 2010	Technical Standard					
NERC	OASIS EDXL-HAVE (Free)	Emergency Data Exchange Language Hospital AVailability Exchange (EDXL-HAVE)	Defines and describes EDXL-HAVE which specifies an XML document format that allows the communication of the status of a hospital, its services and resources.		Version 1.0 December 2009	Technical Standard					
	OASIS EDXL-SitRep (Free)	Emergency Data Exchange Language Situation Reporting (EDXL-SitRep)	Defines and describes EDXL-SitRep which specifies standard formats for XML emergency response messages aimed at transmitting timely situation reports. Designed as payloads of the EDXL-DE.		Version 1.0 April 2013	*Technical Standard*					
	OASIS EDXL-DE (Free)	Emergency Data Exchange Language Distribution Element (EDXL-DE)	Defines and describes EDXL-DE, which is used to facilitate the routing of any properly formatted XML emergency message to recipients.		Version 1.0 May 2006	Technical Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	OASIS EDXL-RM (Free)	Emergency Data Exchange Language Resource Messaging (EDXL-RM)	Defines and describes EDXL-RM, which provides a set of standard formats for XML emergency response messages.		Version 1.0 December 2009	Technical Standard					
NERC	OASIS EDXL-TEC (Free)	Emergency Data Exchange Language - Tracking of Emergency Clients (EDXL-TEC)	Defines and describes EDXL-TEC which enables automated data exchange between disparate systems which support various emergency and disaster preparedness, mitigation, response and recovery processes.		Version 1.0 June 2014	Technical Standard					
	OGC 06-042 (Free)	OpenGIS® Web Map Server (WMS) Implementation Specification	Provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases.		Version 1.3.0 March 2006	Technical Standard					
OASIS	OGC 06-121r9 (Free)	OGC Web Service Common Standard	Specifies many of the aspects that are, or should be, common to all or multiple OWS interface Implementation Standards. Those specifications currently include the Web Map Service (WMS), Web Feature Service (WFS), and Web Coverage Service (WCS).		Version 2.0 April 2010	Technical Standard					
	OGC 07-006r1 (Free)	OpenGIS® Catalogue Services Specification	Specifies the interfaces, bindings, and a framework for defining application profiles required to public and access catalogues of metadata for geospatial data, services, and related resource information.		Version 2.0.2 February 2007	Technical Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	OGC 07-36 (Free)	OpenGIS® Geography Markup Language (GML) Encoding Standard	GML defines an XML data encoding for geographic data and a grammar to express models of such data using XML Schema. GML is the standard that enables information communities and other standards organizations to insert geospatial elements into their standards and be confident that their standards will be compatible with mainstream information infrastructure methods of conveying spatial/temporal information.		Version 3.2.1 August 2007	Technical Standard					
OASIS	OGC 07-074 (Free)	OpenGIS® Open Location Services Interface Standard (OpenLS)	Specifies interfaces that enable companies in the Location Based Services (LBS) value chain to "hook up" and provide their pieces of applications such as emergency response (E911, for example), personal navigator, traffic information service, proximity service, location recall, mobile field service, travel directions, restaurant finder, corporate asset locator, concierge, routing, vector map portrayal and interaction, friend finder, and geography voice-graphics.		Version 1.2 September 2008	Technical Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	OGC 07-147r2 (Free)	OGC KML (formally Keyhole Markup Language)	KML is an XML language focused on geographic visualization, including annotation of maps and images. Geographic visualization includes not only the presentation of graphical data on the globe, but also the control of the user's navigation in the sense of where to go and where to look.		Version 2.2 April 2008	Technical Standard					
	OGC 08-007r1 (Free)	OpenGIS® City Geography Markup Language (CityGML) Encoding Standard	CityGML is an open data model and XML-based format for the storage and exchange of virtual 3D city models.		Version 1.0 August 2008	Technical Standard					
OGC	OGC 09-025r2 (Free)	Web Feature Service	The Web Feature Service (WFS) represents a change in the way geographic information is created, modified and exchanged on the Internet. Rather than sharing geographic information at the file level using File Transfer Protocol (FTP), for example, the WFS offers direct fine-grained access to geographic information at the feature and feature property level.		Version 2.0.2July 2014	Technical Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	OGC 09-083r3 (Free)	GeoAPI Implementation Specification	The GeoAPI Implementation Standard defines, through the GeoAPI library, a Java language application programming interface (API) including a set of types and methods which can be used for the manipulation of geographic information structured following the specifications adopted by the Technical Committee 211 of the International Organization for Standardization (ISO) and by the Open Geospatial Consortium (OGC).		Version 3.0.0 April 2011	Technical Standard					
OGC	OGC 11-030r1 (Free)	Open GeoSMS Standard—Core	Provides developers with an extended Short Message Service (SMS) encoding and interface to facilitate communication of location content between different location based services (LBS) devices or applications.		Version 1.0 January 2012	Technical Standard					
	OGC 12-019 (Free)	OGC City Geography Markup Language (CityGML) Encoding Standard	Encoding standard for the representation, storage and exchange of virtual 3D city and landscape models. CityGML is implemented as an application schema of the Geography Markup Language version 3.1.1 (GML3).		Version 2.0 April 2012	Technical Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
