iCERT
Industry Council for Emergency Response Technologies

The Critical Role of Testing to Achieve and Maintain NG911 Standards Conformance and Interoperability

iCERT Conformance Working Group
www.theindustrycouncil.org
October 2019

Foreword

Now more than ever, the world's citizens need the technologies and innovation embodied in the emergency response technology, software, and communications industries. Since 2005, the Industry Council for Emergency Response Technologies, Inc. (iCERT) has represented the interests of emergency response technology hardware, software, and services providers through effective advocacy and education and by creating a forum for industry leaders to work together to promote innovative solutions for public safety.

One of the ways iCERT accomplishes this is through cooperative member-driven efforts, such as this paper, which capture leading edge experiences and best practices that provide both educational and practical benefits to readers and practitioners. iCERT members know that history has repeatedly proven business leaders' expertise can assist public policymakers and government emergency communications professionals as they address complex choices regarding the installation, use, and maintenance of advanced communications, public safety, and related technologies.

On behalf of iCERT's members and the emergency response technology industry, thank you for reviewing this information We hope that it is of benefit. Comments and questions are always welcome. Thank you.

Kim Robert Scovill, Esq.
Executive Director
iCERT

To learn more, or to join iCERT, go to www.theindustrycouncil.org.
To contact iCERT, executivedirector@theindustrycouncil.org

Table of Contents

Contributors

Name	Working Group Role	Company
Ray Paddock	Chair	Inteliquent
Al Brisard	Vice-Chair	Exacom
Jared Hertzler	Member	Comtech
Michael Hooker	Member	T-Mobile
Elisabeth Madden	Member	Winbourne Consulting
Christian Militeau	Member	Intrado
Jackie Milnes	Member	Mission Critical Partners
Henry Unger	Member	Pulsiam
Jeff Wittek	Member	Motorola

Objective

Next Generation 911 (NG911) is no longer a dream but quickly becoming a reality. Governmental bodies, standards bodies, service providers, and vendors are all moving to implement NG911. While there are several opinions for how this will occur, all agree that significant testing is required to ensure all the elements within an NG911 system and between NG911 systems, work together as intended. But exactly what testing is necessary? What testing is required to ensure a sufficient level of confidence by the public safety community in the solutions being deployed? iCERT has developed this white paper to answer these and similar questions. The objectives of this white paper are to:

1. Highlight the role of standards in NG911 testing;

2. Define the types of testing that should be considered; and

3. Identify the challenges of Interoperability testing.

NG911 Environment

The migration from E911 to NG911 has been led by early adopters comprised of thought leaders capable of identifying adequate funding to support the transition while leveraging a governance body with the authority and foresight to drive the migration. However, for many State, County and Regional 911 Authorities across the country, concerns over operational issues, such as interoperability with neighboring jurisdictions, have slowed the migration to NG911, and restricted its deployment to isolated pockets across the country.

It is generally agreed that NG911 services will ultimately bring tremendous improvements in 911 service delivery functionality and will provide a more resilient and reliable system for the public and emergency responders. Among the many benefits of NG911 will be the capacity for increased data sharing from the 911 caller to the Public Safety Answering Point (PSAP), otherwise referred to as Emergency Communications Center (ECC),[1] to First Responders, between First Responders and, when necessary, data sharing among neighboring jurisdictions.

As the transition to NG911 expands, states, counties and municipalities require the ability to interoperate with 911 services in neighboring states and across jurisdictional boundaries. This will directly benefit citizens because it enables more accurate call routing, faster and more efficient rerouting and transfer of misrouted calls, and increased collaboration between 911 centers.

[1] As the transition to NG911 occurs, PSAPs are increasingly being referred to as Emergency Communications Centers (ECCs) in recognition of their expanded role in the NG911 environment. The term ECC is used interchangeably with PSAP throughout this document.

Jurisdictions must be confident that they will not lose any functionality they have now, albeit limited, with regard to communicating, transferring, or receiving calls from neighboring PSAPs or ECCs. They need to be confident that they can transfer the 911 voice call, as they do today, and transfer any additional data, such as Computer Aided Dispatch (CAD) data, notes, detailed location data, and text messages. The continued migration to NG911 depends on addressing these and other challenges and leveraging standards to accelerate the interoperability.

Standards

NG911 standards have been developed over more than a decade through the collaborative efforts of the National Emergency Number Association (NENA), the Association of Public-Safety Communications Officials International (APCO), and numerous industry groups and professionals, and are codified as *NENA Detailed Functional and Interface Standards for the NENA i3 Solution*, enumerated as NENA STA-010 (i3). Version 3 of this standard is intended to become an American National Standards Institute (ANSI) standard. The expectation is that this will happen sometime in 2020. In addition, there are many other standards that are relevant to the current 911 industry and will continue to be relevant to NG911. Some of these are consensus standards and are not limited to those developed by NENA.

There are five (5) major components of a NG911 system as defined in NENA STA-010 (i3):

1) The Emergency Services Internet Protocol (IP) network (ESInet);
2) Next Generation 911 Core services (NGCS);
3) Call Handling Equipment (CHE);
4) Geospatial Information Systems (GIS); and
5) Management Information Systems (MIS).

Of these components, only the first three are involved in 911 call processing and are the primary focus of this white paper. The last two are important but relate to supportive systems and are not addressed in this paper.

While many interfaces in a NG911 system are defined in the i3 specification, there are several in use by 911 Authorities[2] that have proprietary internal interfaces supporting backward compatibility with legacy systems such as: CHE, CAD, mapping, and emergency medical dispatch (EMD) systems.

[2] According to 911.gov, 911 Authority is defined as: Entity that is ultimately responsible for the geographic planning, coordination, and funding of 911 environments. Authorities could be state agencies, regional entities, federal entities, or even individual PSAPs (particularly in states that operate under a single statewide system and PSAP).

Other examples are interfaces for proprietary external communications systems used by individuals and businesses, such as legacy Private Branch Exchanges (PBX), paging and alerting systems.

While proprietary interfaces to new products and services should be avoided, testing and support for legacy proprietary interfaces should be considered. Legacy systems will continue to exist for some period so proprietary interfaces will likewise have to be supported.

Current Testing Approaches

NENA Industry Collaboration Events

Participation in NENA's confidential Industry Collaboration Events (ICE),[3] held periodically since November 2009, has included many vendors offering NG911 products and services. They have focused exclusively on collaborative testing of the interfaces defined in the NENA i3 specifications. The results of these events have been used by the participating NG911 vendors to evaluate their interpretation and implementation of the interfaces tested. By agreement of the parties, results have not been made available to 911 Authorities, and vendors are restricted in what they can disclose. It is important to note that, to date, Originating Service Providers (OSPs) have not been represented at ICE.

Other Testing Approaches

In addition to participating in ICE, some vendors of NG911 products and services have invested heavily in self-testing programs. Vendors offering a complete NG911 package unilaterally test the interoperability of their own NG911 components. Some vendors also conduct testing with other vendors, including competitors where the market has indicated a demand or requirement. Most vendors offer only a subset of an end-to-end NG911 system and as such, out of necessity, conduct testing with other vendors. The cadence of testing is often driven by new standards, a new NG911 component (or a new version of an NG911 component), market expectations or a customer requiring a demonstration of interoperability. It is, for the most part, voluntary.

[3] https://www.nena.org/page/NG911_ICE

Testing Challenges

The current testing approaches, as described above, vary in the breadth and depth based on the components tested. While these collaborative testing methods are useful, they also come with challenges:

- Inconsistency across vendors regarding their adoption of Life-Cycle Testing;
- Regular, and sometimes necessary, evolution of the underlying standards;
- Costs in creating a robust test environment;
- Misalignment of different vendor roadmaps; and
- Coordinating and resourcing vendor to vendor testing.

Implementing to a Standard – the Reality

Standards are extremely important when trying to focus many players within an industry on a common objective. However, it is impractical to believe that if every vendor implements to a "standard", every system will work as intended and all systems will work together. While standards are a vital industry foundation, they alone do not ensure a successful implementation.

It is virtually impossible to define a standard in enough detail that it eliminates some need for interpretation. In fact, two companies can look at a line item requirement in the same standard and both interpret it differently. In some cases, both implementations can still deliver the intended result, but in other cases they do not. If you consider the plentitude of vendors implementing to a standard, compounded by the complexity and extent of that standard, the probability for multiple variations throughout the development and implementation process is high.