OGC	OMA-ERELD-SUPL-V3_0-20140916-C (Free)	Enabler Release Definition for Secure User Plane Location (SUPL)	Outlines the Enabler Release Definition for SUPL Enabler and the respective conformance requirements for clients and servers implementing claiming compliance to it as defined by OMA across the specification baseline.		Candidate Version 3.0 September 2014	Technical Standard		X	X		
	OMA-ERELD-LPPe-V2_0-20141202-C (Free)	Enabler Release Definition for LPP Extensions (LPPe)	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.		Candidate Version 2.0 December 2014	Technical Standard		X	X		
	OMA-LIF-MLP-V3_1-20110920-A (Free)	Mobile Location Protocol (MLP)	Identifies the MLP, an application-level protocol for getting the position of mobile stations independent of underlying network technology.		Approved Version 3.1 September 2011	Technical Standard		X	X		
OGC	OMA-ERELD-LOCSIP-V1_0-20100803-C (Free)	Enabler Release Definition for Location in SIP/IP Core	The Location Service in SIP/IP core network (LOCSIP) provides mechanisms to expose location information to Location Clients that reside in terminals or in Application Servers connected to a SIP/IP core network.		Candidate Version 1.0 August 2010	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	ANSI/SCTE 24-1 2009 (Free)	IPCablecom 1.0 Part 1: Architectural Framework for the Delivery of Time Critical Services Over Cable Television Networks Using Cable Modems	This document 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.	IPCablecom Series	2009	Technical			X		
	ANSI/SCTE 24-2 2009 (Free)	IPCablecom 1.0 Part 2: Audio Codec Requirements for the Provision of Bi-directional Audio Service Over Cable Television Networks Using Cable Modems	This standard specifies the audio (voice) codes that are to be used in the provisioning of bi-directional audio services over cable television distribution networks using IP technology (i.e., IPCablecom service). The standard also addresses codec options and packetization issues. Specifically, it identifies the audiocodecs necessary to provide the highest quality and the most resource-efficient service delivery to the customer. Additionally, this document describes a suggested methodology for optimal network support for codecs.	IPCablecom Series	2009	Technical			X		
OGC	ANSI/SCTE 24-3 2009 (Free)	IPCablecom Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems	This document describes the NCS profile of an application programming interface (MGCI) and a corresponding protocol (MGCP) for controlling embedded clients from external call control elements.	IPCablecom Series	2009	Technical			X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
OMA	ANSI/SCTE 24-4 2009 (Free)	IPCablecom 1.0 Part 4: Dynamic Quality of Service for the Provision of Real-Time Services over Cable Television Networks Using Data Modems	This specification describes a dynamic Quality-of-Service (QoS) mechanism for the IPCablecom project. It was issued this specification to facilitate design and field-testing leading to the manufacture and interoperability of conforming hardware and software by multiple vendors.	IPCablecom Series	2009	Technical			X		
	ANSI/SCTE 24-21 2012 (Free)	BV16 Speech Codec Specification for Voice over IP Applications in Cable Telephony	This document contains the description of the BV16 speech codec1. BV16 compresses 8 kHz sampled narrowband speech to a bit rate of 16 kb/s by employing a speech coding algorithm called Two-Stage Noise Feedback Coding (TSNFC), developed by Broadcom.	IPCablecom Series	2012	Technical			X		
	ANSI/SCTE 24-22 2013 (Free)	iLBCv2.0 Speech Codec Specification for Voice over IP Applications in Cable Telephony	This document contains the description of an algorithm for coding of speech signals sampled at 8 kHz. The algorithm, called iLBC, uses a block-independent linear-predictive coding (LPC) algorithm and has support for two basic frame lengths: 20 ms at 15.2 kb/s (kilobits per second) and 30 ms at 13.33 kb/s.	IPCablecom Series	2013	Technical			X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
OMA	ANSI/SCTE 24-23 2012 (Free)	BV32 Speech Codec Specification for Voice over IP Applications in Cable Telephony	This document contains the description of the BV32 speech codec1. BV32 compresses 16 kHz sampled wideband speech to a bit rate of 32 kb/s (kilobits per second) by employing a speech coding algorithm called Two-Stage Noise Feedback Coding (TSNFC), developed by Broadcom.	IPCablecom Series	2012	Technical			X		
SCTE	ANSI/SCTE 165-12 2009 (Free)	IPCablecom 1.5 Part 12: PSTN Gateway Call Signaling Protocol	This document is part of the IPCablecom suite of specifications. The document is based on MGCP 1.0 [1], an IETF Informational RFC.	IPCablecom Series	2009	Technical			X		
	SR-4163 (Fee/Charge)	E9-1-1 Service Description	Describes the telecommunications network and its associated network elements and features needed to provide E911 service. It also describes capabilities of the PSAP, typically provided through the PSAP's CPE, that interact with network elements (e.g., E911 tandem).		Issue 2 May 1997	Technical Information Document		X	X		
SCTE	TIA-1057 (Fee/Charge)	Telecommunications—IP Telephony Infrastructure—Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED)	Defines/describes extensions to the IEEE 802.1AB protocol requirements (including device location for Emergency Call Service/E911) that support VoIP equipment in IEEE 802-based LAN environments.	ANSI/TIA-1057	Revision 6 August 2011	Technical Standard (Product/ Design)	X	X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	TIA TSB-146 (Fee/Charge)	Telecommunications—IP Telephony Infrastructures—IP Telephony Support for Emergency Calling Service	This TSB covers issues associated with support of ECS from IP Telephony terminals connected to an Enterprise Network (EN). It describes new network architecture elements needed to support ECS, and the functionality of those new elements.		Revision A November 2012	Technical Standard		X	X		
	TIA/EIA/IS-834 (Free)	G3G CDMA-DS to ANSI/TIA/EIA-41	Provides general requirements and detailed Upper Layers (Layer 3) signaling radio protocols and procedures for the DS-41 radio interface.		March 2000	Technical Standard		X	X		