Another nuance regarding the efficacy of a standard is that its usefulness often depends on how extensive a standard is and the breadth it attempts to address. Often not all aspects of a standard are applicable to every system, subsystem, component, or element that has been implemented in a system that uses the standard as a guide. In these cases, the respective vendor only implements the items believed to be relevant. This is expected. However, when there are multiple vendors delivering solutions representing the same functional system, subsystem, component, or element, and those vendors are not in agreement on what is relevant and what is not, interoperability with upstream or downstream elements may be challenging.

As this paper explores testing relative to NG911, understanding these two considerations is highly significant in appreciating the complexities and efforts required to achieving standards conformance, ongoing compliance, and interoperability.

Evolving NG911 Environment

While voice calls initiated by a human dialing “911” are the most common 911-initiated requests for assistance today, the volume of alerts or requests for assistance generated by non-traditional means, such as Internet of Things (IoT) devices, is anticipated to grow rapidly over time. Therefore, the interface between IoT and NG911 systems is and will become even more important as NG911 implementation progresses.

Standards for a data sharing interface between NG911 CHEs and between other systems such as CAD are under development. The Emergency Incident Data Object (EIDO) Standard, as currently under development by NENA, is the data format that will be used for sharing information between the Call Handling System and CAD as well as other authorized entities that are involved in handling emergency situations. These entities may include hospital emergency rooms, hazardous materials (HAZMAT) personnel, First Responders, and other entities that are not in the direct call path of a 911 call but could benefit from having access to incident information.

OSPs continue to transition commercial voice and messaging services away from legacy circuit switched networks and towards IP based networks such as 3GPP-defined IP Multimedia Subsystem (IMS) networks that support multimedia telephony service (MMTel) and offer real-time multimedia communication services such as High Definition (HD) voice, real-time video, real-time text (RTT), rich communications services (RCS) and file sharing. As a result of this transition, the number of emergency calls originating from IMS-based networks will continue to increase. As NG911 networks mature to support Session Initiated Protocol (SIP)-based Network-to-Network Interfaces (NNIs), it may be prudent to include ingress of emergency calls to and egress from NG911 systems in any NG911 testing regimen to ensure successful negotiation of media capability with NG911 PSAP, or ECC, endpoints and for backwards compatibility to Legacy PSAPs limited to voice and TTY.

Broadband wireless networks open a wide range of possibilities for sending information to First Responders and other pertinent public safety personnel. The architecture defining the interface between a NG911 system and broadband wireless systems has not yet been defined in detail but will provide several opportunities to provide information egressing from NG911 systems. Consideration should be given to including the egress of information to other downstream systems in any NG911 testing regime.

Multimedia adoption by citizens and First Responders has started but will become more prevalent over time. This includes data from bodycams, surveillance video, citizen provided media (audio, text, video, and photos), and other sources of media. Incorporating and leveraging these types of media more effectively to improve public safety and emergency response has begun. New media types will require new testing regimens.

Types of Testing

In the communications networking space, there are generally accepted levels or types of testing used to ensure initial conformance through ongoing compliance. The five key types of testing are:

1) **Conformance Testing** - the testing of a vendor system, subsystem, component, or element against a promulgated/published standard. This type of testing requires a known working standard implementation as the "reference implementation," and formalized test plans specific to a system, subsystem, component, or element. This testing is typically done in a lab environment by an independent third party. Vendors can perform testing without coordinating with other vendors.

2) **Interoperability Testing** - the testing of the functional interaction of two or more systems, subsystems, components or elements at the point/method of interconnection. This type of testing is typically done on a cooperative basis by vendors supplying a system, subsystem, component or element that must interact with each other seamlessly. This effort is usually done in the lab of one of the vendors and sometimes done over a site-to-site VPN[4]. In some cases, this can also be done in a lab by an independent third party, but this option generally costs more. Many times, this testing is done because the participating vendors are business partners and routinely collaborate preparing proposals in response to RFPs.[5] Sometimes the testing is done at the request of a customer or customers.

3) **End-to-End Testing** - testing of all systems, subsystems, components or elements comprising a complete system or solution. This testing is almost always done in the customer environment and typically at the time of turn-up of the heterogeneous system. Some large customers have lab environments established to support this type of testing. Most customers, however, depend on the vendors to set up the test environment.