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
SCTE	TIA-102.BAEA (Fee/Charge)	Project 25—Data Overview and Specification	Provides an overview of the standardized set of data communication services such that data connectivity will operate in accordance with any Project 25 radio and across any Project 25 digital radio system. The document describes circuit and packet data. Additionally, the description serves the requirement to transport multiple packet protocols, including TCP/IP, X.25 and SNA. The APCO 25 system defines 2 different categories of data services in 3 different categories of data configurations for a total of 6 distinct service/configuration combinations. This document does not include a multipoint interface, or low speed data, which is data embedded in voice.	TIA-102	Revision B June 2012	Technical Standard		X	X		
	TIA-102.BAED (Fee/Charge)	Project 25 Packet Data Logical Link Control Procedures	Specifies the Logical Link Control (LLC) procedures that permit the conveyance of Common Air Interface (CAI) data packets between air interface endpoints for all packet data configurations.	TIA-102	Revision 13 September 2013	Procedural Standard					

SDO	Standard ID	Standard Title	Standard Description	Associated Standards	Latest Revision/ Release Date	Standard Type	Relation to NENA i3 Architecture				
							Client	Access Networks	Origination Networks	ESInets	PSAPs
	J-STD-110 (Fee/Charge)	Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification	Defines the requirements, architecture and procedures for text messaging to 911 emergency services using native wireless operator SMS capabilities for the existing generation and next generation (NG911) Public Safety Answering Points.	J-STD-110.01	March 2013	Joint Standard					X
Telcordia (Now part of Ericsson)	J-STD-110.01 (Fee/Charge)	Joint ATIS/TIA Implementation Guideline for J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification	These implementation guidelines address Commercial Mobile Service Providers (CMSPs) and Text Control Center (TCC) provider deployment considerations of J-STD-110.	J-STD-110	November 2013	Joint Standard					X
TIA	J-STD-110.a (Fee/Charge)	Joint ATIS/TIA Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification	The purpose of this Supplement is to provide errata and clarifications to J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification.	J-STD-110	November 2013	Joint Standard					X

Appendix B: 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 Cable Labs	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 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 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 LSRG was the same as the 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 will be documented in an approved update of the NENA 08-003 (i3) architecture standard. Priority 2	Call routing partially addressed in **NENA 08-003**, Version 1, page 124 (NENA 08-003, Version 2 is in development and could address these gaps)
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	Possibly 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. Priority 2	**RFC 5985 (September 2010)** defines and describes a XML-based protocol that can be used to acquire device location information from a Location Information Server (LIS) within access networks employing both wired technology (DSL, cable) and wireless technology

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Third party Originating Service Providers (e.g., OnStar, Relay services)	NENA 08-003 IETF, TIA	Some are proprietary, but they must comply with ESInet interfaces using a standard public interface Priority 1	Still needs to be addressed (NENA 08-003, Version 2 is in development and could address these gaps)
Legacy Origination Networks	Legacy selective router Legacy network gateway NENA 08-003 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. This method has been resolved and will be documented in an approved update of the NENA 08-003 (i3) architecture standard. Priority 1	Call routing partially addressed in **NENA 08-003**, Version 1, page 204 (NENA 08-003, Version 2 is in development and could address these gaps)
Femto Cell	NENA 03-509 v1	Specification needs to be updated for NG911 Priority 3	Still needs to be addressed
ESInet			
IP network	NENA 08-003	Testing, Operations Priority 1	Operations partially addressed in **NENA 08-003**, Version 1, page 44 (NENA 08-003, Version 2 is in development and could address these gaps)
Core functions (DNS, DHCP, …)	IETF	None	N/A
Interconnect with other ESInet	NENA 08-003	Testing, Operations Priority 1	(NENA 08-003, Version 2 is in development and could address these gaps)
Interconnect with origination networks	NENA 08-003, IETF RFC 6881	Testing, Operations Priority 1	(NENA 08-003, Version 2 is in development and could address these gaps)
Interconnect with access networks	NENA 08-003, IETF RFC 6881	Testing, Operations Priority 1	(NENA 08-003, Version 2 is in development and could address these gaps)

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
ESInet to PSAP interface	NENA 08-003	Testing, Operations Priority 1	Still needs to be addressed (NENA 08-003, Version 2 is in development and could address these gaps)
Interconnection with other emergency service entities	NENA 08-003, other NENA and APCO standards in development	Testing, Operations Priority 1	Still needs to be addressed (NENA 08-003, Version 2 is in development and could address these gaps)
Management		NENA work in development Priority 2	Mentions a technical standard is to be determined and will be developed as a guide for PSAP staff and policy makers to evaluate and consider the opportunities and challenges presented with the Next Generation 911 systems as they relate to personnel and PSAP management
Location	3GPP ATIS IMS ESInet IETF NENA		
PIDF-LO - the location interchange format	IETF 4119	IMS and IETF/NENA location format incompatibilities Priority 1	Still needs to be addressed
Functional definition of Location Information Server (and similar terms)	NENA 08-003	None	N/A
IP Based Emergency Services	NENA 08-505	Initial version is incomplete. Future revisions of document are required. Priority 2	**NENA 08-505** (December 2006) acknowledges the first edition of what will be a comprehensive document addressing many access network configurations. This edition