4) **Performance Testing** - testing of systems, subsystems, components or elements to determine responsiveness and stability under actual or simulated load to validate other attributes such as resource utilization, availability or resiliency. This testing is typically done in a testing lab by the vendor of the system, subsystem, component or element. Since a real-world deployment is impossible to duplicate in a lab, this type of testing has some risk. Very large 911 systems supporting the largest metropolitan areas in the country are particularly interested in testing the performance of a system.

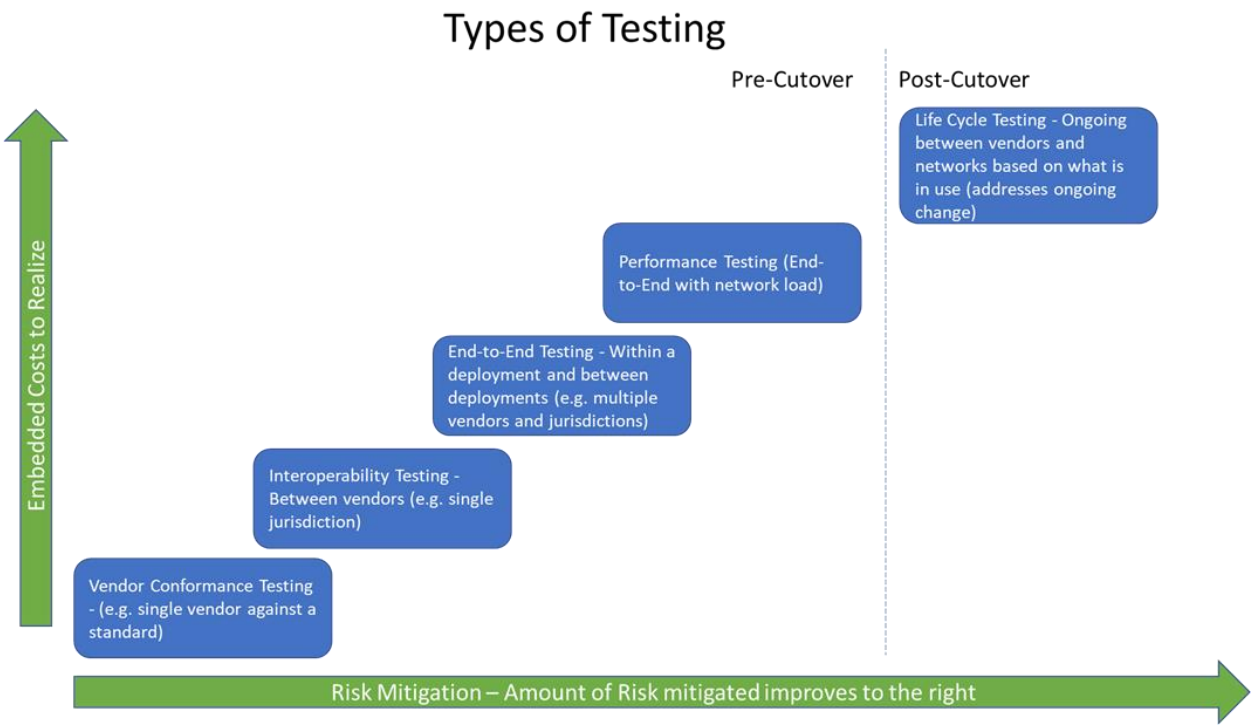
[4] A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

[5] A request for proposal (RFP) is a document that solicits a specific proposal, often made through a competitive bidding process, by an agency or company interested in procurement of commodity, service, or valuable asset, to potential suppliers to submit business proposals. It is submitted early in the procurement cycle, either at the preliminary study, or procurement stage.

5) **Life-Cycle Testing** - Interoperability testing performed prior to the market release of any system changes since the last successful interoperability testing scenario. This testing is the same as interoperability testing but done proactively prior to allowing any changes being made to a customer's environment. This testing is also discussed under "Life-Cycle Testing" below.

All the testing types above are considered "static testing" because they are based on the specific set of conditions at a particular moment in time. Primary conditions include the current version of a standard, element software version, and component hardware configuration. If any one condition changes, relevant testing will need to be repeated including the new condition set.