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
			has a narrow solutions focus and addresses only the automated mechanism for the residential broadband market
Location Configuration Protocols		IMS OTT issues Priority 2	Still needs to be addressed
Location Dereferencing Protocols	IETF RFC 6753	Depends on results of ATIS IMS ESInet work Priority 2	Still needs to be addressed
Location Query Protocols (to the extent we decide they are different from LCPs)		Pending other work	N/A
Location Validation	IETF 5222, IETF5223	None	N/A
Interwork to existing location sources, such as ALI	NENA LSRG	None	N/A
GIS & 9-1-1 Attribute Data			
Address, political boundary, and service boundary layer	NENA GIS V3	None	N/A
Service boundary polygons – how we route	NENA GIS V3, NENA 08-003	None	N/A (NENA 08-003, Version 2 is in development)
Data management, quality assurance	NENA	Further work needed Priority 2	Still needs to be addressed
Distribution – how does it get from GIS to everything else	NENA 08-003, OGC	OGC work needs further standardization Priority 1	Still needs to be addressed (NENA 08-003, Version 2 is in development)
Adjustment of street/address layer to polygon layer	NENA ECRF/LVF	Further work needed Priority 1	Addressed in **NENA 08-003**, Version 1, page 146 (NENA 08-003, Version 2 is in development and could address these gaps)
Call Signaling			
Basic SIP call signaling	IETF 3261, IETF RFC 6881	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
IMS SIP call signaling	3GPP	IMS ESINET identified some gaps Priority 1	Still needs to be addressed
Call Routing			
Routing database (ECRF)	IETF 5222, 5223 NENA 08-003	None	N/A (NENA 08-003, Version 2 is in development)
Routing proxies (ESRP)	IETF 3261, RFC 6881 & NENA 08-003	None	N/A (NENA 08-003, Version 2 is in development)
Policy based routing	NENA 08-003	None	N/A (NENA 08-003, Version 2 is in development)
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
RTT, IMS MMES, "total conversation"	3GPP, IETF, NENA	None	N/A
Accessibility			
EAAC issues & gaps in i3	FCC EAAC ATIS INES Incubator FCC NG9-1-1 NPRM	Identify the TTY replacement technology, Adoption of that technology, method of delivering TTY replacement to the NG911 and PSAP Output of FCC NG9-1-1 NPRM may identify additional gaps Priority 1	Still needs to be addressed The FCC EAAC Report lists some of the gaps, and makes recommendations to fill some of these gaps.
Interface between IMS-originating networks and relay services	FCC EAAC ATIS	How do calls originating from IMS connect to the relay service. Also, given that 911 calls originating on IMS are direct to ESINet, how do the responders get notification that a relay service needs to be involved? Need to have	Still needs to be addressed

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
		specification developed to define how IMS interfaces with Relay Service. Priority 1	
Callback	3GPP, IETF, NENA		
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. Priority 1 (generally)	**NENA 71-001** describes the use of additional data available with NG911 (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 Emergency Information Data Document (EIDD) Specification (NENA 71-001, Version 2 is in development and could address these gaps)
Call	NENA 08-003, 70-001 IETF additional data, 3GPP ATIS IMS ESInet	None	N/A (NENA 08-003, Version 2 is in development)
Caller	NENA 08-003, 70-001 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 NG911 (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 Emergency Information Data Document (EIDD) Specification (NENA 71-001, Version 2 and NENA 08-003 are in development and could address these gaps)

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Premise (e.g. floor plans, alarm data, etc.)	NENA 08-003, 71-001 NIST	Further work needed Priority 3	Partially addressed by **NENA 71-001,** version 1, page 28 (NENA 71-001, Version 2 and NENA 08-003 are in development and could address these gaps)
PSAP	APCO, NENA, EIDD	Further NIEM work needed Priority 1	Still needs to be addressed
Logging			
Within the ESInet and related functions	NENA 08-003	NENA and APCO have identified a number gaps such as Radio over IP Priority 2	Still needs to be addressed (NENA 08-003, Version 2 is in development)
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. Priority 2	Still needs to be addressed
Security			
Credentials	3GPP, IETF, NENA ATIS IMS ESInet NIST	None	N/A
Securing Protocol Interaction including authentication, integrity protection, privacy	IETF, NENA 08-003 ATIS IMS ESInet NIST	None	N/A (NENA 08-003, Version 2 is in development)
Attack Mitigation	NENA 08-003 NIST	None	(NENA 08-003, Version 2 is in development)
End User Location Integrity	IETF ATIS IMS ESInet	Standards in development Priority 3	Still needs to be addressed
Transition (including data)			
Wireline	NENA	None	N/A
Wireless	NENA	None	N/A
VoIP	NENA	None	N/A
PSAP aspects	NENA ATIS RFAI	None	N/A

Process	Applicable Standards	Identified Gaps	Gap Addressed in Standards Document?
Relay services (e.g., IP relay, Video relay, etc.)	NENA	None	N/A
TTY	NENA	None	N/A
Legacy PSAP	NENA	None	N/A
		Several gaps associated with Testing Priority 1	**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
Testing			
Self-test	IETF, NENA	None	N/A
Discrepancy Reporting	NENA		
Data Management & Maintenance	NENA	In development	