In the heterogeneous real-world 911 environment, the dynamic nature of change to continually make improvements makes testing even more important to ensure that NG911 systems work as intended. But what extent of testing is practical to mitigate the risks? The chart below is intended to show the risk mitigation benefits and the associated cost implication of the types of testing performed. While significant risk mitigation is possible, it comes at a cost.



Interoperability of NG911 Networks

Legacy 911 systems have traditionally been implemented at stand-alone centers, with limited abilities to transfer calls and associated data, including location data, among PSAPs or regions; as a result, there is generally very limited situational awareness with neighboring 911

environments. NG911, however, provides the capability for a broader perspective on 911 activity. The FCC-commissioned Task Force on Optimal PSAP Architecture (TFOPA), states that in both the Jurisdictional and National End State of NG911, interoperability is necessary. In the National End State, "ESInets are interconnected providing interoperability which is supported by established agreements, policies and procedures".[6]

Interoperability of NG911 networks can be viewed as the interactions required between NG911 networks for the purpose of information transfer between jurisdictions including the caller's location, all notes taken, and any additional information about the caller or the incident to enable the continuation of handling a call.

Benefits of Interoperability of NG911 Networks

Interoperability is a key building block of NG911, providing the following end-state benefits:

- Ability to dynamically share network resources and reroute calls with call-taker notes and data, across NG911 jurisdictions;
- Support for an environment of nationally shared data;
- Capability for overall system monitoring across a region or state;
- Ability to share call answering loads across jurisdictions in the case of a major incident; and
- Ability to benefit from shared mapping or technology to locate and respond to citizens in need.

Status of Interoperability between NG911 Networks

Today, it is more common for interoperability to exist between functional elements *within* a NG911 deployment, but less so for interoperability *between* NG91-1 deployments.

Currently, a significant percentage of 911 jurisdictions have started the transition to NG911 and are in various stages of the process. As these projects are completed, working toward interoperability between NG911 networks will be the next logical effort. Many RFPs that are being issued mention interoperability with neighboring NG911 networks as a requirement.

Achieving real interoperability between NG911 deployments to facilitate complete information exchange and call experience preservation requires mutual agreement in the areas of policy, process, cost sharing, acceptable limitations, technology, testing and continuous improvement. For example, funding policies should facilitate interoperability among jurisdictions, and governance bodies should establish compatible policies and procedures for operations and cybersecurity in an interoperable environment.

[6] Section 3.3 of TFOPA Final Report, Working Group 2, December 2016.

In a pure NG911 environment, interoperability will not be achieved without significant planning, cooperation, and effort.

Future Actions and Possibilities

While interoperability between networks should be (and is, technically) possible today, in practice, such interoperability is rare because of the cost involved and the lack of requirements specified in current RFPs. The complexities of interoperability testing are higher than conformance testing, due to the requirements for multiple vendors to participate in a broad multi-stakeholder environment. . Today, interoperability testing is typically limited to partnerships developed between vendors and occasionally as required by a procuring agency.

In general, there is little formal interoperability testing between disparate deployments. Put simply, each procuring jurisdiction tends to focus on deployment tasks within its own boundaries first and foremost, as to be expected. Therefore, while it is possible and even expected that adjoining but disparate solutions will communicate seamlessly with each other, the reality is that is usually not the case without further consideration and effort. Interoperability testing between NG911 solution providers could address this issue.

Interoperability testing will require a structured agreement by participating NG911 solution providers regarding the following points:

- the extent of testing that is deemed relevant and applicable;
- the standards that will be used for testing; and
- the communication methods expected in the deployment.

To date, the agreements that would set this structure in place are arranged on an as-needed basis rather than as a structured and controlled testing approach.

Interoperability testing is possible through in-house testing labs and/or a structured interoperability lab. However, the vendor community must agree to support this testing, and procuring agencies must agree to accept the additional costs that testing requires. The most important consideration for interoperability is likely a definition of what is relevant and applicable to each disparate solution. Given an agreeable definition, it is a reasonable expectation that solution providers will embrace the need to perform interoperability testing between NG911 systems.

Applying the types of testing outlined in this whitepaper will assure the technical aspects of interoperability persist but when extended to test process and policy, operational excellence can also be achieved.

Life-Cycle Management

Life-cycle management of any product, including software, covers all aspects from start to finish. This includes concept/ideation, design, development, testing, deployment/launch, ongoing support, and finally how the product is retired. Any change, for new or installed product, is also covered by this Life-Cycle Management approach. The goal of this methodology is to ensure that a quality product and all future changes are delivered to the market in a fashion that works as intended and meets the market requirements over the entire expected usefulness of that product.

In many cases, the product requirements are not isolated to how a customer would use or experience the product. Oftentimes the requirements also include interfacing or integrating with another functional element such as a product by another vendor. In the case of NG911 based on the NENA STA-010 (i3) standard, implementation of that standard by different vendors for different elements can still pose a challenge for vendors when attempting to apply the rigorous testing required for interoperability. However, Life-Cycle Management requires this extensive testing and must contemplate the combination of elements that will be in the field to validate any changes prior to being deployed in the field.

Consider, for example, the 911 CHE that needs to interface with a carrier for ANI/ALI or a text provider. If one of these services change and are deployed prior to retesting and revalidation with the 911 CHE solution, there is a possibility that key information will not be available to the telecommunicator. This would have an obvious impact to the 911 operation for as long as it takes to revert or to get a fix agreed upon, tested, and deployed.

The challenge faced by vendors striving for ongoing Life-Cycle Management is how to buy, house, and manage the systems of their integration partners to enable the necessary ongoing testing. Given the breadth of integration partnerships, this can be extremely costly, time consuming, and sometimes unrealistic for vendors even with a standard in place, which is why it is not prevalent in the industry today.

Ongoing Life-Cycle Management testing is critical to ensure that the expectations of 911 Authorities are met and that ongoing interoperability is maximized. The vendor community must diligently practice Life-Cycle Management principles and work closely with their integration partners to retest and revalidate all software updates or other changes prior to those changes being deployed at the 911 Center.

Final Thoughts

Interoperability is an important and complex topic. While ensuring interoperability of NG911 systems will provide enormous benefits, such as increased sharing of resources and data, there are significant challenges to achieving it in a multi-vendor environment. The complexities are compounded by the number of vendors delivering NG-911 products and the frequency of product releases each vendor delivers. Performing the level of testing necessary to ensure interoperability among numerous vendor configurations requires significant investments in time and money. Hopefully this educational white paper has enlightened the reader as to what is required to achieve NG911 interoperability. The iCERT community is committed to working toward the goal of interoperability by working together, with customers, and legislators.

Potential Future Work Items

While this paper covers the general topic of NG911 testing, there are a few topics that may benefit from additional consideration. These include:

1) Security testing. Testing the ability of a system to detect and prevent security intrusions is critical for a NG911 system. Telecommunications Denial of Service Attacks (TDoS) and cybersecurity should be tested; however, how the testing is performed and the results derived therefrom must be treated carefully.
2) Additional details on how each type of testing is best performed including the environment, structure, and oversight.
3) Verification of alarms from IoT devices and systems to ensure they are have met established validation rules.

Glossary[7]

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

Automatic Number Identification (ANI). Telephone number associated with the access line from which a call originates.

American National Standards Institute (ANSI). Entity that coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. www.ansi.org

Border Control Function (BCF). Provides a secure entry into the ESInet for emergency calls presented to the network. The BCF incorporates firewall, admission control, and may include anchoring of session and media as well as other security mechanisms to prevent deliberate or malicious attacks on PSAPs, or ECCs, or other entities connected to the ESInet.

Call. A generic term used to include any type of Request for Emergency Assistance (RFEA); and is not limited to voice. This may include a session established by signaling with two-way real-time media and involves a human making a request for help. We sometimes use "voice call", "video call" or "text call" when specific media is of primary importance. The term "non-human-initiated call" refers to a one-time notification or series of data exchanges established by signaling with at most one-way media, and typically does not involve a human at the "calling" end. The term "call" can also be used to refer to either a "Voice Call", "Video Call", "Text Call" or "Data–only call", since they are handled the same way through most of NG9-1-1. *Source: NENA*

Call Handling System or Equipment (CHE). A Functional Element concerned with the details of the management of calls. It handles all communication from the caller. It includes the interfaces, devices and applications utilized by the Agents to handle the call.

Computer Aided Dispatch (CAD). A computer system, that aids PSAP Telecommunicators by automating selected dispatching and record keeping activities.

Emergency Call Routing Function (ECRF). A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP (or ECC) for the caller's location or towards a responder agency.

Emergency Communications Center (ECC). A facility that is designated to receive a 9–1–1 request for emergency assistance and perform one or more of the following functions: (A)

[7] Except as otherwise noted, the reference source used for the terms in this glossary is the "NENA Master Glossary of 9-1-1 Terminology," NENA-ADM-000.22-2018, released Apr. 13, 2018.

process and analyze 9–1–1 requests for emergency assistance and other gathered information; (B) dispatch appropriate emergency response providers; (C) transfer or exchange 9–1–1 requests for emergency assistance and other gathered information with other emergency communications centers and emergency response providers; (D) analyze any communications received from emergency response providers; or (E) support incident command functions. *Source: Next Generation 911 Act of 2019.*

Emergency Services Routing Proxy (ESRP). A functional element in an ESInet which is a LoST protocol server where location information (either civic address or geo-coordinates) and a Service URN serve as input to a mapping function that returns a URI used to route an emergency call toward the appropriate PSAP, or ECC, for the caller's location or towards a responder agency.

Emergency Incident Data Object (EIDO). A JSON object that is used to share emergency incident information between and among authorized entities and systems and that is conformant with the National Information Exchange Model (NIEM). The EIDO represents the state of an incident as known by the sender at the time it was sent. The EIDO and its conveyance mechanism replace the serial port data connection between CHE and CAD, as well as providing a standardized CAD to CAD interface. It standardizes incident data exchanges between responders and agencies and between agencies working multi-agency incidents and provides a standardized way to send incident data to Emergency Operations Centers (EOCs), tow truck operators, utilities, and even news organizations.

Emergency Medical Dispatch (EMD) refers to a system that enhances services provided by Public Safety Answering Point (or ECC) emergency call takers, such as municipal emergency services dispatchers. It does so by allowing the call taker to quickly narrow down the caller's type of medical or trauma situation, so as to better dispatch emergency services, and provide quality instruction to the caller before help arrives. *Source: Wikipedia*

Emergency Services IP Network (ESInet). An ESInet is a managed IP network that is used for emergency services communications, and which can be shared by all public safety agencies. It provides the IP transport infrastructure upon which independent application platforms and core services can be deployed, including, but not restricted to, those necessary for providing NG911 services. ESInets may be constructed from a mix of dedicated and shared facilities. ESInets may be interconnected at local, regional, state, federal, national and international levels to form an IP-based inter-network (network of networks). The term ESInet designates the network, not the services that ride on the network.

Geospatial Information System (GIS). A system for capturing, storing, displaying, analyzing and managing data and associated attributes which are spatially referenced.

Hazardous Material (HAZMAT). Substances in quantities or forms that may pose a reasonable risk to health, property, or the environment. HAZMATs include such substances as toxic chemicals, fuels, nuclear waste products, and biological, chemical, and radiological agents. HAZMATs may be released as liquids, solids, gases, or a combination or form of all three, including dust, fumes, gas, vapor, mist, and smoke. *Source: National Ocean Service*

Internet Protocol Multimedia Subsystem (IMS). The IP Multimedia Subsystem comprises all 3GPP/3GPP2 core network elements providing IP multimedia services that support audio, video, text, pictures alone or in combination delivered over a packet switched domain.

Next Generation 911 (NG911) Services. A secure, IP-based, open standards system comprised of hardware, software, data, and operational policies and procedures that (A) provides standardized interfaces from emergency call and message services to support emergency communications; (B) processes all types of emergency calls, including voice, text, data, and multimedia information; (C) acquires and integrates additional emergency call data useful to call routing and handling; (D) delivers the emergency calls, messages, and data to the appropriate public safety answering point and other appropriate emergency entities based on the location of the caller; (E) supports data, video, and other communications needs for coordinated incident response and management; and (F) interoperates with services and networks used by first responders to facilitate emergency response. *Source: NENA*

Next Generation Core Services (NGCS). The base set of services needed to process a 911 call on an ESInet. It includes the ESRP, ECRF, LVF, BCF, Bridge, Policy Store, Logging Services, and typical IP services such as DNS and DHCP. The term NG911 Core Services includes the services and not the network on which they operate. See Emergency Services IP Network.

Public Safety Answering Point (PSAP). An entity responsible for receiving 911 calls and processing those calls according to a specific operational policy.